بسم الله الرحمن الرحيم

كتاب بعنوان

شرح لبعض مفاهيم وأساليب التشفير وسرية الشبكات

المحتويات

الحمد

الحمد لله رب العالمين، أعطى اللسان، وعلَّم البيان، وخلق الإنسان، فبأيِ آلاء ربكما تكذبان..

لك الحمد يا من هو للحمد أهل، أهل الثناء والمجد، أحقُّ ما قال العبد وكلنا لك عبد

لك الحمد.. من ضعيف يطلب نُصرتك..

لك الحمد.. من فقير يطلب غناك..

لك الحمد.. من ذليلٍ يطلب عزك..

لك الحمد.. ما دعوناك إلا احسن ظنٍ بك.. وما رجوناك إلا ثقةً فيك، وما خفناك إلا تصديقاً بوعدك ووعيدك.. فلك الحمد..

حمدتك ربي كلما لاح كوكبُ*** وما ناح قمري على الغصن ينددبُ

وشكر جزيلاً والثناء مردودٌ*** لك الحمد ما امتدت إليك المطالبُ

إهداء

إلى النور الذي ينير لي درب النجاح ..أبي

ويا من علمتني الصمود مهما تبدلت الظروف.. أمي

إلى من كانوا يضيئون لي الطريق ويساندوني ويتنـــــــــازلون عن حقوقهم

لإرضائي والعيـــــــــــــــش في هناء ..إخوتي

أحبـــــــكم حبا لو مر عـــلى أرض قاحلة

لتفجرت منها ينابيع المحـــــــبة

أهدي هذا الكتاب المتواضع راجياً من المولى

عز وجل أن يجد القبول والنجاح

لا زلت طالبا في مدرسة الحياة من ظن أنه قد علم فقد جهل

ولا تنسوني من صالح دعواتكم . . .

تنبيه

هذا الكتاب ليس مرجعا كاملا للمذاكرة وإنما هو تجميعي لبعض المفاهيم وفهم بعض النقاط التي تكون غامضة لدى بعض الدراسين فهناك بعض العناوين التي لم أتطرق لها في هذا الكتاب

أسأل الله تعالى أن يكون هذا العمل خالصا لوجه الكريم..

أتقبل آراءكم وجميع انتقاداتكم بكل فرح وسرور فالمسلم مرآة أخيه المسلم إن أصبت فأعينوني وإن أخطأت فقوموني...

معلومات عن كاتب البحث :

الاسم : محمود بشرى محمد إبراهيم

العمر : ٢٣ سنة .

المؤهل : بكلاريوس علوم الحاسوب جامعة السودان للعلوم والتكنولوجيا .

سنة التخرج : ٢٠١٣ .

البريد الالكتروني : hoota0500@hotmail.com

Chapter 1

Introduction

Chapter 1

Introduction

*** Computer security:** هو عبارة عن حماية نظم المعلومات لتحقيق الأهداف الأساسية التالية:

١- تكامل البيانات (Date integrity) . ٢- الاتاحية (**availability**)
٢- السرية (**confidentiality**) .

إضافة إلى أهداف أخرى هي:

التحقق (**Authenticity**) و المسؤولية (**Accountability**) .

*** level impact تعني مستويات التأثير في الشبكة :**

١- high ٢- moderate . ٣- low

أمثلة على ذلك :

الهدف	تأثير **high**	تأثير **moderate**	تأثير **low**
confidentiality	درجات الطلاب تكون متوفرة لهم فقط	معلومات التسجيل للطلاب	دليل الكلية او القوائم الإدارية متوفرة للجميع
Integrity	المعلومات الخاطئة للمريض تؤدي إلى أذى او موت حقيقي	مواقع الويب المنتديات تتطلب التسجيل لمناقشة موضوع معين	الاستطلاع على الانترنت مجهول الهوية
availability	خدمات التحقق للأنظمة الحرجة	موقع ويب عام للجامعة به معلومات الطلاب	مشاهدة دليل الهاتف على الانترنت

*** تحديات أمن الكمبيوتر (computer security challenge) :**

١- ليس بسيط. ٢- الاخذ بالاعتبار بهجمات مختلفة. ٣- الاجراءات الغير متوقعة .

٤- ضمان الخوارزمية والمعلومات السرية. ٥- معرفة الذكاء بين المهاجم والإدارة.

٦- المراقبة المنتظمة. ٧-اعتبار عوائق العمل.

*** يركز OSI Security Architecture on Security attack على :**

١- security machine :

هي عملية مصممة لاكتشاف أو منع أو استعادة security attack

٢- security service:

هي خدمة اتصال أو معالجة تحسن من أمن نظم تشغيل البيانات او انتقال المعلومات .

(service التي تنوي مواجهة attack تستعل وحدا من machine أو أكثر) .

*** سمات السرية (aspect of security) :**

- ***threat***: عملية تجهز لعمل attack وهي علمية إنذار بحدوث هجوم

- **attack**: هجوم مباشر حدث على نظام المعلومات .

* متطلبات نموذج الشبكات :

- model for network Security:

١- خوارزمية مناسبة. ٢- توليد المفاتيح قبل الخوارزمية . ٣- تطوير طرق التوزيع والاشتراك في المعلومات السرية.

٤- تحديد نظام للمسؤول لتحويل المعلومات السرية إلى جهاز الأمن.

- model for network Access security:

١- تشغيل البوابة (المنفذ) لتمييز المستخدمين.

٢- دخول المعلومات مضمون لوجود المستخدم المصرح له فقط.

1.1 What is the OSI security architecture?

1.1 The OSI Security Architecture is a framework that provides a systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. The document defines security attacks, mechanisms, and services, and the relationships among these categories.

1.2 What is the difference between passive and active security threats?

1.2 **Passive attacks** have to do with eavesdropping on, or monitoring, transmissions. Electronic mail, file transfers, and client/server exchanges are examples of transmissions that can be monitored. **Active attacks** include the modification of transmitted data and attempts to gain unauthorized access to computer systems.

1.3 List and briefly define categories of passive and active security attacks

1.3 **Passive attacks:** release of message contents and traffic analysis. **Active attacks:** masquerade, replay, modification of messages, and denial of service.

security mechanisms

Encipherment
Digital signature
Access control
Data integrity
Authentication exchange
Traffic padding
Routing control
Notarization

security services

Peer entity authentication
Data origin authentication
Access control
Confidentiality
Traffic flow confidentiality
Data integrity
Non-repudiation
Availability

Chapter 2

Cryptography and Network Security

Chapter 2: Cryptography and Network Security

* **التشفير (Encryption) أو (E) :** اخفاء المعنى الحقيقي لمحتوى الرسالة باستخدام KEY بطريقة يتم الاتفاق عليها بين المرسل والمستقبل للرسالة

* **فك التشفير (Decryption) أو (D):** عكس عملية التشفير ويتم فيها اظهار محتوى الرسالة باستخدام KEY أيضا .

* **مفاهيم أساسية أو كلمات مفتاحية :**

- **cryptography :** دراسة التشفير ومبادئه وطرقه. وهذا محور دراستنا في هذا الفصل
- **cryptanalysis :** دراسة الطرق والمبادئ والتحليل لمعرفة فك التشفير بدون KEY
- **cryptology** : دمج للمفهومين السابقين .
- **plaintext**: النص قبل عملية التشفير وهو الأصلي أو الصريح.
- **ciphertext** : النص بعد عملية التشفير وهو النص المشفر.

* **يمكن دراسة خصائص cryptography system من خلال التقسيم التالي:**

١. **نوع عملية التشفير:**
   - **Substitution**
   - **transposition**
   - **product**
٢. **عدد المفاتيح :**
   - **single-key or private or symmetric**
   - **two-key or public or asymmetric**
٣. **طريقة معالجة plaintext النص الأصلي :**
   - **Steam cipher**
   - **Block cipher**

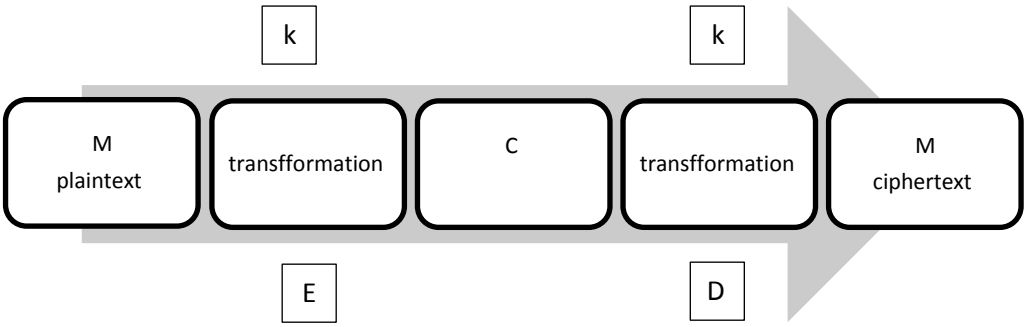
* **متطلبات التشفير المتماثل:**

١- خوارزمية تشفير قوية. ٢- secret key يكون معروف فقط لدى المرسل والمستقبل

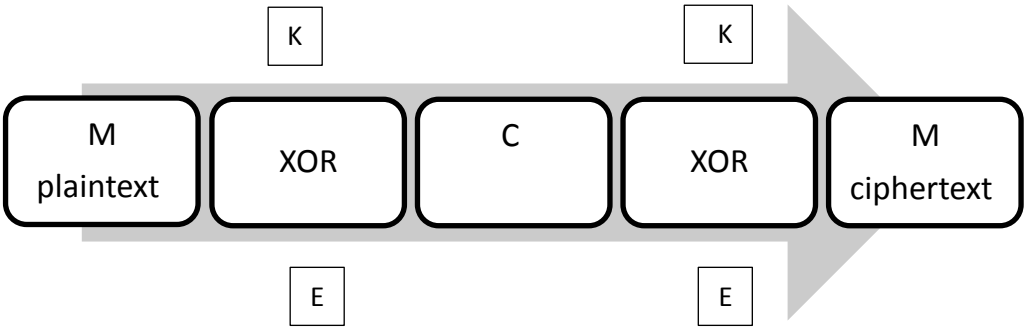
* **يتكون نظام التشفير الانسيابي (Stream) من :**

١- خوارزمية توليد سلسلة المفاتيح شبه العشوائية. ٢- المازج (MIXER) وهو XOR .

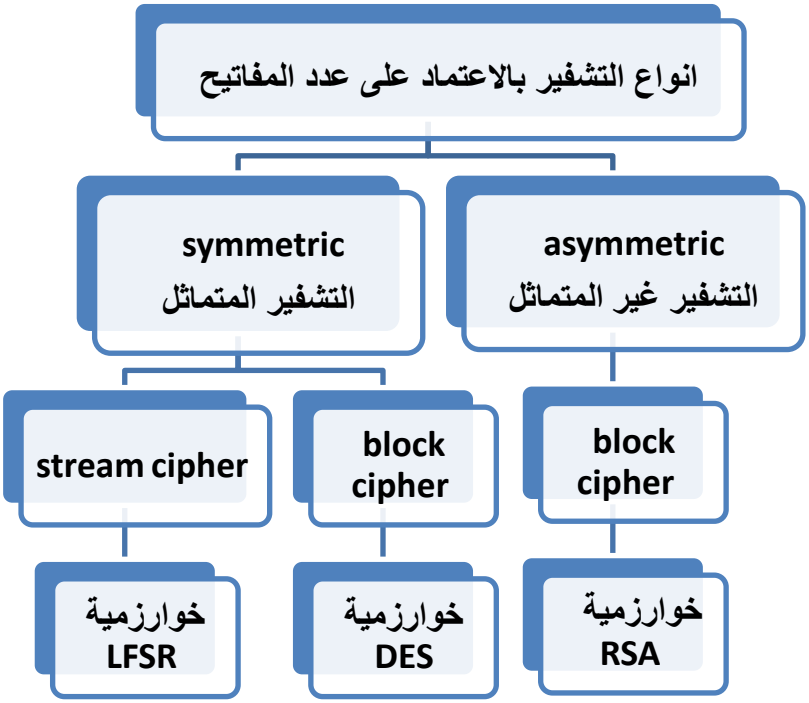
* **أشكال التشفير:**



Block cipher



Stream cipher



* **الهدف من Cryptanalysis** : استرجاع ومعرفة Key + Message

* **طرق Cryptanalysis :**

١- **cryptanalytic attack :** يحتاج إلى معرفة طبيعة الخوارزمية + بعض خصائص plaintext

٢- **brute-force attack:** عدد من المحاولات لمعرفة ايضا معرفة طبيعة الخوارزمية + بعض خصائص plaintext

* **أنواع Cryptanalytic Attacks :**

١- **ciphertext only :** معرفة الخورازمية + ciphertext أصعب نوع

٢- **known plaintext :** معرفة الخوارزمية + ciphertext + plaintext

٣- **chosen plaintext:** اختيار عشوائي ويقوم بعملية التشفير على plaintext

٤- **chosen ciphertext**: اختيار عشوائي ويقوم بعملية فك التشفير على ciphertext

٥- **chosen text**: سلسلة من الاختيارات بين ciphertext + plaintext

* **مستويات الأمن :**

١- **unconditional security :** المهاجم إذا وصلته شفرة لا يستطيع كسرها مهما كلف الأمر ووجدت فقط في **خوارزمية One-time pad**

٢- **computational security** : يمكن فك الشفرة للخوارزمية ولكن هذا يتطلب الكثير من التكلفة الوقت ويتم تحقيق هذا المستوى من الأمن باستخدام مفتاح مناسب ذو طول ١٦٤ بت مثلا .

* **التشفير بالاحلال (Substitution) وتعمتد على تبديل الاحرف يوجد نوعين :**

١- **الأحادية الأبجدية (Monoalphabetic Ciphers) :** أقدم نوع وأسهل كثيرا لكل حرف بديل واحد فقط . ويتم ذلك عن طريق استبدال كل حرف بالحرف الثالث بعده في الترتيب الأبجدي في علمية التشفير وقبله في عملية فك التشفير . مثال :

تشفير كلمة P H : ME الحرف الثالث بعد M هو P والثالث بعد E هو H

فك تشفير كلمة J B : ME الحرف الثالث قبل M هو J والثالث قبل E هو B

٢- **أبجدية بولي(Polyalphabetic Ciphers) :** يمكن ان يكون لأي حرف اكثر من بديل

ونأخذ مثال لها خوارزمية **Playfair Cipher** :

يتم انشاء مصفوفة 5*5 يوضع كل حرف في خانة وتعتبر هذه المصفوفة مفتاح التشفير

والتشفير يتم : يتم تشفير كل خرفين من النص الأصلي سويا وتوجد حالات له في المثال :

L	O	V	E	I/J
S	A	M	N	Y
P	D	R	T	H
G	B	C	F	K
Q	U	W	X	Z

قم بتشفير النص التالي باستخدام المصفوفة أعلاه :

AMBASSADORSHOT

الحل :

- ✓ تقسيم النص إلى Block يتكون من حرفين :

AM BA SS AD OR SH OT

- ✓ الحروف المتشابهة نضيف بينها حرف X

AM BA SX SA DO RS HO T

- ✓ الحرف الوحيد نضيف له أيضا حرف X
- ✓ AM BA SX SA DO RS HO TX
- ✓ نأخذ ال Block الأول ونبدأ عملية التشفير :
  - الحروف في نفس الصف كل حرف بالحرف الذي يليه يمينا
  - الحروف في نفس العمود كل حرف بالحرف الذي تحته مباشرة
  - الحروف المتباعدة نشفر بأحرف التقاطع .

AM: M =A N = M

BA: U = B D = A

SX: تشفير S الحرف المشترك الذي هو في عمود S وصف X وهو Q

تشفير X الحرف المشترك الذي هو في عمود X وصف S وهو N

*** خوارزمية تشفير ONE- Time pad (الشفرة الآمنة):**

- إذا استخدما مفتاح عشوائي نفس طول الرسالة يكون التشفير آمن - لماذا؟

لأنه لا يوجد تكرار للمفتاح وبالتالي عند فك التشفير للرسالة تظهر رسالتين لا تعرف أيهم الرسالة الأصلية .

- غير قابلة للكسر: لأنه لا توجد علاقة إحصائية بين النص المشفر والنص الأصلي.

- ولفك التشفير تحتاج إلى مفتاح عشوائي بنفس طول النص الصريح ومعرفته صعبة.

*** مشاكل خوارزمية ONE- Time pad :**

١- توليد كمية كبيرة من المفاتيح العشوائية.

٢- مشكلة التوزيع والحماية حيث تتطلب مساواة طول المفتاح مع الرسالة المرسلة بين المرسل والمستقبل.

*** التشفير باستخدام (Transposition) : تعتمد على إخفاء الرسالة عن طريق إعادة ترتيب أحرف الرسالة دون تغييرها بحروف أخرى وتوجد طريقتين هي :**

١- **Rail –fence cipher:** وتعتمد على إعادة ترتيب بطريقة عشوائية بدون قاعدة :

النص الأصلي Hello World إعادة ترتيبه هي HLOOl EIWRD

٢- **Row Transposition Ciphers :** إعادة ترتيب للعمود حسب المفتاح المطلوب فهو يعطي plaintextونضعها في مصفوفة من ١ـــ ٧ ترقم حسب Key المعطى
ثم يعاد ترتيبها من ١ـــــ٧ باعتبار الترقيم حسب KEY قائم . (تفهم مع المثال) :

مثال :

Key : 4 3 1 2 5 6 7

Plaintext : attack postponed until two me

4	3	1	2	5	6	7
a	T	T	A	C	k	P
p	S	T	P	O	n	E
d	U	N	T	I	l	T
W	O	A	M	X	y	Z

- ✓ نقوم بكتابة الترتيب من ١ ـــــ٧
- ✓ نقوم بأخذ العمود اللي يمثل رقم ١ وهو رقم ٣
- ✓ نقوم بأخذ العمود اللي يمثل رقم ٢ وهو رقم ٤
- ✓ نقوم بأخذ العمود اللي يمثل رقم ٣ وهو رقم ٢
- ✓ نقوم بأخذ العمود اللي يمثل رقم ٤ وهو رقم ١
- ✓ وهكذا .....

1	2	3	4	5	6	7
3	4	2	1	5	6	7

فك التشفير : نأخذ العمود ==> وفك التشفير نقوم بالعكس

التشفيـــــــــــــر : TTNAAPTMSUOAODWCOIXKNLYPETZ

*** خوارزمية Product Ciphers**

هي الخوارزميات التي تستخدم **Substitution** يتبعها Transposition وتعتبر أكثر أمانا ومقاومة للكسر وهذا هو الجسر الفاصل ين الخوارزميات الكلاسيكية والحديثة.

Note

O One-Time Pad

- since for **any plaintext** & **any ciphertext** there exists a key mapping one to other
- can only use the key **once** though
- has two fundamental difficulties:
- **large quantities of random keys-**heavily used system
- **key distribution and protection.**

2.1 What are the essential ingredients of a symmetric cipher?
2.1 Plaintext, encryption algorithm, secret key, ciphertext, decryption algorithm.

2.2 What are the two basic functions used in encryption algorithms?
2.2 Permutation and substitution.

2.3 How many keys are required for two people to communicate via a cipher?
2.3 One key for symmetric ciphers, two keys for asymmetric ciphers.

2.4 What is the difference between a block cipher and a stream cipher?
2.4 A **stream cipher** is one that encrypts a digital data stream one bit or one byte at a time. A **block cipher** is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

2.5 What are the two general approaches to attacking a cipher?
2.5 Cryptanalysis and brute force.

2.8 Briefly define the Caesar cipher
2.8 The **Caesar cipher** involves replacing each letter of the alphabet with the letter standing *k* places further down the alphabet, for *k* in the range 1 through 25.

2.9 Briefly define the monoalphabetic cipher
2.9 A **monoalphabetic substitution cipher** maps a plaintext alphabet to a ciphertext alphabet, so that each letter of the plaintext alphabet maps to a single unique letter of the ciphertext alphabet.

2.10 Briefly define the Playfair cipher.

2.10 The **Playfair algorithm** is based on the use of a 5 × 5 matrix of letters constructed using a keyword. Plaintext is encrypted two letters at a time using this matrix.

2.11 What is the difference between a monoalphabetic cipher and a polyalphabetic cipher?

2.11 A **polyalphabetic substitution cipher** uses a separate monoalphabetic substitution cipher for each successive letter of plaintext, depending on a key.

2.13 What is a transposition cipher?

2.13 A **transposition cipher** involves a permutation of the plaintext letters.

2.14 What is steganography?

2.14 Steganography involves concealing the existence of a message.

Chapter 3

Block Ciphers and the data encryption standard

Chapter 3

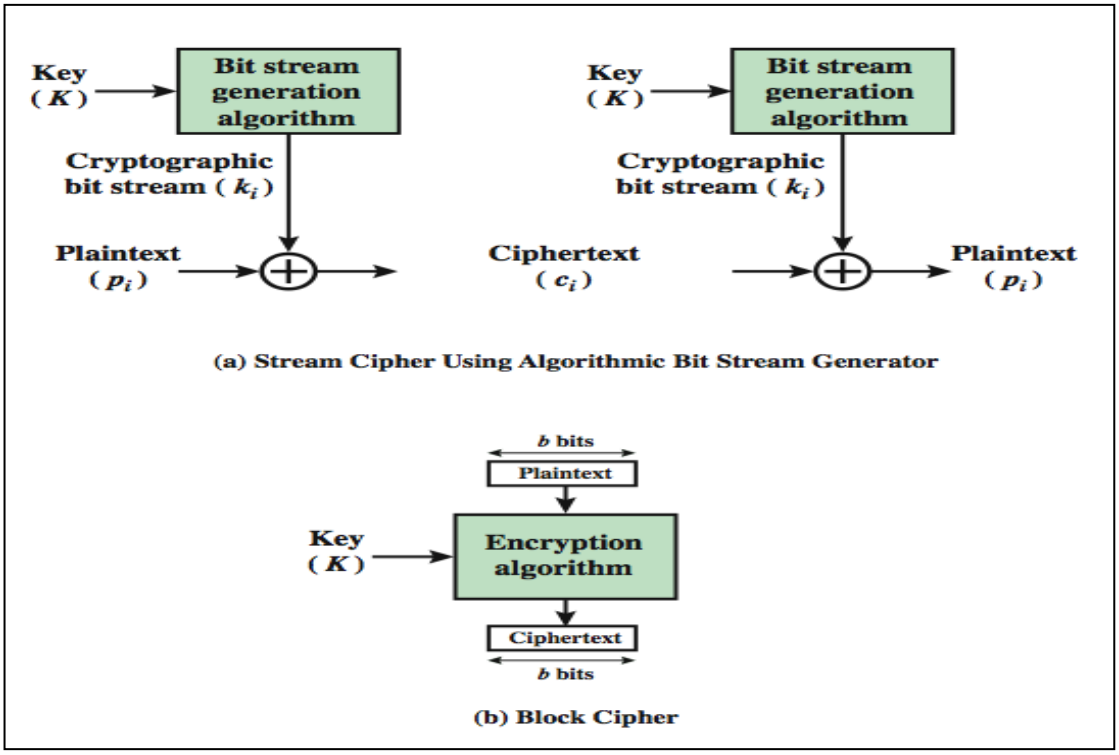
Block Ciphers and the data encryption standard

*** stream cipher:** عبارة عن تشفير بيانات على هيئة bit او عدد من byte كل مرة

أمثلة : autokeyed Vigenère cipher and the Vernam cipher. .

*** Block cipher:** عبارة عن block من plaintext يعالج لإنتاج cipher text مساويا للطول واغلب cipher عبارة عن block cipher .

الرسم :



Note

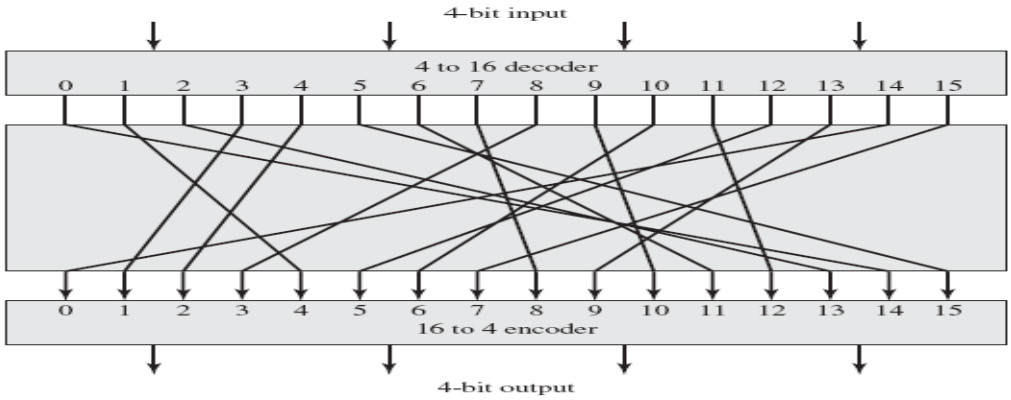
Many symmetric block encryption algorithms in current use are based on a structure referred to as a **Feistel block cipher**

Feistel approximates the ideal block cipher by utilizing the concept of a ***product*** cipher

Feistel proposed the use of a cipher that alternates ***substitutions*** and ***permutations***.

In fact, Feistel's is a practical application of a proposal by ***Claude Shannon*** to develop a product cipher

Feistel block cipher



4-bit input produces one of ***16*** possible input states, which is mapped by the substitution cipher into a unique one of ***16*** possible output states, each of which is represented by ***4*** ciphertext bits.

اقترح Feistel أنه يمكن تطوير شفرات تبديل الحروف البسيط عن طريق تطبيق مفهوم ضرب التشفير حيث يمكن تطبيق تشفيرين متتالين أو اكثر بحيث يكون أقوى.

التشفير الكتلي يستخدم : ٦٤ أو ١٢٨ خانة

ideal block cipher : هو عبارة عن هيكلة التصميم معتمدة على جدول به تمثيل ثنائي ٠.١ لل plaintext وciphertext في عملية التشفير وفك التشفير.

Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Ciphertext	Plaintext
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100
0110	1010
0111	1111
1000	0111
1001	1101
1010	1001
1011	0110
1100	1011
1101	0010
1110	0000
1111	0101

* لدينا مقترح من ***Claude Shannon***

بانتاج تشفير مؤلف من تعاقب تابعي البعثرة والنشر ***confusion*** & ***diffusion***

حيث اشار إلى انه يجب أن تكون كل المعلومات الإحصائية للنص المشفر مستقلة عن المفتاح الخاص بالمستخدم باستخدام :

Diffusion (النشر) : أن تكون العلاقة ين النص الصريح والنص المشفر أعقد ما يكون.

Confusion) البعثرة): ان تكون العلاقة بين النص المشفر وقيمة المفتاح أعقد ما يكون.

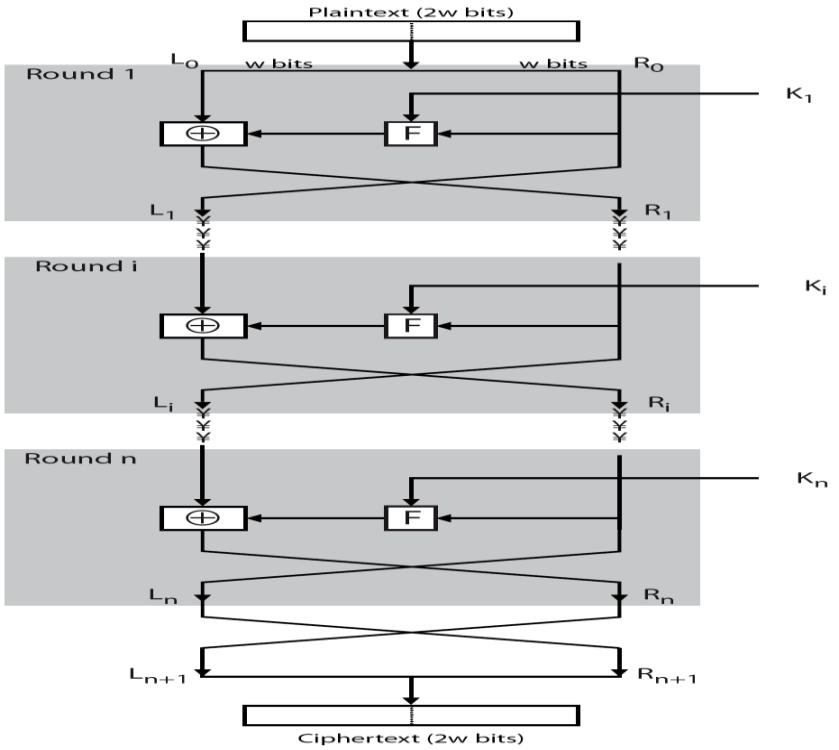
_النشر والبعثرة هي جوهرة عملية التشفير الكتلي وحجر الأساس في تصميم نظام التشفير الكتلي الحديثة.

*** بنية نظام التشفير *Feistel Cipher Structure* :**

عدد الحلقات هي ١٦ حلقة .

طول الكتلة : ٦٤ **طول المفتاح** ١٢٨

المفتاح الاطول مستوى أمن أكبر لكن سرعة تشفير وفك تشفير أقل .



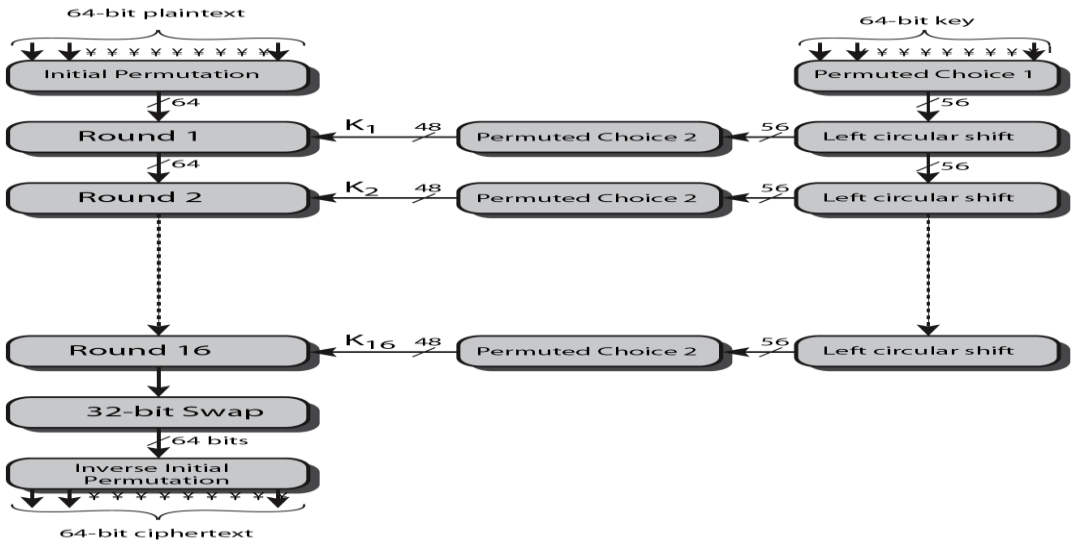
*** مقياس تشفير المعطيات (The Data Encryption Standard(DES))**

يتم تشفير المعطيات على شكل block بطول ٦٤ وطول مفتاح باستخدام ٦٥ خانة

- قامت شركة IBM بإنتاج خوارزمية LUCIFER عبارة عن نظام تشفير Block fesitel ويعمل طول كتلة ٦٤ خانة ومفتاح ١٢٨ خانة .

- قام باحثون من NSA بإنتاج خوارزمية LUCIFER ولكن بطول ٥٦ خانة .

*** البنية العامة للتشفير وفق DES**



اختصار ما سبق :

- **الدخل** : plaintext = M KEY = K مقسمة وكل واحد يساوي ٦٤ خانة
- **الخرج** : ciphertext= C وتحدث به الإجرائيات التالية:

١- توليد المفاتيح بعدد ١٦ مفتاح طول كل وحد ٤٨ .

٢- L0, R0 ويستخدم التبديل في ذلك

٣- التبديل والتوسيع.

*** توليد المفاتيح:**

- **الدخل:** مفتاح ذو ٦٤ خانة (ثماني خانات ازدواجية) .

- الخرج : ١٦ مفتاح كل مفتاح طوله ٤٨ خانة.

- تتم معالجة المفتاح ذو ٥٦ خانة على نصفين كل واحد ٢٨ خانة وتحصل عملية ازاحة دورانية يسارية ينتج عنها مفتاح طوله ٥٦ خانة يدخل للحلقة القادمة .

Details Of Single Round*

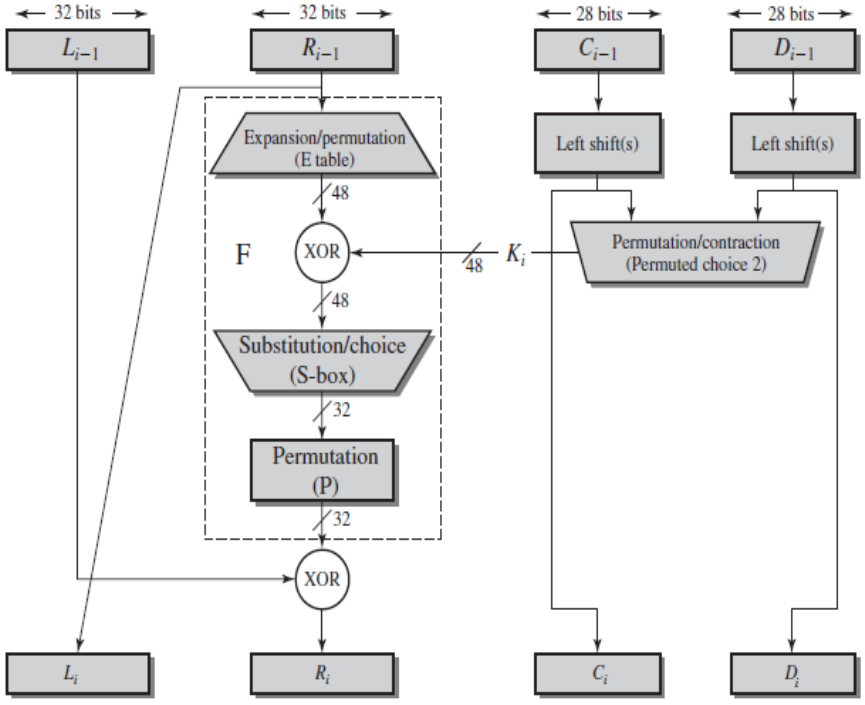


Figure 3.6 Single Round of DES Algorithm

تستخدم العمليات التالية:

Expansion : توسيع المفتاح إلى قيمة أكبر .

permutation : تبديل مواقع محتوى الرسالة بينهم .

S-boxes: تبديل محتوى الرسالة بمحتوى آخر من جدول مركب . **إضافة إلى XOR**

*** قوة خوارزمية DES:**

١- طول المفتاح ٥٦ :

يعني وجود ٥٥٦ مفتاحا مختلفا حيث ان محاولة الهجوم الأعمى غير عملية نهائيا

- قامت شركة مرة بإعلان عن كسر خوارزمية DES باستخدام طريقة DES cracker machine وتمت بأقل من 250,000$.
- وجدت اطوال بديلة بإنتاج خوارزميات من DES-3 وخوارزمية جديدة AES

٢- طبيعة الخوارزمية :

ركزت على جدول التباديل (S-box) والتي تستخدم كل مرة ولم تنشر للعوام .

*** الهجوم الزمني (timing Attack) :**

هو الذي يتم من خله الحصول على معلومات طول المفتاح أو النص الأصلي من خلال مراقبة الزمن اللازم في تطبيق ما لإنجاز عملية فك التشفير لنصوص مشفرة مختلفة.

- توصلوا إلى ان ال DES مقاومة للهجوم الزمني.
- أكدوا ان الهجوم لن يكون ناجحا مع خوارزمية ال Desأو خوارزميات Des الثلاثية أو خوارزمية AES

3.1 Why is it important to study the Feistel cipher?

3.1 Most symmetric block encryption algorithms in current use are based on the Feistel block cipher structure. Therefore, a study of the Feistel structure reveals the principles behind these more recent ciphers.

3.2 What is the difference between a block cipher and a stream cipher?

3.2 A **stream cipher** is one that encrypts a digital data stream one bit or one byte at a time. A **block cipher** is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

3.4 What is a product cipher?

3.4 In a product cipher, two or more basic ciphers are performed in sequence in such a way that the final result or product is cryptographically stronger than any of the component ciphers.

3.6 Which parameters and design choices determine the actual algorithm of a Feistel cipher?

- Block size
- Key size.
- Number of rounds.
- Subkey generation algorithm.
- Round function.
- Fast software encryption/decryption.
- Ease of analysis**.**

3.7 What is the purpose of the S-boxes in DES?

3.7 The S-box is a substitution function that introduces nonlinearity and adds to the complexity of the transformation.

3.8 Explain the avalanche effect.

3.8 The avalanche effect is a property of any encryption algorithm such that a small change in either the plaintext or the key produces a significant change in the ciphertext.

3.9 What is the difference between differential and linear cryptanalysis?

3.9 **Differential cryptanalysis** is a technique in which chosen plaintexts with particular XOR difference patterns are encrypted. The difference patterns of the resulting ciphertext provide information that can be used to determine the encryption key. **Linear cryptanalysis** is based on finding linear approximations to describe the transformations performed in a block cipher.

Chapter 5

Advanced Encryption Standard

Chapter 5
Advanced Encryption Standard

* يعد مقياس AES **Advanced Encryption Standard** من أشهر خوارزميات التشفير.

* كان مقياس Des على وشك الاختراق ولم تكن تلك الخوارزمية ذات فعالية واستخدمت مفتاح ذو ٥٦ خانة لعلمية التشفير وفك التشفير.

* تم استبدال مقياس DES بمقياس AES عام ٢٠٠٠ م

* وفي عام ١٩٩٧م قام معهد (ANSI) بإجراء منافسة باستخدام مقياس AES لتخطي سلبيات DES ويحقق المعايير التالية :

١- أن تكون الخوارزمية معرفة علنا وتكون السرية في المفتاح المستخدم.

٢- أن يستخدم التشفير المتماثل. ٣- إمكانية زيادة طول المفتاح حسب الحاجة.

٤- إمكانية تنفيذ الخوارزمية إما عن طريق Hardware أو Software .

تلك هي المعايير الأولية ومن ثم جاءت معايير أخرى مستندة على المعايير الأولى وهي :

١- الأمن .
٢- الكفاءة والبساطة والمرونة .
٣- التكلفة.
٤- آلية التنفيذ

ولقد تم اختيار خوارزمية **Rijndael** .

*** مفاهيم أساسية:**

- مقياس AES يستخدم خمس وحدات قياس للإشارة إلى البيانات هي :

State	Block	Word	Byte	Bit
4*4 = 128bit	128 bit	32 bit	8bit	0,1

- المدخلات والمخرجات عبارة عن Block ذو 128 bit

- التشفير وفك التشفير في AES يستخدم Round تحتوي **على أربع عمليات** .

*** خوارزمية Rijndael :**

- تعتمد على عمليات تختص بالمصفوفات الرياضية

- تدعم 128 – 192 – 256 bit كطول للمفتاح .

- تشفر نصوص بأحجام مختلفة.

- أخذ في الاعتبار أثناء تصميمها يكون مقاوم لجميع الهجمات المعروفة وأن يكون سريعا لا يستهلك الكثير من الذاكرة.

- مكونات الخوارزمية :

عدد من الدورات يمكن تكرارها كل دورة بها اربع عمليات لها معكوس **تكرر الدورات حسب طول المفتاح**.

كل عملية تسمى layer وكل layer تقدم خاصية أمنية معينة .

علاقة بين عدد الدورات وطول المفتاح

عدد الدورات	طول المفتاح	AES
10	4	AES 128
12	6	AES192
14	8	AES256

*** هيكل كل دورة من الدورات :**

تحتوي الدورة على اربع عمليات تقدم كل منها خاصية أمنية معينة في التشفير وهي :

١- الاستبدال (**Substitute**).
٢- التقليب او الإزاحة (**Permutation**).
٣- المزج (**MixColumns**).
٤- إضافة المفتاح الخاص بالدورة (**AddRoundKey**) .

Note: الدورة الاخيرة في العمليات تحتوي على جميع العمليات ما عدا **AddRoundKey**

*** عمليات التشفير:**

- قبل بداية التشفير يتم تحويل النصوص إلى أرقام سداسي عشرية باستخدام الجدول كما سيأتي.

- المدخلات فيه بطول 128 bit ويتم التقسيم إلى إلى مجموعات كل مجموعة بها 16byte
لاحظ ان 128bit = 16 byte

a	b	c	D	E	F	G	H	I	J	.....	.....	Z
00	01	02	03	04	05	06	07	08	09	.....	.....	25

١- الاستبدال (**Substitute**):

يطلق عليها SubBytes: هي عملية استبدال غير خطية نستخدم فيها S-box يقوم باستبدال المدخلات بمخرجات مختلفة حسب جدول الاستبدال وتكون مصفوفة 4*4 .

٢- التقليب (**Permutation**) :

يطلق عليها ShiftRow: تغيير أماكن البايت بناء على رقم الصف الذي ينتمي إليه

الصف(0) لا نغير فيه أي شيء الصف(1) إزاحة بمقدار 1 بت

الصف(2) إزاحة بمقدار 2 بت الصف(3) إزاحة بمقدار 3 بت

مع ملاحظة الإزاحة في **التشفير إلى اليسار ــ وفك التشفير إلى اليمين**

٣- المزج (**MixColumns**) **:**

إخفاء العلاقة بين النص المشفر والنص الصريح حيث تعمل على ضرب كل عمود من أعمدة المصفوفة بمصفوفة ثابتة وهي **عملية ضرب صف في عمود** .

مثال :

1	1	1	1	1	1	1	1
X^7	X^6	X^5	X^4	X^3	X^2	X	1

نقوم بتمثيل الرقم 02 والتمثيل يكون : 0010 0000 وتعني X^2 ----------> معادلة *1*

نقوم بتمثيل الرقم *87* والتمثيل يكون : *1000 0111* وتعني $X^7 + X^2 + X + 1$ -- > *2*

نقوم بضرب المعادلة *1* في المعادلة *2* ونحصل على الآتي :

$$X^2 * (X^7 + X^2 + X + 1) = X^8 + X^3 + X^2 + X + 1 = 10000\ 111$$

نرى أن الناتج عبارة عن *9* خانة نقوم بحذف الخانة الاخيرة *10000 111*

ونعمل عملية *XOR* مع القيمة الثابتة *00011011*

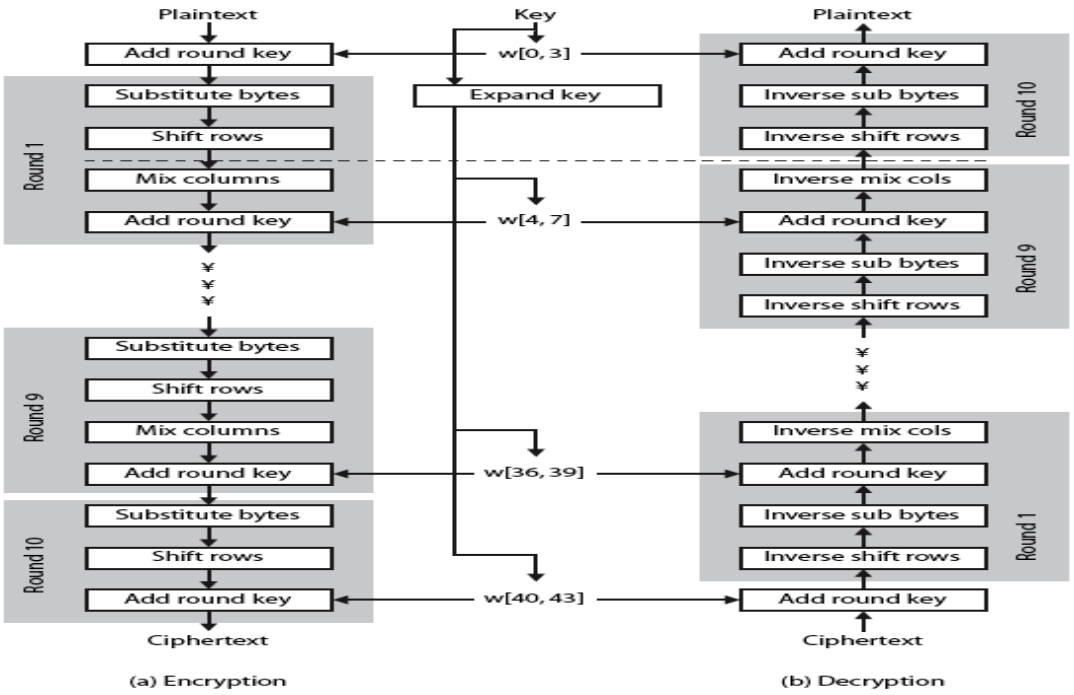
$$00001110 \oplus 00011011 = 00010101$$

٤- إضافة المفتاح الخاص بكل دورة (**AddRoundKey**) **:**

هي اهم عملية في مقياس *AES* : تكمن الأهمية في فيها حيث أن جميع العليمات السابقة معلنة ومعروفة لدى الجميع فسرية التشفير هي سرية المفتاح المستخدم

- مقياس التشفير *AES* يستخدم ما يسمى بمولد المفاتيح (*Key generation*) يقوم بتوليد مفتاح لكل دورة كل دورة تحتاج إلى مفتاح طوله *128 bit* .

- تقوم هذه العملية بجمع مفتاح الدورة القادم من مولد المفاتيح مع المصفوفة أي تعمل عملية المصفوفة *Key XOR* .



*** *KEY Schedule* :**

- ونقصد بها أخذ ال *Key* ونعمل منه *11* نسخة يستخدموا في عملية *Add round Key* في عملية التشفير .

- يكون لدينا *Round* بحسب نسخ المفاتيح وهي *Round 0 –round1 …….round 10*

- أول خطوة هي وجود مصفوفة كبيرة بها ٤٤ عمود *Expanded Key*

- ويتم اختيار الاعمدة ذات *index* من مضاعفات الرقم ٤ وهي *4, 8, 16 ..etc* . ويعتبر *0* مضافا إليهم وهنا تحدث ثلاث عمليات :

١- *Rot word* : أول خانة في العمود تكون آخر خانة ونعمل *shift* لأعلى.
٢- *sybByte*: نأخذ الرقم ونرى نظائره في اعمدة والصف جدول *S-box* .
٣- *Rcon*: جدول ثابت مثل *S-box*.

لاحظ ان الأعمدة ذات مضاعفات *4* يتم عمل الثلاث العمليات السابقة لها والاعمدة الأخرى نعمل لها عملية واحدة هي *XoR with RCon*

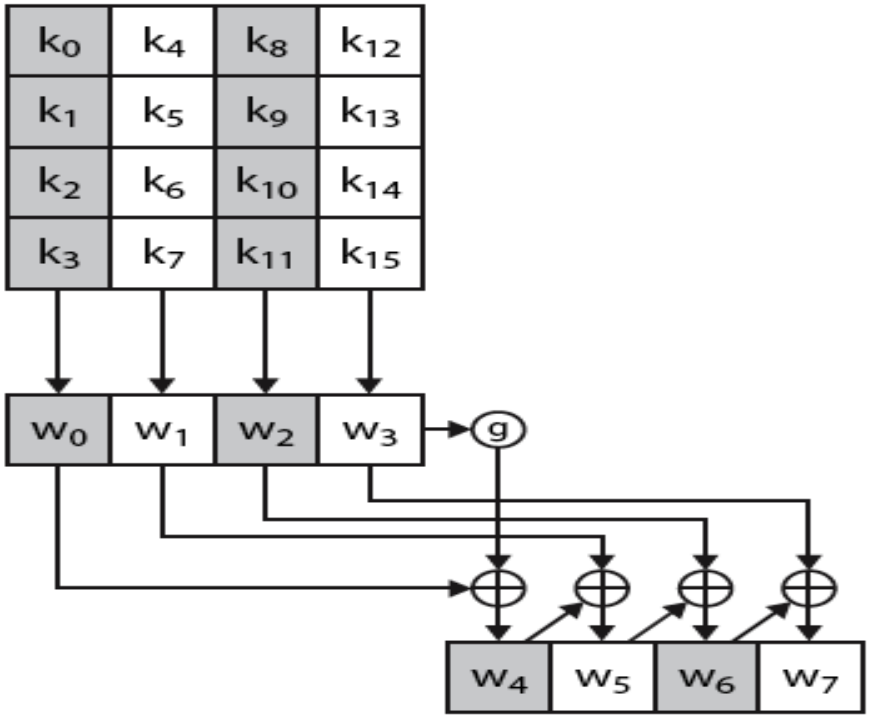
ويكون لدينا الناتج عبارة عن *Expanded Key* ويكون من ضمنه *Round Key 11* بما فيهم *Round Key 0* الذي هو ال *Key* الأصلي ويستخدم في عملية *Add round Key*

مثال : للاطلاع

For example,the round key for round 8 is:

EA D2 73 21 B5 8D BA D2 31 2B F5 60 7F 8D 29 2F

Then the first 4 bytes (first column) of the round key for round 9



i (decimal)	temp	After RotWord	After SubWord	Rcon (9)	After XOR with Rcon	w[i−4]	w[i] = temp ⊕ w[i−4]
36	7F8D292F	8D292F7F	5DA515D2	1B000000	46A515D2	EAD27321	AC7766F3

Note :

The AES Cipher - Rijndael

- *designed by Rijmen-Daemen in Belgium*
- *has 128/192/256 bit keys, 128 bit data*
- *an **iterative** rather than **feistel** cipher*

5.1 What was the original set of criteria used by NIST to evaluate candidate AES ciphers?

5.1 **Security:** Actual security; randomness; soundness, other security factors.

Cost: Licensing requirements; computational efficiency; memory requirements.

Algorithm and Implementation Characteristics: Flexibility; hardware and software suitability; simplicity.

5.2 What was the final set of criteria used by NIST to evaluate candidate AES ciphers?

5.2 General security; software implementations; restricted-space environments; hardware implementations; attacks on implementations; encryption vs. decryption; key agility; other versatility and flexibility; potential for instruction-level parallelism.

5.3 What is power analysis?

5.3 The basic idea behind power analysis is the observation that the power consumed by a smart card at any particular time during the cryptographic operation is related to the instruction being executed and to the data being processed.

5.4 What is the difference between Rijndael and AES?

5.4 Rijndael allows for block lengths of 128, 192, or 256 bits. AES allows only a block length of 128 bits.

5.5 What is the purpose of the State array?

5.5 The State array holds the intermediate results on the 128-bit block at each stage in the processing.

5.7 Briefly describe SubBytes.

5.7 Each individual byte of **State** is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value. These row and column values serve as indexes into the S-box to select a unique 8-bit output value.

5.8 Briefly describe ShiftRows.

5.8 The first row of **State** is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the third row, a 3-byte circular left shift is performed.

5.9 How many bytes in State are affected by ShiftRows?

5.9 12 bytes.

5.10 Briefly describe MixColumns.

5.10 MixColumns operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column.

5.11 Briefly describe AddRoundKey.

5.11 The 128 bits of **State** are bitwise XORed with the 128 bits of the round key.

5.12 Briefly describe the key expansion algorithm

5.12 The AES key expansion algorithm takes as input a 4-word (16-byte) key and produces a linear array of 44 words (156 bytes). The expansion is defined by the pseudocode in Section 5.2.

5.13 What is the difference between SubBytes and SubWord?

5.13 SubBytes operates on State, with each byte mapped into a new byte using the S-box. SubWord operates on an input word, with each byte mapped into a new byte using the S-box.

5.14 What is the difference between ShiftRows and RotWord?

5.14 ShiftRows is described in the answer to Question 5.8. RotWord performs a one-byte circular left shift on a word; thus it is equivalent to the operation of ShiftRows on the second row of State.

5.15 What is the difference between the AES decryption algorithm and the equivalent inverse cipher?

5.15 For the AES decryption algorithm, the sequence of transformations for decryption differs from that for encryption, although the form of the key schedules for encryption and decryption is the same. The equivalent version has the same sequence of transformations as the encryption algorithm (with transformations replaced by their inverses). To achieve this equivalence, a change in key schedule is needed.

Chapter 6

Block Cipher Operation

Chapter 6

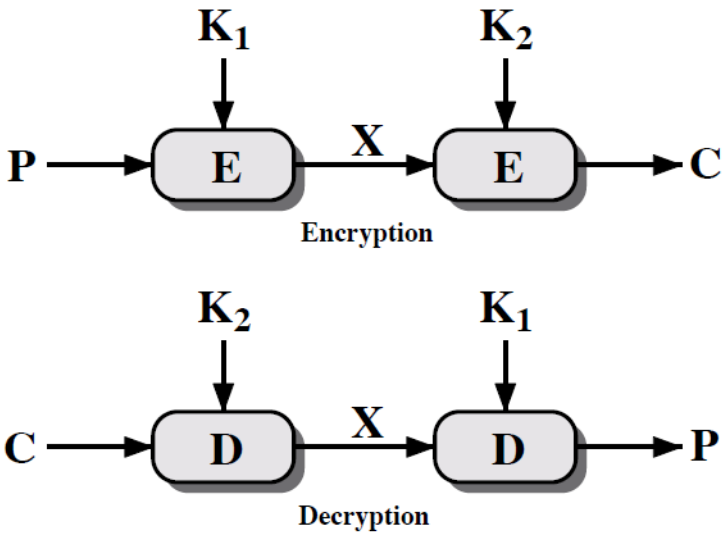
Block Cipher Operation

* تم إيجاد بديل لخوارزمية DES لأن الهجمات النظرية تستطيع كسرها .

* أول بديل لخوارزمية هو AES قبله كانت تستخدم إصدارات من DES .

* التشفير المتعدد (Multiple encryption) تقنية بها خوارزمية تشفير تستعمل في اوقات متعددة بداية يحول Plaintext إلى ciphertext ويستخدم هذا الناتج كمساهمة تطبق مرة اخرى.

* Double – DES *



(a) Double Encryption

- أسهل شكل للتشفير المتعدد له مرحلتين تشفير ومفتاحين .

- فك التشفير له مرحلتين ومفتاحين .

- طول المفتاح هو 2 * 56 = 112 bit

* قضية تخفيض عدد المراحل :

قد يكون هناك مفتاح مكافئ للمفتاحين الأخرين وهذا غير محتمل وأقت أنه مستحيل في عام ١٩٩٢ م .

- يستطيع المهاجم تشفير المفتاح K1 مع القيمة المخزنةX .
- وكذلك فك التشفير المفتاح K2 مع القيمة المخزنة X
- وعمل مقارنة ين الأزواج الناتجة والاختبارات نجد ان تاتج صحيح ويقبلان المفتاح.

* **Triple – DES with two Keys**

- استعمال ٣ تشفيرات باستخدام مفتاحين في السلسة.
- لا توجد هجمات معروفة حاليا ٠
- بالرغم من عدم وجود هجمات عملية عليه يمكن استخدام ٣ تشفيرات مع ٣ مفاتيح وتظهر هذه في تطبيقات الانترنت S/MIME and PGP

* **Mode of operation** :

تقنية لتحسين تأثير خوارزمية التشفير أو تكييف الخوارزميات مع التطبيقات ويمكن تطبيق ذلك على هيئة Stream او Block.

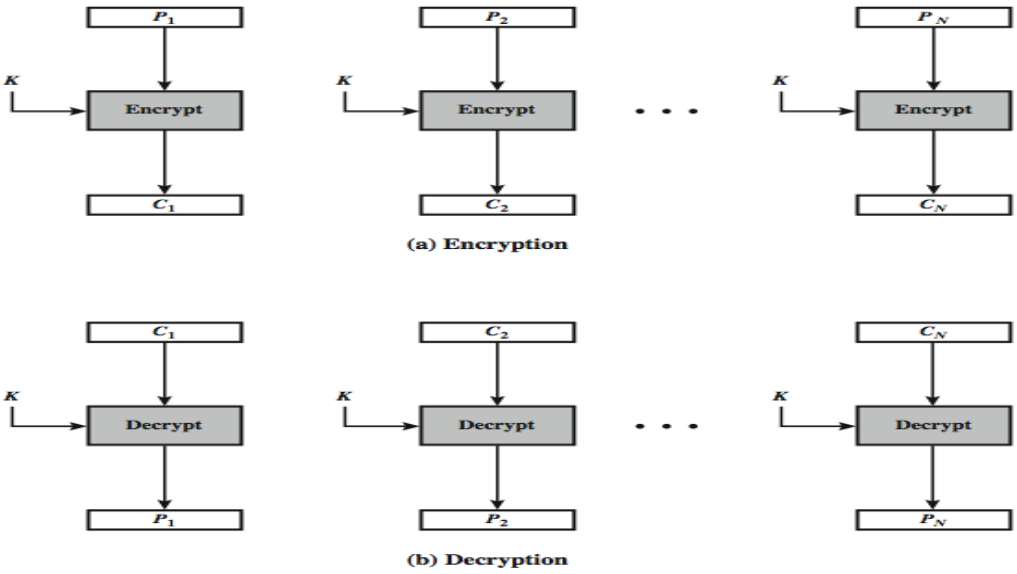
- أغلب التطبيقات تستخدم Block cipher

أولا: Block Cipher:

(١) Electronic Codebook Book (ECB) :

يستخدم في :

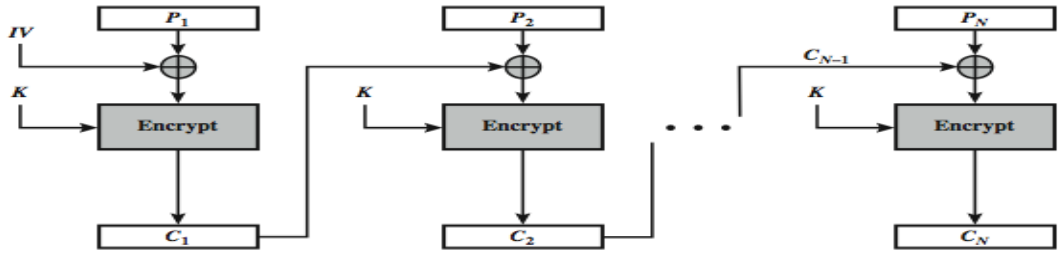
secure transmission of single values(transmit a DES or AES key securely



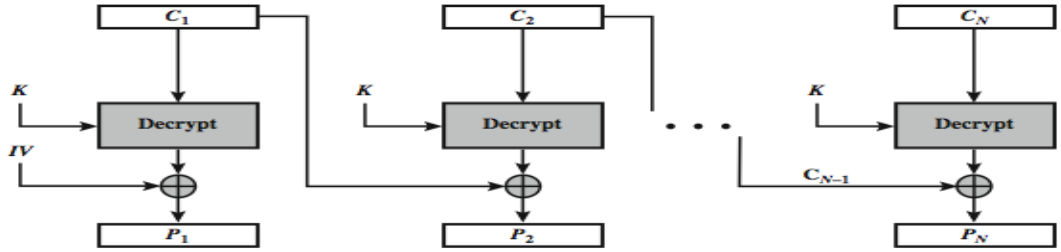
Cipher Block Chaining (CBC) (٢)

يستخدم في :

bulk data encryption, authentication



(a) Encryption

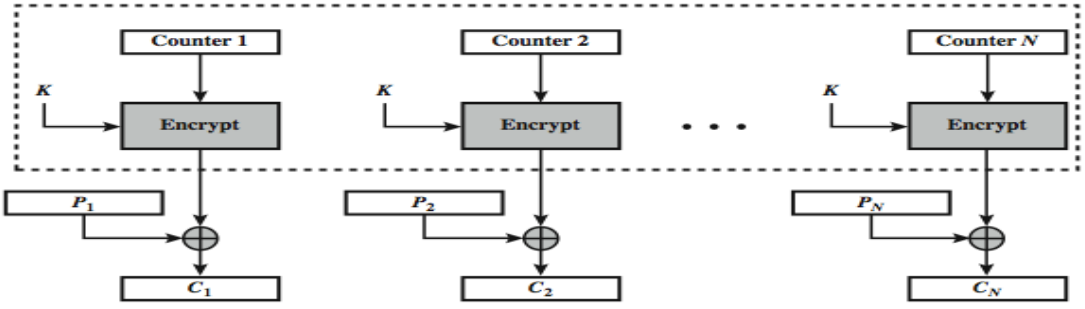


(b) Decryption

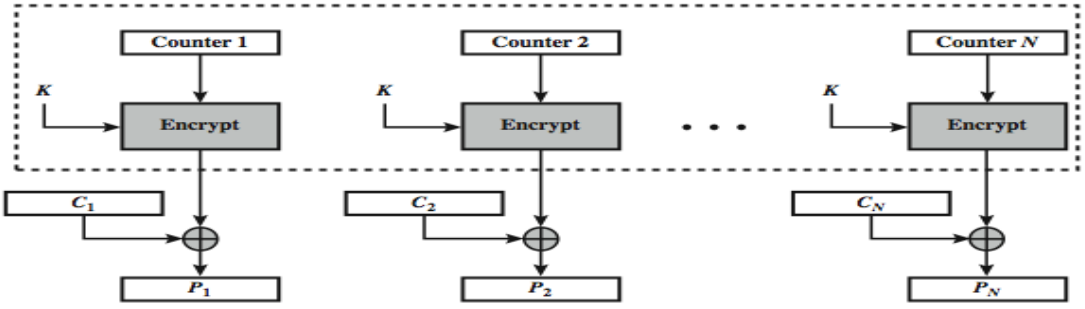
ثانيا: Stream Cipher :

Counter (CTR) (١)

يستخدم : high-speed network encryptions



(a) Encryption

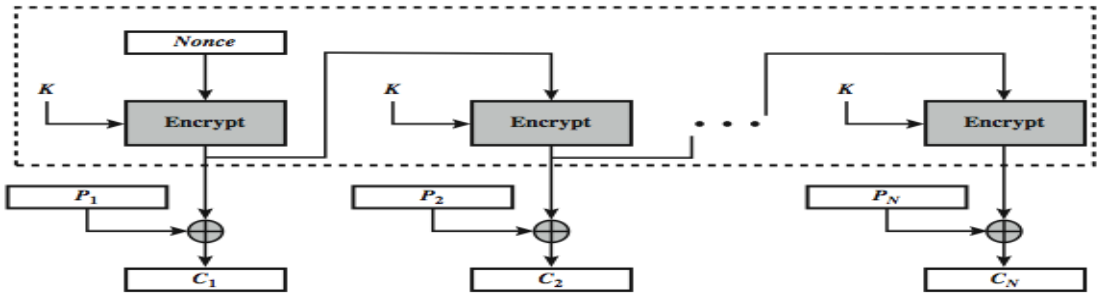


(b) Decryption

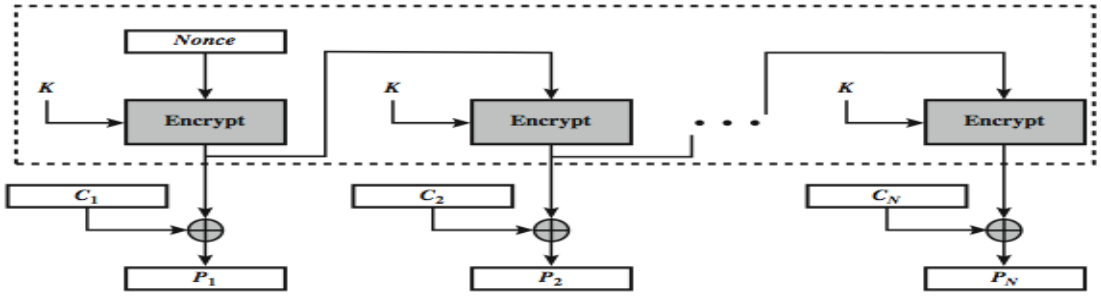
Output FeedBack (OFB) (٢)

يستخدم في :

stream encryption on noisy channels



(a) Encryption

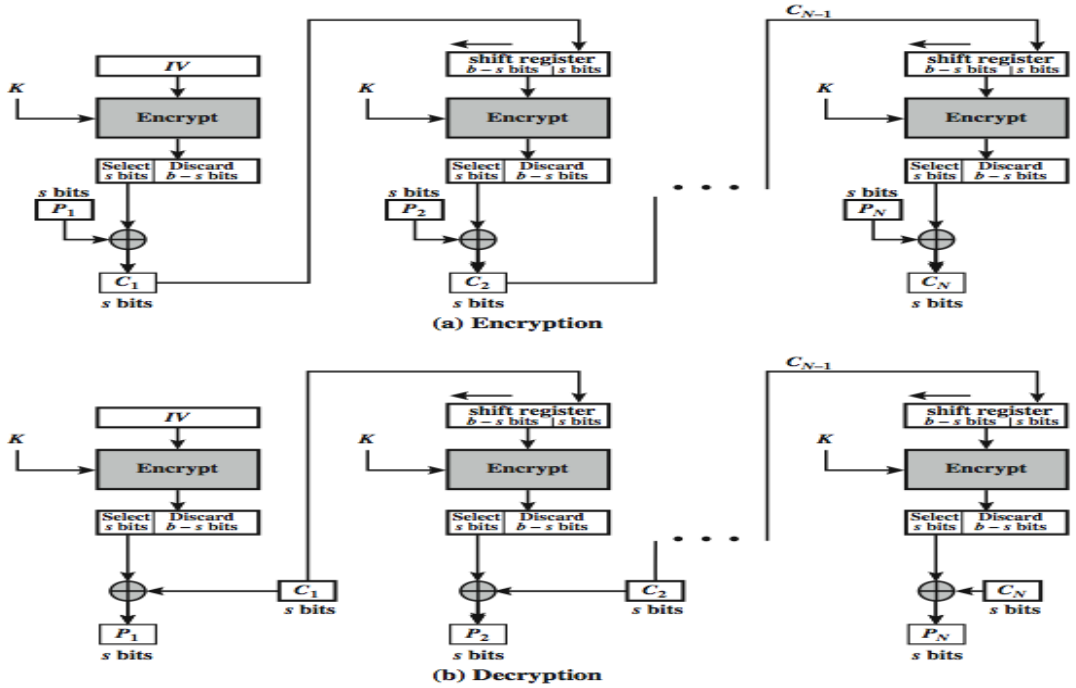


(b) Decryption

Cipher FeedBack (CFB) (٣)

يستخدم في :

stream data encryption, authentication



- لاحظ ان الأنماط الثلاثة CFB , OFB , CTR لا تحتوي على عملية Decryption في الرسم والمفتاح واحد .
- لاحظ أن IV , Counter , Nonce يجب ان تكون ذو 64bit ثم تكون plaintext بأي حجم Size or bit .

6.1 What is triple encryption?

6.1 With triple encryption, a plaintext block is encrypted by passing it through an encryption algorithm; the result is then passed through the same encryption algorithm again; the result of the second encryption is passed through the same encryption algorithm a third time. Typically, the second stage uses the decryption algorithm rather than the encryption algorithm.

6.2 What is a meet-in-the-middle attack?

6.2 This is an attack used against a double encryption algorithm and requires a known (plaintext, ciphertext) pair. In essence, the plaintext is encrypted to produce an intermediate value in the double encryption, and the ciphertext is decrypted to produce an intermediation value in the double

encryption. Table lookup techniques can be used in such a way to dramatically improve on a brute-force try of all pairs of keys.

6.3 How many keys are used in triple encryption?

6.3 Triple encryption can be used with three distinct keys for the three stages; alternatively, the same key can be used for the first and third stage.

6.4 Why is the middle portion of 3DES a decryption rather than an encryption?

6.4 There is no cryptographic significance to the use of decryption for the second stage. Its only advantage is that it allows users of 3DES to decrypt data encrypted by users of the older single DES by repeating the key.

6.5 List important design considerations for a stream cipher.

6.5 1. The encryption sequence should have a large period. **2.**The keystream should approximate the properties of a true random number stream as close as possible. **3.** To guard against brute-force attacks, the key needs to be sufficiently long. The same considerations as apply for block ciphers are valid here. Thus, with current technology, a key length of at least 128 bits is desirable.

6.6 Why is it not desirable to reuse a stream cipher key?

6.6 If two plaintexts are encrypted with the same key using a stream cipher, then cryptanalysis is often quite simple. If the two ciphertext streams are XORed together, the result is the XOR of the original plaintexts. If the plaintexts are text strings, credit card numbers, or other byte streams with known properties, then cryptanalysis may be successful.

6.7 What primitive operations are used in RC4?

6.7 The actual encryption involves only the XOR operation. Key stream generation involves the modulo operation and byte swapping.

6.8 Why do some block cipher modes of operation only use encryption while others use both encryption and decryption?

6.8 In some modes, the plaintext does not pass through the encryption function, but is XORed with the output of the encryption function. The math works out that for decryption in these cases, the encryption function must also be used.

6.5 If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode, how far does the error propagate?

6.5 Nine plaintext characters are affected. The plaintext character corresponding to the ciphertext character is obviously altered. In addition, the altered ciphertext character enters the shift register and is not removed until the next eight characters are processed.

6.6 Fill in the remainder of this table

6.6

Mode	Encrypt	Decrypt
ECB	$C_j = E(K, P_j) \quad j = 1, \ldots, N$	$P_j = D(K, C_j) j = 1, \ldots, N$
CBC	$C_1 = E(K, [P_1 \oplus IV])$ $C_j = E(K, [P_j \oplus C_{j-1}]) \quad j = 2, \ldots, N$	$P_1 = D(K, C_1) \oplus IV$ $P_j = D(K, C_j) \oplus C_{j-1} \quad j = 2, \ldots, N$
CFB	$C_1 = P_1 \oplus S_s(E[K, IV])$ $C_j = P_j \oplus S_s(E[K, C_{j-1}])$	$P_1 = C_1 \oplus S_s(E[K, IV])$ $P_j = C_j \oplus S_s(E[K, C_{j-1}])$
OFB	$C_1 = P_1 \oplus S_s(E[K, IV])$ $C_j = P_j \oplus S_s(E(K, [C_{j-1} \oplus P_{j-1}]))$	$P_1 = C_1 \oplus S_s(E[K, IV])$ $P_j = C_j \oplus S_s(E(K, [C_{j-1} \oplus P_{j-1}]))$
CTR	$C_j = P_j \oplus E[K, Counter + j - 1]$	$P_j = C_j \oplus E[K, Counter + j - 1]$

Chapter 7

PSEUDORANDOM NUMBER GENERATION AND STREAM CIPHERS

Chapter 7

PSEUDORANDOM NUMBER GENERATION AND STREAM CIPHERS

*** استخدام الأرقام العشوائية:**

- من الخوارزميات التي تستخدم الأرقام العشوائية والتي تعمل على التشفير :

١- استخدام المعرفات (Nonce) من اجل منع هجوم التكرار .

٢- توليد مفاتيح الجلسات Session key .

٣- توليد المفاتيح لخوارزمية RSA والتي تستخدم المفتاح العمومي .

*** تفرض هذه الخوارزميات مطلبين مستقلين على تسلسل الأرقام العشوائية وليس بالضرورة ان يكونا متوافقين :**

١- العشوائية . ٢- عدم القدرة على التوقع او التخمين .

*** وللحكم على خوارزمية ما بأنها عشوائية نستخدم المعيارين التاليين:**

١- التوزيع الموحد (Uniform distribution) .

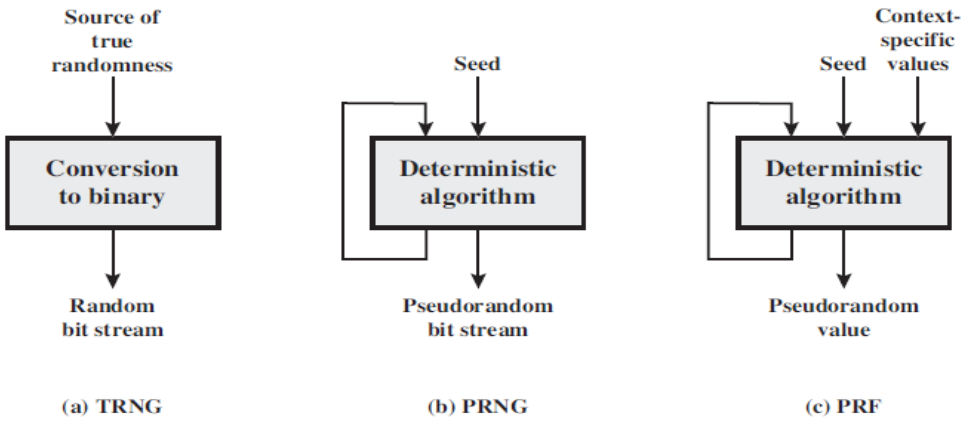
٢- الاستقلالية.

*** هناك نوعان مختلفان من PRNGs مستندة على التطبيقات :**

Pseudorandom number generator

Pseudorandom function (PRF)

*** أنواع المولدات:**



- **TRNG:** عبارة عن مصدر مسحوب من البيئة الطبيعية للحاسوب مثل أنماط توقيت ضربة المفتاح وحركات الماوس وساعة النظام.
- **متطلبات الـ PRNG :**

١- استخدام عدد من الاختبارات للتأكد من العشوائية :
Uniformity (الاتساق) - scalability (السلاسل الثانوية تكون عشوائية
Consistency : اختبار الـ output معتمد على single seed .

٢- استخدام عدد من الاختبارات للتأكد من عدم التقلب (***Unpredictability***)
- التقلب الأمامي : لا يمكن معرفة Seed من خلال معلومات معروفة .
- التقلب الخلفي : لا يمكن معرفة Seed من خلال أي قيم مولدة .

- **خصائص الـ Seed :**

١- آمن.
٢- إذا عرف يمكن معرفة وتقرير output .
٣- يجب ان يكون عشوائي او شبة عشوائي.

- **قسمت خوارزميات PRNG إلى قسمين :**

١- خوارزميات حسب الطلب : فقط توليد pseudorandom (شبه عشوائية).
٢- خوارزميات مستندة على خوارزميات تشفير .

- **وهناك ثلاث أنواع من الخوارزميات المستندة تستخدم لخلق وإنشاء الـ PRNG :**

١- Symmetric block ciphers
٢- Asymmetric ciphers
٣- Hash functions and message authentication codes .

- **وهناك نوعان أخرى للـ PRNG هي :**

١- Linear Congruential Generators
٢- Blum Blum Shub Generator

- **Linear Congruential Generators :**

$X_{n+1} = (aX_n + c) \bmod m$ m يجب ان تكون كبيرة جدا 2^{31}

ونقول عن هذه الخوارزمية ***أنها full-period*** *إذا كان تجميع القيم المولدة بين* 0 و M دون تكرار.

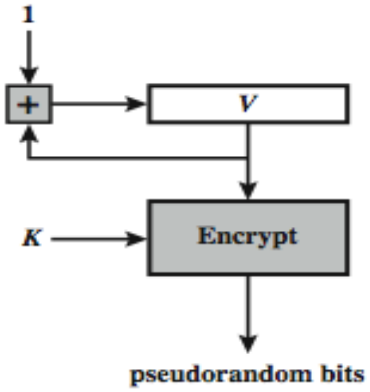
- **Blum Blum Shub Generator :**

$p = q = 3(mod\ 4)$ حيث n = P*q ونختار رقم عشوائي S

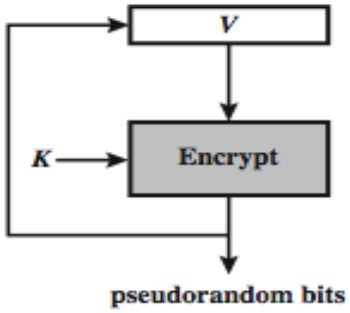
$Bi = Xi \bmod 2$, $Xi = (Xi\text{-}1)^2 \bmod n$, $X0 = s^2 \bmod n$

- **استخدام الـ block cipher كـ PRNG:**

يوجد منهجان :



(a) CTR Mode



(b) OFB Mode

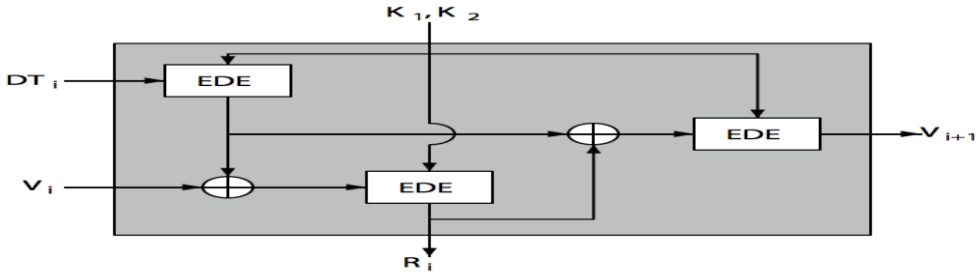
- **مولد الأرقام العشوائية ANSI X9.17:**

يعتبر أحد اقوى المولدات المتوقرة حيث يستخدم فيه Des الثلاثية للتشفير وعناصره الأساسية :

١- الدخل: دخلان شبه عشوائية أحدهما 64 خانة للتاريخ الوقت والاخر 64 قيمة Seed

٢- المفاتيح: يستخدم زوج المفاتيح طولها 56 .

٣- الخرج : يتألف من رقم عشوائي ذو 64 خانة وقيمة Seed 64 خانة

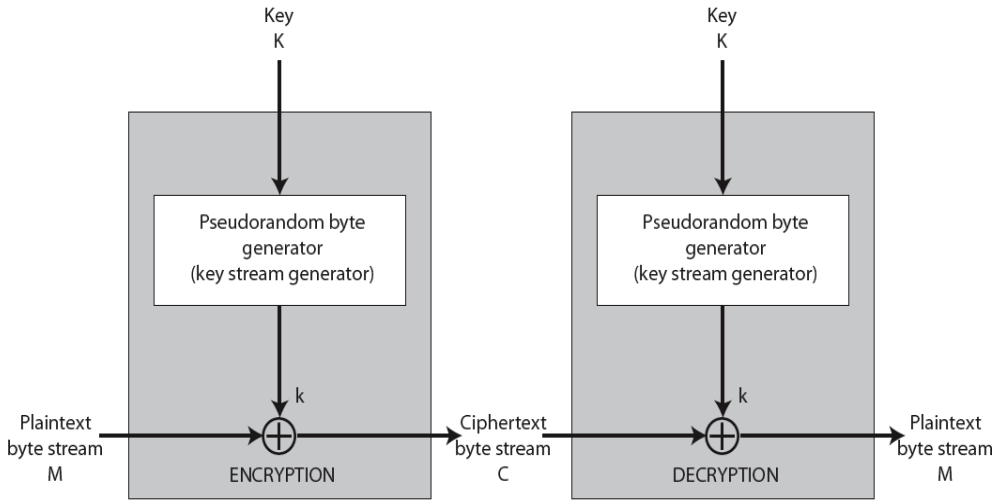


$$R_i = \mathrm{EDE}([K_1, K_2], [V_i \oplus \mathrm{EDE}([K_1, K_2], DT_i)])$$
$$V_{i+1} = \mathrm{EDE}([K_1, K_2], [R_i \oplus \mathrm{EDE}([K_1, K_2], DT_i)])$$

- **استخدام Stream cipher كـ PRGN:**

تمتلك **keystream** pseudo random مواصفاته : **لا يعاد استخدامه** + **destroy** .

$$C_i = M_i \; XOR \; StreamKey_i$$



- **هناك اعتبارات في تصميم Stream cipher كـ PRGN :**

١- فترات طويلة دون تكرار.

٢- العشوائية بشكل إحصائي.

٣- تعتمد على كبر المفتاح المستخدم.

٤- large linear complexity

- **عندما يصمم بشكل جيد يكون مثل سرية block cipher ولكنه اسرع وأبسط عادة.**
- **مقارنة بين طول المفتاح والسرعة :**

Table 7.4 Speed Comparisons of Symmetric Ciphers on a Pentium II

Cipher	Key Length	Speed (Mbps)
DES	56	9
3DES	168	3
RC2	Variable	0.9
RC4	Variable	45

*** خوارزمية RC4 :**

- يستخدم هذا النظام في المقياس (SSL/TLS) وكذلك WEP .

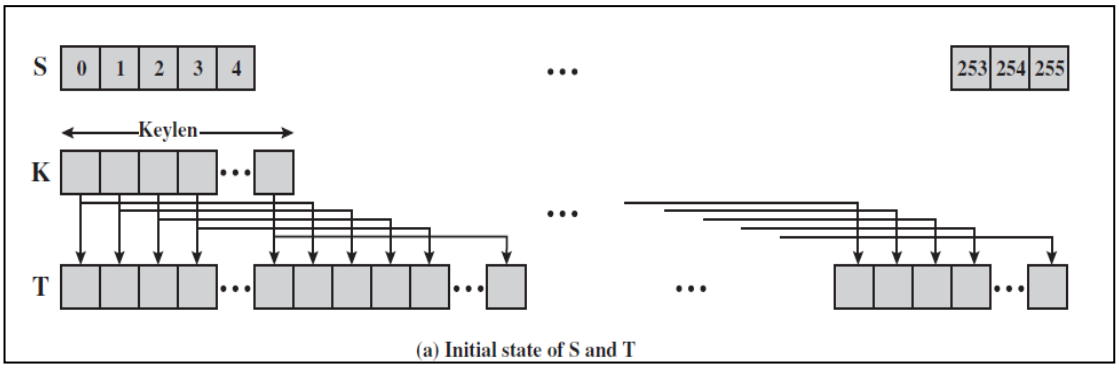
- يستخدم المفتاح ذو الطول المتغير من ١ إلى ٢٥٦ بايت (٨ ـــ ٢٠٤٨ خانة) في تهئية الشعاع (S) المؤلف من ٢٥٦ بايت يبدأ بـ 0 وينتهي بـ ٢٥٥ .

- حيث يحتوي على إعداد تغيير الأماكن لكل الأعداد.

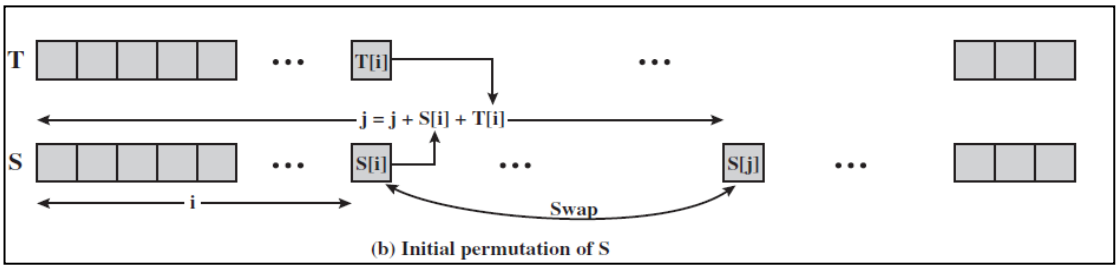
- يتم توليد Key في التشفير وفك التشفير من خلال الشعاع (S).

- العملية الوحيدة المطبقة على الشعاع هي عملية **التبديل** .

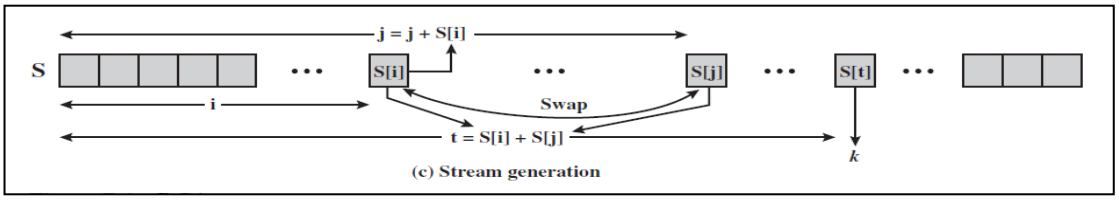
- مبدئيا يتم نقل محتويات K إلى T هو عبارة عن شعاع مؤقت



(a) Initial state of S and T



(b) Initial permutation of S



(c) Stream generation

- **ملاحظة:**
  - في عملية التشفير تطبق XOR بين القيمة K والبايت القادم من plaintext
  - في فك التشفير تطبق XOR بين القيمة K والبايت القادم من ciphertext
- **قوة خوارزمية RC4:**

لم يكن هناك أي طريقة عملية ضدها وخاصة إذا كان طول المفتاح 128 bit

- تعريف Skew (problem of bias) :

يعرف بـ uneven distribution في الاشارة حيث يكون هناك عددا من ones اكثر من zero او العكس وتم حلها باستخدام multiple sources + hash في خوارزمية RFC4086 .

- These applications mentioned above give rise to two distinct requirements for a sequence of random numbers: ***randomness*** and ***unpredictability***
- a PRNG takes as input a fixed value, called the **seed**, and produces a sequence of output bits using a deterministic algorithm.
- since RC4 is a stream cipher, must **never reuse a key**

7.1 For a user workstation in a typical business environment, list potential locations for confidentiality attacks.

7.1 LAN, dial-in communications server, Internet, wiring closet.

7.2 What is the difference between link and end-to-end encryption?

7.2 With **link encryption**, each vulnerable communications link is equipped on both ends with an encryption device. With **end-to-end encryption**, the encryption process is carried out at the two end systems. The source host or terminal encrypts the data; the data in encrypted form are then transmitted unaltered across the network to the destination terminal or host.

7.3 What types of information might be derived from a traffic analysis attack?

7.3 Identities of partners. How frequently the partners are communicating. Message pattern, message length, or quantity of messages that suggest important information is being exchanged. The events that correlate with special conversations between particular partners

7.4 What is traffic padding and what is its purpose?

7.4 Traffic padding produces ciphertext output continuously, even in the absence of plaintext. A continuous random data stream is generated. When plaintext is available, it is encrypted and transmitted. When input plaintext is not present, random data are encrypted and transmitted. This makes it impossible for an attacker to distinguish between true data flow and padding and therefore impossible to deduce the amount of traffic.

7.5 List ways in which secret keys can be distributed to two communicating parties.

7.5 For two parties A and B, key distribution can be achieved in a number of ways, as follows:

1. A can select a key and physically deliver it to B.
2. A third party can select the key and physically deliver it to A and B.
3. If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
4. If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B.

7.6 What is the difference between a session key and a master key?

7.6 A **session key** is a temporary encryption key used between two principals. A **master key** is a long-lasting key that is used between a key distribution center and a principal for the purpose of encoding the transmission of session keys. Typically, the master keys are distributed by noncryptographic means.

7.7 What is a nonce?

7.7 A nonce is a value that is used only once, such as a timestamp, a counter, or a random number; the minimum requirement is that it differs with each transaction.

7.8 What is a key distribution center?

7.8 A key distribution center is a system that is authorized to transmit temporary session keys to principals. Each session key is transmitted in encrypted form, using a master key that the key distribution center shares with the target principal.

7.9 What is the difference between statistical randomness and unpredictability?

7.9 Statistical randomness refers to a property of a sequence of numbers or letters, such that the sequence appears random and passes certain statistical tests that indicate that the sequence has the properties of randomness. If a statistically random sequence is generated by an algorithm, then the sequence is predictable by anyone knowing the algorithm and the starting point of the sequence. An unpredictable sequence is one in which knowledge of the sequence generation method is insufficient to determine the sequence.

Chapter 9

Public-Key Cryptography

Chapter 9

Public-Key Cryptography

*** كانت معظم الخوارزميات السابقة ونظام Desتعتمد على :**

تبديل الحروف وتبديل المواقع ***permutation*** and ***substitution*** .

_ اعتمدت خوارزمية التشفير العمومي على التوابع الرياضية ***mathematical*** .

- وهي نوع تشفير (غير متماثل) يستخدم مفتاحين منفصلين.

*** حقائق خاطئة حول التشفير العمومي :**

١- يعتبر أكثر امانا من التشفير المتماثل وهذا خطأ إذ يعتمد على طول وحجم المفتاح.

٢- قيل ان التشفير المتماثل أصبح بلا فائدة وهذا خطأ .

*** حقائق خاصة صحيحة:**

- حدود استخدام نظام التشفير العمومي : تطبيقات إدارة المفاتيح والتوقيع الرقمي.

*** تعتمد خوارزميات التشفير بالمفتاح العمومي علي :**

- وجود مفتاح لعملية التشفير ومفتاح آخر لعلمية فك التشفير .

*** ملاحظة: من غير الممكن حسابيا تحديد مفتاح التشفير بمجرد معرفة خوارزمية التشفير.**

*** أضافة خوارزمية التشفير RSA مميزات اخرى :**

١- من الممكن استخدام أي من المفاتيح لعملية التشفير والاخر لعملية فك التشفير.

٢- plaintext : عبارة عن الرسالة أو المعطيات .

٣- public and private key: يستخدم أحدها للتشفير والأخر لفك التشفير.

٤- ciphertext: عبارة عن رسالة الخرج وتعتمد على key and plaintext .

حيث استخدام two key with one plintext الناتج two different ciphertext .

- مقارنة بين التشفير المتماثل والتشفير غير المتماثل :

التشفير المتماثل	التشفير الغير متماثل
يلزم للعمل : ١- نفس الخوارزمية ونفس المفتاح للتشفير وفك التشفير ٢- يجب ان يشترك المرسل والمستقبل الخوارزمية والمفتاح	يلزم للعمل : ١- خوارزمية واحدة للتشفير وفك التشفير مع زوج مفاتيح للتشفير والاخر لفك التشفي ٢- خوارزمية واحدة للتشفير وفك التشفير مع زوج مفاتيح للتشفير والاخر لفك التشفير
يلزم للتأمين: ١- يبقى المفتاح سريا ٢- من غير الممكن فك التشفير اذا توفرت معلومات اخرى . ٣- يجب ان لا تكون معرفة الخوارزمية + نموذجا من ciphertext سببا لتحديد Key	يلزم للتأمين: ١- يبقى أحد المفتاحين سريا. ٢- من غير العملي فك التشفير إذا لم تتوفر معلومات أخرى. ٣- يجب ان لا يكون معرفة الخوارزمية + أحد ciphertext + Key سببا لتحديد الـ key الاخر

*** حالات التشفير العمومي :**

١- التحقق من الهوية: التشفير باستخدام المفتاح الخاص private للمرسل ويمكن التأكد من المصدر والمحتوى ولكن غير آمنه حيث يمكن لأي شخص آخر فك التشفير باستخدام المفتاح العام public للمرسل .

٢- التحقق والسرية معا: عن طريق استخدام المضاعف حيث :
تشفير الرسالة باستخدام المفتاح الخاص للمرسل (التوقيع الرقمي = التحقق).
تشفير الرسالة مرة أخرى باستخدام المفتاح العام للمستقبل.
ويتم فك التشفير مرة أخرى باستخدام المفتاح الخاص الموافق الموجه للمستقبل فقط .

*** متطلبات نظام التشفير والمفتاح العام :**

١- من السهل حسابيا على المرسل A معرفة المفتاح العمومي للطرف B والرسالة المراد إرسالها وتوليد الرسالة المشفرة.

٢- من السهل حسابيا على الطرف B توليد زوج من المفاتيح public و private .

٣- من السهل حسابيا على الطرف B فك التشفير باستخدام المفتاح الخاص.

٤- من المستحيل معرفة المفتاح الخاص من قبل المهاجم من خلال معرفة المفتاح العمومي.

٥- عملية استرجاع الرسالة الأصلية بمجرد معرفة المفتاح العام و الرسالة المشفرة غير مجدية حسابيا .

*** إضافة إلى ذلك يوجد ما يسمى بالتابع (F) مصيدة ذو اتجاه واحد ونعني به :**

هو الذي يحول قيم الرسالة إلى قيم أخرى بحيث تكون تلك القيم قيمة **عكس وحيدة** مع وجود شرط أن يكون **حساب التابع سهلا** بينما يكون **حساب العكس صعبا او غير مجدي** . باختصار هو عالة من التوابع العكوسة.

* تحليل التشفير بالمفتاح العمومي :

١- Brute force : يعتبر عرضة لهذا الهجوم ويمكن استخدام المفاتيح الطويلة مع الأخذ بعين الاعتبار التابع ، حيث أن استخدام المفتاح العمومي كبير الحجم يجعل الهجوم غير عملي ولكن يؤثر في سرعة التشفير وفك التشفير وتكون بطيئة في الاستخدامات العامة **لهذا هي محصورة في إدارة المفاتيح والتوقيع الرقمي** .

٢- الهجوم بإيجاد طريقة لحساب المفتاح الخاص انطلاقا من معرفة المفتاح العام (**لم تثبت رياضيا عدم فعالة هذه الطريقة على أي من الخوارزميات**) .

٤- هجوم الرسالة المحتملة: لدينا رسالة مؤلفة من مفتاح DES ذو56 يمكن للمتعدي تشفير المفاتيح المحتملة باستخدام المفتاح العام ويمكن مطابقة الرسالة مع أحد المفاتيح ليحصل على كسر التشفير ويمكن مقاومته (**بإضافة الخانات العشوائية للرسالة Plaintext)** .

*** خوارزمية RSA :**

هي عبارة عن نظام تشفير block دخله plaintext وخرجه ciphertext وهو مكون من أرقام صريحة تتراوح بين 0 و n حيث n قيمة ما لعدد .

الحجم النموذجي للعدد n هو 1024 خانة وتعني 309 خانة عشرية .

*** لحساب Key SETYP في RSA :**

١- نختار p,q عددين أولين

قوانين الحل : $n= p*q$ $Øn = (p-1)(q-1)$

$d= (p-1)(q-1)(e+1) / e$

$ku= \{e,n\}$ $kr= \{d,n\}$

التشفير $C= M^e \bmod n$

فك التشفير $M= C^d \bmod n$

1. Select primes: **p=17 & q=11**
2. Calculate **n = pq =17 x 11=187**
3. Calculate **ø(n)=(p–1)(q-1)=16x10=160**

4. Select **e: gcd(e,160)=1; choose e=7**
5. Determine **d: de=1 mod 160 and d < 160** Value is **d=23 since 23x7=161**
6. Publish public key **PU={7,187}**
7. Keep secret private key **PR={23,187}**

M = 88 (nb. 88<187)

$C = 88^7 \bmod 187 = 11$

$M = 11^{23} \bmod 187 = 88$

وسيأتي في نهاية هذا الفصل تمارين على هذا التطبيق

*** هناك عدة طرق لمهاجمة خوارزمية RSA:**

١- الهجوم الأعمى : يتضمن تجريب كل المفاتيح الحل (زيادة طول المفاتيح) .

٢- الهجوم الرياضي: عن طريق تحليل ناتج ضرب إلى عددين أولين).

٤- الهجوم الزمني: يعتمد على زمن تنفيذ خوارزمية فك التشفير ٠

*** يمكن تعريف ثلاث طرق الهجوم الرياضي :**

١- تحليل n إلى عاملين أولين . ٢- تحديد n مباشرة دون ايجاد عاملين p,q

٣- تحديد d مباشرة.

* يعتبر الهجوم الزمني من الهجوم المباغت لسببين:

١- يأتي من مكان غيرمتوقع كليا. ٢- هجوم على النص المشفر فقط .

* يعتبر الهجوم الزمني من التهديدات الجادة ولكن يوجد بعض المضادات الحلول البسيطة

١- زمن ثابت للرفع إلى أس content expansion time

٢- تأخير عشوائي. Random delay

٣- التعميم : ضرب النص المشفر برقم عشوائي قبل رفعه إلى أس Blinding

public-key algorithms are based on ***mathematical*** functions rather than on ***substitution*** and ***permutation***.

Complements **rather than** replaces private key crypto.

A **public-key**, which may be known by anybody, and can be used to **encrypt messages**, and **verify signatures**

A related **private-key**, known only to the recipient, used to **decrypt messages**, and **sign** (create) **signatures**

- Like symmetric encryption, a public-key encryption scheme is vulnerable to a ***brute-force attack***.
- Thus, the key size must be ***large*** enough to make brute-force attack impractical but small enough for ***practical*** encryption and decryption.
- In practice, the ***key sizes*** that have been proposed do make brute-force attack ***impractical*** but result in encryption/decryption ***speeds*** that are ***too slow*** for general purpose use.
- Instead, as was mentioned earlier, public-key encryption is currently confined to ***key management*** and ***signature*** applications.

Another form of attack is to find some way to compute the ***private*** key given the ***public*** key

9.1 What are the principal elements of a public-key cryptosystem?

- Plaintext
- . Encryption algorithm
- Public and private keys
- Ciphertext
- . Decryption algorithm

9.2 What are the roles of the public and private key?

9.2 A user's private key is kept private and known only to the user. The user's public key is made available to others to use. The private key can be used to encrypt a signature that can be verified by anyone with the public key. Or the public key can be used to encrypt information that can only be decrypted by the possessor of the private key.

9.3 What are three broad categories of applications of public-key cryptosystems

- Encryption/decryption:
- . Digital signature
- . Key exchange

9.5 What is a one-way function?

9.5 A **one-way function** is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy whereas the calculation of the inverse is infeasible:

9.6 What is a trapdoor one-way function?

9.6 A **trap-door one-way function** is easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known. With the additional information the inverse can be calculated in polynomial time.

9.2 Perform encryption and decryption using the RSA algorithm, as in Figure 9.6, for the following:

1. p = 3; q = 11, e = 7; M = 5

2. **p = 5; q = 11, e = 3; M = 9**

3. **p = 7; q = 11, e = 17; M = 8**

4. **p = 11; q = 13, e = 11; M = 7**

5. **p = 17; q = 31, e = 7; M = 2. Hint: Decryption is not as hard as you think; use some finesse.**

9.2 **a.** $n = 33$; $\phi(n) = 20$; $d = 3$; C = 26.

b. $n = 55$; $\phi(n) = 40$; $d = 27$; C = 14.

c. $n = 77$; $\phi(n) = 60$; $d = 53$; C = 57.

d. $n = 143$; $\phi(n) = 120$; $d = 11$; C = 106.

e. $n = 527$; $\phi(n) = 480$; $d = 343$; C = 128. For decryption, we have

$$128^{343} \bmod 527 = 128^{256} \times 128^{64} \times 128^{16} \times 128^{4} \times 128^{2} \times 128^{1} \bmod 527$$

$$= 35 \times 256 \times 35 \times 101 \times 47 \times 128 = 2 \bmod 527$$

$$= 2 \bmod 257$$

Chapter 10

Other Public Key Cryptosystems

Chapter 10
Other Public Key Cryptosystems

*** خوارزمية Diffie-Hellman :**

- **فكرة الخوارزمية :**

تعتبر هذه الخوارزمية الأولى من نوعها في موضوع تبديل المفاتيح حيث تسمح لشخصين من تبادل بيانات حساسة دون أن يفهمها الطرف الثالث المتنصت حتى لو حصل على نسخة منها.

تعتمد على إنشاء مفتاح سري مشترك يمكن استخدامه فيما بعد لتشفير المحادثات باستخدام خوارزمية مفتاح متماثل.

- **البروتوكول(طريقة العمل) :**

ليكن B , n عددان صحيحان حيث يكونان أوليان فيما بينهما.

سريا يختار طرف أول عددا صحيحا عشوائيا نسميه α

$A= B^{a} \% n$ يرسل علنا للطرف الثاني

سريا يختار طرف أول عددا صحيحا عشوائيا نسميه g

$G= B^{g} \% n$ يرسل علنا للطرف الثاني

وحقيقة العددان أنها متساويان $B^{a\ g} \% n$ حيث لا يعرفه أحد غيرهما ويمكن استخدامه كمفتاح.

- **كيف لا يمكن للطرف الثالث معرفة أو التنصت :**

حيث ان العددان لا يدخلان ضمن المعلومات المتبادلة علنا والمعلومات التي يمكن للمتنصت الحصول عليها هي G,n,G,A ولتحديد α انطلاقا من A يجب تخطي عقبة discrete algorithm التي يستحيل كسرها عمليا حتى يومنا هذا.

- **عندما يرسل الطرف الأول رسالة يتم تشفيرها اما بالمفتاح الخاص به او المفتاح العام التابع للطرف الثاني ويتم إرسال توقيع المرسل.**
- **مقارنة الـ Hash المرسل مع الـ Hash المستقبل للتأكد من سلامة البيانات من التحريف والتزوير.**

- **حساب primitive root :**

N	G(n) primitive root
2	
3	**2**
4	**3**
5	**2,3**
6	**5**
7	**3,5**
9	**2,5**
10	**3,7**
11	**2,6,7,8**
13	**2,6,7,11**

10.1 What are two different uses of public-key cryptography related to key distribution?

10.1 **1.** The distribution of public keys. **2.** The use of public-key encryption to distribute secret keys

10.2 List four general categories of schemes for the distribution of public keys.

10.2 Public announcement. Publicly available directory. Public-key authority. Public-key certificates

10.3 What are the essential ingredients of a public-key directory?

10.3 **1.** The authority maintains a directory with a {name, public key} entry for each participant. **2.** Each participant registers a public key with the directory authority. Registration would have to be in person or by some form of secure authenticated communication. **3.** A participant may replace the existing key with a new one at any time, either because of the desire to replace a public key that has already been used for a large amount of data, or because the corresponding private key has been compromised in some way. **4.** Periodically, the authority publishes the entire directory or updates to the directory. For example, a hard-copy version much like a telephone book could be published, or updates could be listed in a widely circulated newspaper. **5.** Participants could also

access the directory electronically. For this purpose, secure, authenticated communication from the authority to the participant is mandatory.

10.4 What is a public-key certificate?

10.4 A public-key certificate contains a public key and other information, is created by a certificate authority, and is given to the participant with the matching private key. A participant conveys its key information to another by transmitting its certificate. Other participants can verify that the certificate was created by the authority.

10.5 What are the requirements for the use of a public-key certificate scheme?

10.5 **1.** Any participant can read a certificate to determine the name and public key of the certificate's owner. **2.** Any participant can verify that the certificate originated from the certificate authority and is not counterfeit. **3.** Only the certificate authority can create and update certificates. **4.** Any participant can verify the currency of the certificate.

10.1 Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root a = 7.

a. If user A has private key XA = 5, what is A's public key YA?

b. If user B has private key XB = 12, what is B's public key YB?

c. What is the shared secret key?

10.1 a. $Y_A = 7^5 \bmod 71 = 51$

b. $Y_B = 7^{12} \bmod 71 = 4$

c. $K = 4^5 \bmod 71 = 30$

10.2 Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root a = 2.

a. Show that 2 is a primitive root of 11.

b. If user A has public key Y

A = 9, what is A's private key XA?

c. If user B has public key Y

B = 3, what is the shared secret key K, shared with A?

10.2 a. $\varphi(11) = 10$

$2^{10} = 1024 = 1 \bmod 11$

If you check 2^n for $n < 10$, you will find that none of the values is 1 mod 11.

b. 6, because $2^6 \bmod 11 = 9$

c. $K = 3^6 \bmod 11 = 3$

10.6 Briefly explain Diffie-Hellman key exchange.

10.6 Two parties each create a public-key, private-key pair and communicate the public key to the other party. The keys are designed in such a way that both sides can calculate the same unique secret key based on each side's private key and the other side's public key.

Chapter 11

Cryptographic Hash Functions

Chapter 11

Cryptographic Hash Functions

*** تمهيد :**

أنواع التشفير:

١- التشفير باتجاهين: عندما يكون بحاجة إلى استعادة المعلومات التي قمنا بتشفيرها إعادتها للنص الاصلي.
٢- التشفير باتجاه واحد: عملية يتم بموجبها تشفير المعلومات باستخدام خوارزمية التشفير ولكن لا يوجد خوارزمية لفك التشفير للرسالة .
ويتم في هذا النوع من التشفير (التشفير باتجاه واحد) استخدام دالة الاختزال Hash function.

- **Hash Functions** : هي عبارة عن عملية تحويل الرسالة او البيانات إلى قيمة عددية ودالة الـ Hash إما :
  - أحادية الاتجاه: لا تسمح للرسالة بالعودة إلى قيمتها الأصلية وهي الاغلب في الاستخدام وتشبه ما يسمى بالبصمة.
  - مزدوجة الاتجاه: يسمح للرسالة بأن تعاد بناءها.
- **أنواع دوال الاختزال Hash Functions :**
  ١- SHA (Secure digest algorithm).
  ٢- سلسلة تلخيص الرسالة MD (Message digest) .
  Message: الرسالة المشفرة.
  digest : الـ hash التشفيري .
- **هذا النوع من الخوارزميات لا يحتاج إلى مفتاح تشفير لأنه لا يستخدم لتشفير النصوص وإنما للتأكد من أن محتوى الرسالة موثوق ولم يتم التعديل عليه .**
- هناك أربع صفات رئيسة للـ Hash :
  ١- يمكن حساب الـ digest بسهولة .
  ٢- من غير الممكن توليد الرسالة عن طريق digestمعطاة .
  ٣- من غير الممكن تغيير رسالة دون أن تتغير الـ digest.
  ٤- من غير الممكن توليد رسالتين لها نفس الـ Digest.
- مفهومين مهمين في hash:
  - One- way: من غير الممكن الحصول على مدخل من خلال مخرج .
  - Collision resistant : من غير الممكن أن يكون هناك دخلين لها نفس المخرج.
- **خوارزمية التشفير MD5 (Message digest) (Message Authentication):**
  - هي دالة تشفير يدخل عليها النص بأي طول ويتم تجزئته إلى نصوص قصيرة بحجم 512bit مثلا .
  - تنتج نص مشفر بطول 128bit يمثل بـ 32 hexadecimal

- ناتج العملية صعب الرجوع منه إلى النص الأصلي.
- مثال:

النص الأصلي : hallo my host

نتيجة الـ MD5 : tggdtsgbbdseaaaaa2115nb

- **تستخدم هذه الطريقة عادة في :**

١- اثبات صحة الملفات من التعديل.

٢- هويات المستخدمين.

٣- التوقيع الرقمي.

- يمر النص في خوارزمية MD5 بست مراحل يمكن اختصارها في الأربعة التالية:

١- تجزئة النص لأجزاء بحجم 512 bit

٢- تكون الكلمة الانشائية لكل جزء بحجم 512bit يتم تجزئته إلى 16word كل word بحجم 32bit .

٣- ثم تمر في أربع دورات كل دورة لها معادلة منطقية خاصة.

٤- ينتج نص غير مفهوم بطول 128bit .

- **تطبيقات خوارزمية الـMD5 :**

١- اثبات صحة الملفات (file integrity) :

عندما نريد مشاركة ملف قراءة دون تعديل نستخدم هذه الدالة.

٢- التواقيع الرقمية (Digital signature) :

يستخدم لإثبات هوية المرسل أو كاتب الملف ويضمن لنا عدم تعديل الملف من قبل متجسس ، يمكن ارسال الرسالة مشفرة أو دون تشفير وطريقة عملها :

- يقوم المرسل بحساب MD5 لرسالة وتشفيره بواسطة المفتاح الخاص .
- يقوم المستقبل بفك التشفير بواسطة المفتاح العام وحساب MD5.
- ويقوم بعمل مقارنة للتأكد من صلاحية الرسالة.

٣- كلمة المرور (Password) :

حينما تضع كلمة المرور على جهاز ليس عليك سوى تخزين القيمة الناتجة من MD5 لكلمة المرور ، وعند الدخول يأخذ قيمة الـ MD5 المدخلة ويقارنها مع القيمة المحفوظة وسوف تكون هناك ثلاث محاولات للإدخال.

- **كسر خوارزمية التشفير MD5 :**

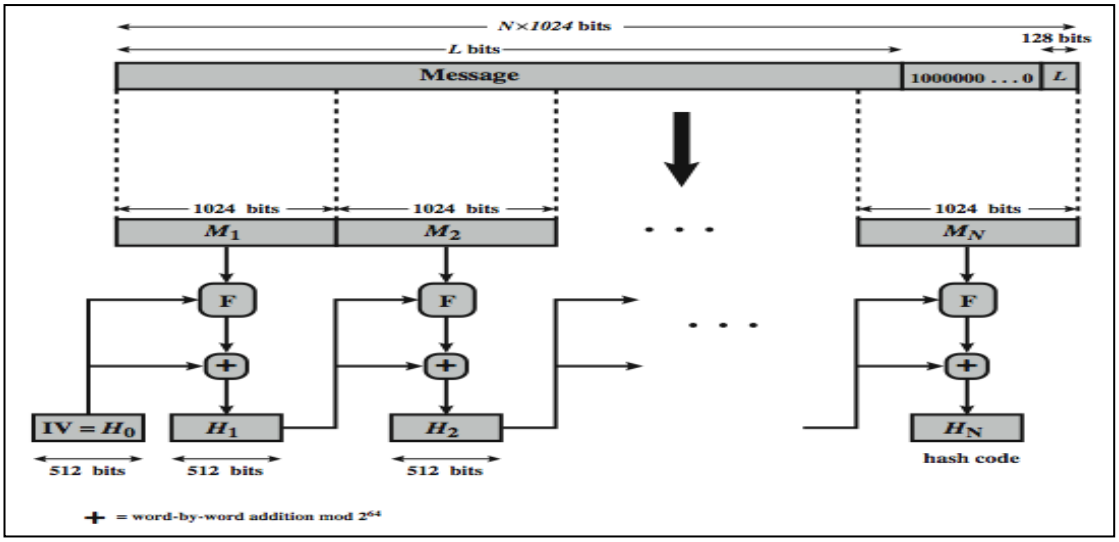
من الصعب جدا كسر هذه الخوارزمية ولكن أكثر الطرق لمحاولة الكسر هي:

١- الهجوم الأعمى : تستخدم في فك تشفير كلمات المرور وتعتمد على جمع عدد من الكلمات المتوقعة وتشفيرها بـ (MD5) ومقارنتها مع الـ(MD5) الأصلي.

٢- جمع عدد كبير من النصوص بالإضافة للـ(MD5) الخاصة في ملف يسمى Raindow table .

٣- بعض المواقع على الانترنت تقوم بحساب MD5 لنص معين .

- **Birthday attack** : هي الحصول على المعلومات بطريقة الهندسة العكسية فمثلا
  $ * $ = 50 و 25* $= 50
  ففي المثال الأول يصعب الحصول على إجابة بمرور الوقت . على عكس المثال الثاني وهو وجود رقم واحد نصل إليه وهو ما يسمى بهجوم عيد الميلاد.
- **خوارزمية (SHA) :**
  تعتمد بشكل كبير على عمل Rone Rivest في خوارزمية MD5 حيث تعمل هذه الخوارزمية على أربعة مراحل إلا أنه هذه المراحل اكثر تعقيدا حيث خرج الرسالة الملخص هو 160bit والذي هو عبارة عن سلسلة من القيم التي يتم انتقالها من مرحلة إلى أخرى والتي هي بطول 160bit ايضا .
- **خوارزمية SHA512 :**
  تأخذ كدخل الرسالة بحجم أقصى اقل من 2^{128} بت
  تنتج رسالة مشفرة بطول 512bit
  الرسالة تعالج كـ block طول كل 1024 bit block .



- **جدول مقارنات بين إصدارات SHA :**

	SHA1	SHA256	SHa224	SHA384	SHA512
Message digest size	160	256	224	384	512
Message size	$<2^{64}$	$<2^{64}$	$<2^{64}$	$<2^{128}$	$<2^{128}$
Block size	512	512	512	1024	1024
Word size	32	32	32	64	64
Number of steps	80	64	64	80	80

- When a hash function is used to provide message authentication, the hash function value is often referred to as a ***message digest*.**

11.1 What types of attacks are addressed by message authentication?

- Masquerade
- Content modification
- Sequence modification
- Timing modification

11.2 What two levels of functionality comprise a message authentication or digital signature mechanism?

11.2 At the lower level, there must be some sort of function that produces an authenticator: a value to be used to authenticate a message. This lower-level function is then used as primitive in a higher-level authentication protocol that enables a receiver to verify the authenticity of a message.

11.3 What are some approaches to producing message authentication?

11.3 Message encryption, message authentication code, hash function.

11.4 When a combination of symmetric encryption and an error control code is used for message authentication, in what order must the two functions be performed?

11.4 Error control code, then encryption.

11.5 What is a message authentication code?

11.5 An authenticator that is a cryptographic function of both the data to be authenticated and a secret key.

11.6 What is the difference between a message authentication code and a one-way hash function?

11.6 A hash function, by itself, does not provide message authentication. A secret key must be used in some fashion with the hash function to produce authentication. A MAC, by definition, uses a secret key to calculated a code used for authentication.

11.8 Is it necessary to recover the secret key in order to attack a MAC algorithm?

11.8 No. Section 11.3 outlines such attacks.

11.9 What characteristics are needed in a secure hash function?

11.9 **1.** H can be applied to a block of data of any size.

2. H produces a fixed-length output.

3. H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.

4. For any given value h, it is computationally infeasible to find x such that H(x) = h. This is sometimes referred to in the literature as the **one-way** property.

5. For any given block x, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$.

6. It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$.

11.10 What is the difference between weak and strong collision resistance?

weak collision resistance : For any given block x, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$.

strong collision resistance :It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$.

11.11 What is the role of a compression function in a hash function?

11.11 A typical hash function uses a compression function as a basic building block, and involves repeated application of the compression function.

—

Chapter 12

Message Authentication Codes(MAC)

Chapter 12
Message Authentication Codes(MAC)

- **رمز التحقق من الرسالة (MAC):**
  - إحدى الطرق المستخدمة لإثبات صحة وأصالة الرسالة وهي عملية استخدام مفتاح سري لتوليد كتلة صغيرة من البيانات تعرف بـ MAC تضاف نهاية الرسالة.
  - نفترض بان طرفي الارسال يشتركون في مفتاح سري عام هو K فمثلا عند إرسال A إلى B يتم حساب MAC كما يلي Mac = F(K,M)
  - عملية الـ Mac تشبه عملية التشفير إلا ان الفرق هو أن خوارزمية اثبات الهوية MAC لا تحتاج إلى عكسها كما تحتاجه عملية فك التشفير.
  - لذلك توجد ثلاث طرق في نظام صلاحية الاستخدام Authorization :
    ١- **DAC:** صاحب الملف له الصلاحية في اختيار السماح لمن يطلع على المحتويات مما يؤدي إلى تسرب بيانات بسبب التفريط .
    ٢- **MAC:** جهة مركزية توزع الصلاحيات يصبح العبء على جهة واحدة.
    ٣- **RBAC:** سياسات وقوانين تتحكم في توزيع الصلاحيات حل وسط بين النظامين السابقين.
- **يستخدم التشفير بالمفتاح العام في الآتي :**
  تشفير أو فك تشفير التوقيع الرقمي تبادل المفاتيح.
- **دلالات الـ function في اثبات الهوية :**
  يمكن عمل ذلك من خلال استخدام التوقيع الرقمي ويظهر مستويين كالآتي:
  ١- المستوى الأدنى: يجب ان يكون هناك نوع من الدوال تنتج **ما يثبت الهوية**.
  ٢- المستوى الاعلى: قيمة يجب استخداماها **لإثبات صحة الرسالة** .
- **توجد ثلاث دوال لإنتاج ما يسمى ب اثبات الهوية:**
  ١- Message encryption .
  ٢- MAC .
  ٣- Hash function .
- **توجد ثلاث طرق لإثبات صحة الرسالة :**
  ١- استخدام مفتاح سري :
  المرسل: يأخذ جزء من الرسالة ويشفر باستخدام الدالة الهاشية
  تأخذ الناتج ويشفر باستخدام المفتاحK .
  يدمج الناتج مع الرسالة ويرسلها للطرف الأخر
  المستقبل: يأخذ جزء من الرسالة ويفك التشفير باستخدام الدالة الهاشية.
  يأخذ الجزء المدمج ويفك التشفير باستخدام المفتاح K
  يقارن الناتجان السابقات .
  ٢- استخدام مفتاح عام:
  نفس الطريقة الأولى ولكن المفتاح المستخدم في التشفير هو المفتاح الخاص والمفتاح المستخدم لفك التشفير هو المفتاح العام.

٣- استخدام قيمة سرية:

المرسل: يأخذ قيمة سرية ويدمجها مع الرسالة ويشفرها باستخدام Hash ويرسلها

المستقبل: يرسل الرسالة مع القيمة السرية ويشفرها باستخدام Hash ثم يقارن .

لاحظ ان القيمة السرية تضاق قبل Hash وتحذف قبل Transmission .

- **: Error – Detecting – code**

تعرف بـ Frame check sequence (FCS) وتوضع لكل رسالة قبل عملية التشفير E ويوجد نوعان :

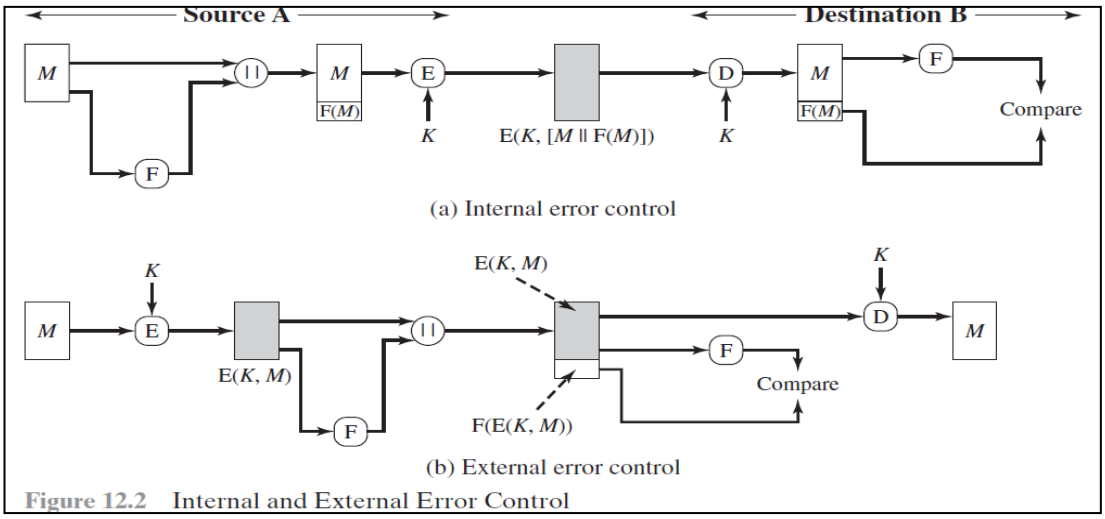


Figure 12.2 Internal and External Error Control

- **الهجوم الأعمى في خوارزمية الـ MAC:**

يعتبر اكثر صعوبة منه في دالة Hash لأنه يحتاج إلى معرفة Message tag Paris .

- **أسباب تطوير تقنية Mac إلى HMAC إلى تقنية عديمة التشفير:**

١- تعتبر برمجيات التشفير بطيئة نسبيا حتى ولو كان المراد تشفيره صغير.

٢- تكلفته المادية لا يمكن أجمالها لأنها تكلفة مرتفعة.

٣- ماديات التشفير محصصة للبيانات الكبيرة الحجم.

٤- خوارزميات التشفير قد تكون ضمن رسوم إجازة الاستخدام الواجب دفعها من قبل المستفيد.

- **خوارزمية الـHMAC (Hash + MAC) :**

هي إحدى خوارزميات MAC تقوم بإيجاد Hash ثابت من أي نص او ملف متغير حيث تعتمد على إحدى خوارزميات الـ hash(DM5. SHA) بالإضافة إلى secret key .

- **يختلف الـMAC عن Hash:**

- MAC: يستخدم secret key لإيجاد hash ثابت من أي رسالة .
- Hash: لا يستخدم secret key لإيجاد سلسلة ثابته من أي نص او ملف .

- **يمكن اختصار خوارزمية HMAC في الآتي :**

$$HMAC_K(M)= H[(K^+ XOR opad)||H[(K^+ XOR ipad)||M)]]$$

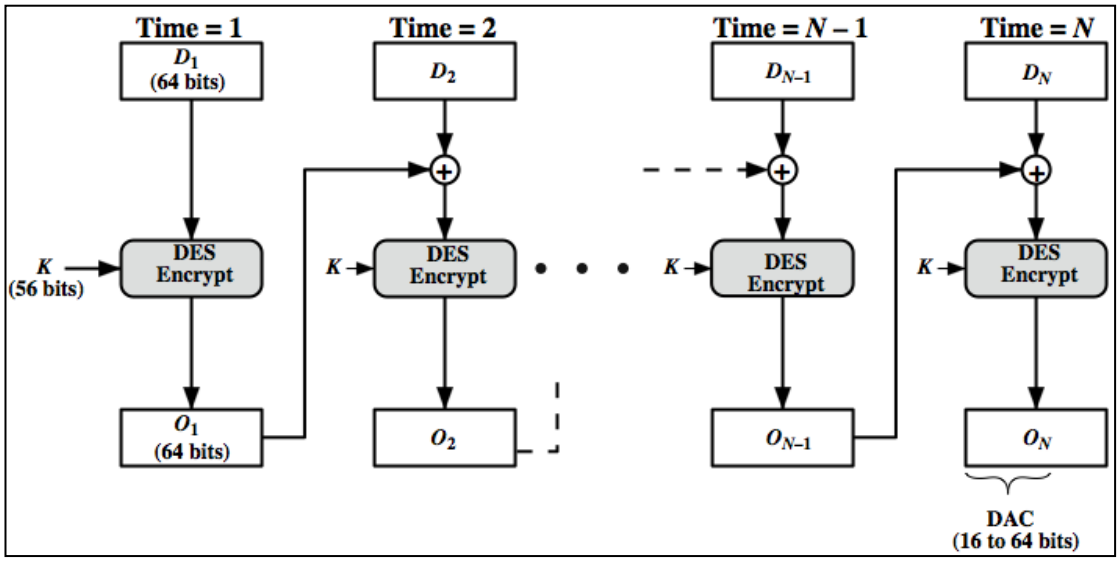
- يستخدم (ipod,opad) للحصول على مفتاحين من مفتاح واحد .

- **توجد خوارزميات Block cipher تستخدم MAC :**

١- DAA (**Data Authentication Algorithm**)

خوارزمية منتشرة تستخدم Mac تعتمد على DES – CBC

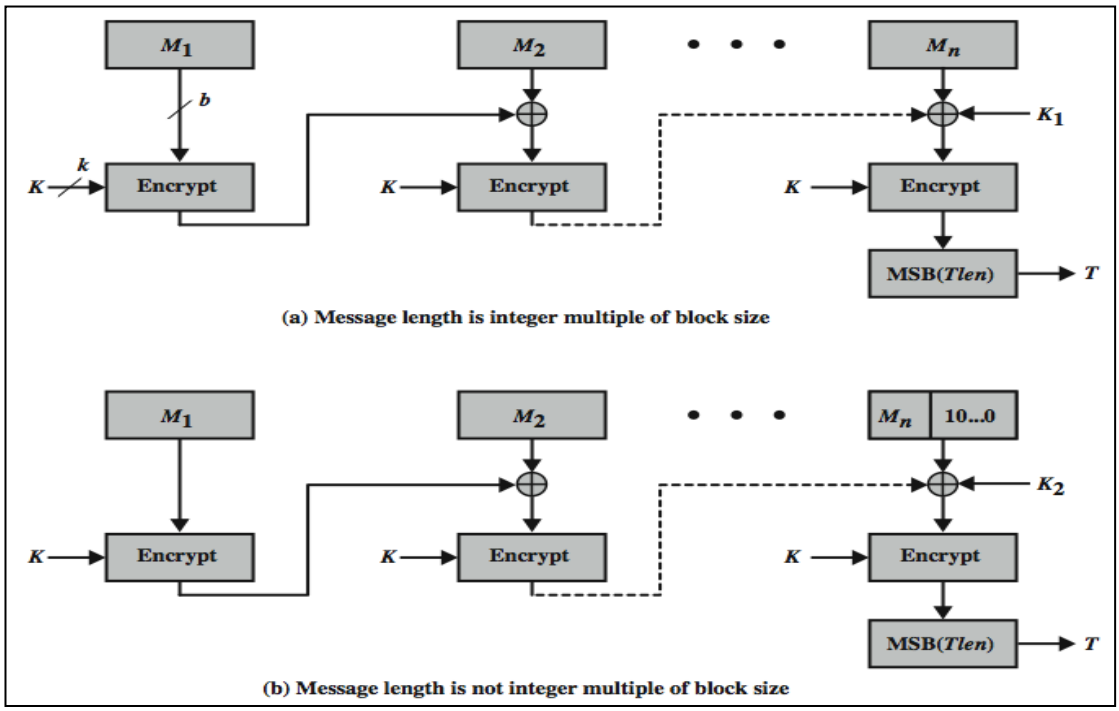
وهي ضعيفة من حيث الأمان.



٢- CMAC (**Cipher-Based Message Authentication Code**) **:**

هي خوارزمية جديدة أقوى من خوارزمية DAA .

تستخدم مفتاحين في عملية padding .

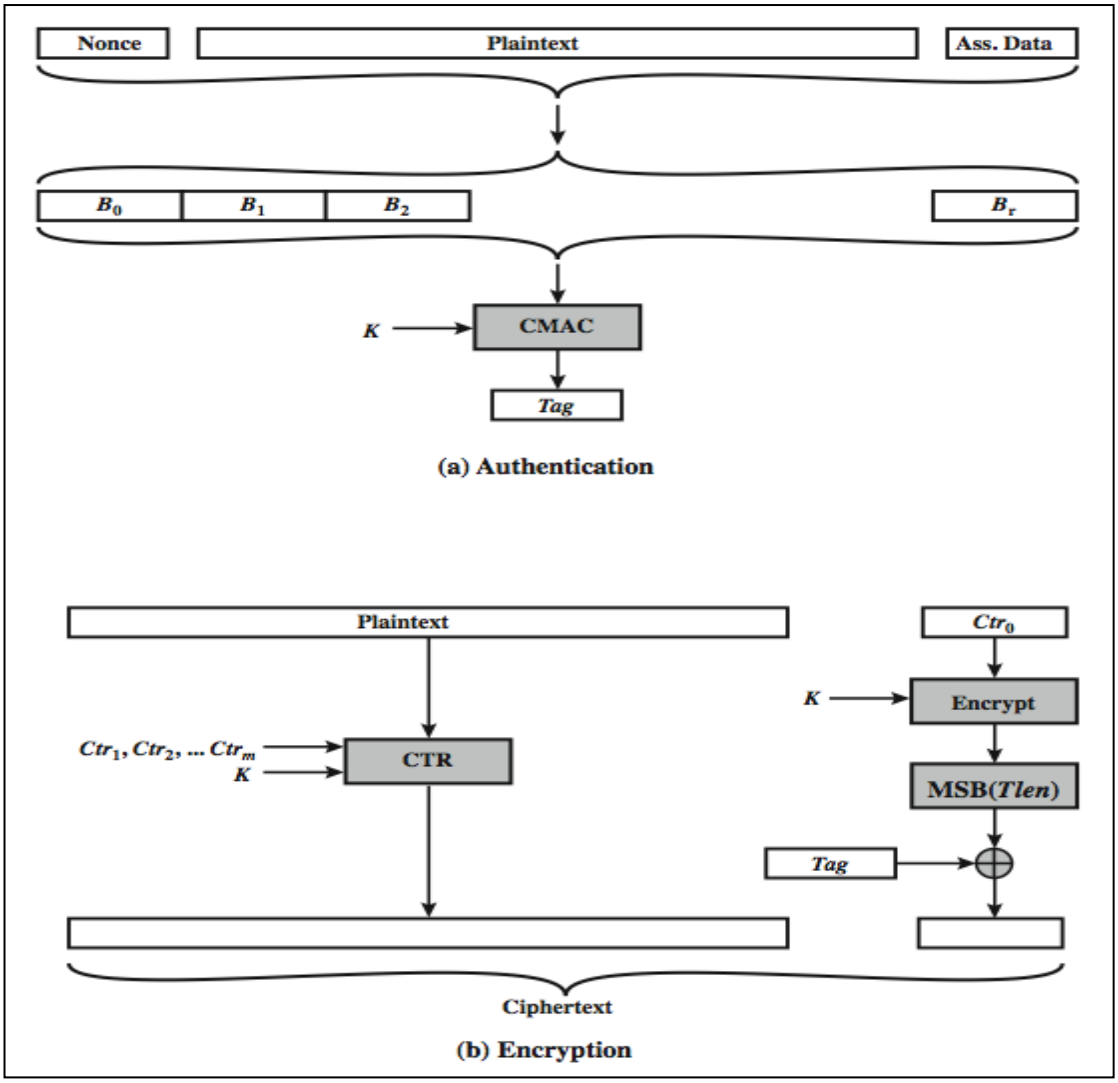


- **Approaches:**
  - **HtE**: Hash-then-encrypt: E(K, (M || H(M))

- **MtE**: MAC-then-encrypt: E(K2, (M || MAC(K1, M))
  - **e.g. SSL/TLS protocols**
- **EtM**: Encrypt-then-MAC: (C=E(K2, M), T=MAC(K1, C)
  - **E.g. IPSec protocol**
- **E&M**: Encrypt-and-MAC: (C=E(K2, M), T=MAC(K1, M)
  - to yield the pair (C,T)

- خوارزمية CCM (**Counter with Cipher Block Chaining-Message Authentication Code**) :

هي عبارة عن معيار لتقنية الـ Wifi تستخدم طريقة Eand MAC ومكونة من عدة خوارزميات CTR + CMAC + AES وهناك مفتاح واحد يستخدم في عملية تشفير الـ MAC



12.1 What is the difference between little-endian and big-endian format?

12.1 In **little-endian format**, the least significant byte of a word is in the low-address byte position. In **big-endian format**, the most significant byte of a word is in the low-address byte position.

12.2 What basic arithmetical and logical functions are used in SHA?

12.2 Addition modulo 2^{64} or 2^{32}, circular shift, primitive Boolean functions based on AND, OR, NOT, and XOR.

12.4 Why has there been an interest in developing a message authentication code derived from a cryptographic hash function as opposed to one derived from a symmetric cipher?

12.4 **1.** Cryptographic hash functions such as MD5 and SHA generally execute faster in software than symmetric block ciphers such as DES. **2.** Library code for cryptographic hash functions is widely available.

12.5 What changes in HMAC are required in order to replace one underlying hash function with another?

12.5 To replace a given hash function in an HMAC implementation, all that is required is to remove the existing hash function module and drop in the new module.

Chapter 13

Digital Signatures

Chapter 13

Digital Signatures

* التوقيع الرقمي (***Digital Signatures*** ***) :***

برهان لهوية المرسل وبرهان على سلامة البيانات المرسلة.

- يحتوي التوقيع الرقمي على:
Hash value أو has result .
يتم احتسابها عن طريق خوارزمية الـ Hash (تحول المعلومات إلى قيمة فريدة بصمة).
- **تقنية التوقيع الرقمي:**
تتم عن طريق صيغة رياضية خلق مفتاحين مختلفين لكنها متربطين رياضيا الأول مفتاح private لا يعرفه سوى المرسل والآخر public معروف لدى المستقبل او جهات موثوقة الوصول.
- **مزايا استخدام التوقيع الرقمي :**
١- التأكد من موثوقية المرسل.
٢- التأكد من موثوقية الرسائل : مقارنة نتائج الـ Hash .
٣- الالتزام: حيث استخدام المفتاح الخاص من قبل المرسل لا يسمح له بإنكار محتوى الرسالة.
- **ومن اجل التأكد من موثوقية التوقيع الرقمي ما علينا سوى معرفة :**
المفتاح العام لصاحب التوقيع وتطابقه مع المفتاح الخاص للمرسل ونستخدم طرف ثالث هو public key certificates وهي تقوم بإصدار شهادات يكون موضوعها المفتاح العام لجهة معينة تملك مقابل ذلك المفتاح الخاص(المرسل) وباختصار:
إذا اراد شخص **توقيع** رسالة ما عليه استخدام مفتاحه الخاص وسوف يستطيع جميع من لديه مفتاحه العام أن يثق من أنه كاتب الرسالة (الوثوقية) **(رسالة عامة)**
إذا اراد شخص عمل **تشفير** للرسالة لإرسالها بحرية عليه استخدام مفتاح المرسل إليه العام ولن يستطيع فتح هذه الرسالة سوى صاحب هذا المفتاح بعد فكها بالمفتاح الخاص **(رسالة خاصة)** .
- **يعتمد PGP على الثقة المتبادلة في الأصل** بين عدد من الأشخاص والذين يعرفون بعض ويريدون استخدام البريد الالكتروني للاتصال مبدأ (صديق صديقي يصبح صديقي).
- **متطلبات التوقيع الرقمي:**
١- أن يكون التوقيع سلسلة من البتات لأصل الرسالة .
٢- أن يستخدم التوقيع بعض المعلومات الفريدة عن المرسل .
٣- أن يكون إنشاء التوقيع سهلا.
٤- أن يكون التحقق سهلا .
٥- ان يكون تزوير التوقيع غير قابل للعمل حسابيا .
- **أنواع التوقيع الرقمي:**

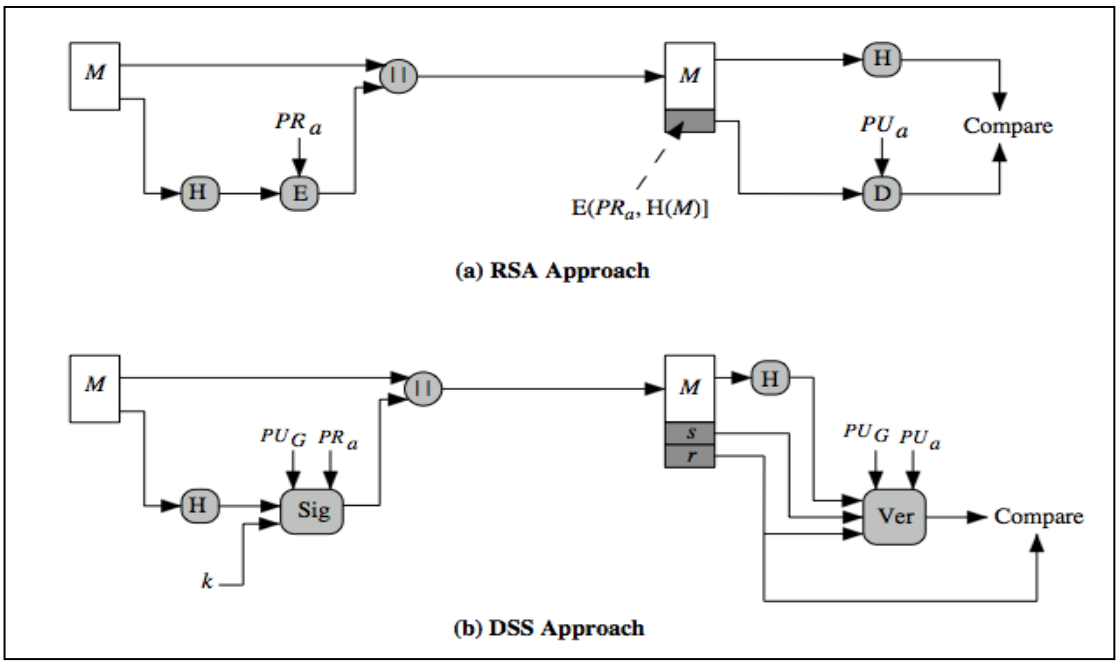
١- **التوقيع الرقمي المباشر**: يستخدم طرفي الاتصال فقط (المصدر – المستقبل) حيق نفترض أن الطرف المستقبل يعرف المفتاح العام للمصدر ويتم إنشاؤه إما بتشفير كامل للرسالة باستخدام المفتاح الخاص للمرسل او تشفير Hash للرسالة باستخدام المفتاح الخاص للمرسل .
نقطة ضعفه: اعتماد التوقيع على المفتاح الخاص للمرسل مما يمسح للمرسل بإنكار التوقيع مدعيا ضياعه.

٢- **التوقيع الرقمي المحكم**: يحل المشاكل المتعقلة بالتوقيع المباشر حيث تذهب كل رسالة موقعة إلى محكم موثوق أولا يقوم بإخضاعها لعدد من الاختبارات لفحص محتواها وأصلها ويؤرخها ويرسلها إلى وجهتها الأمر الذي يمنع المرسل من إنكارها.

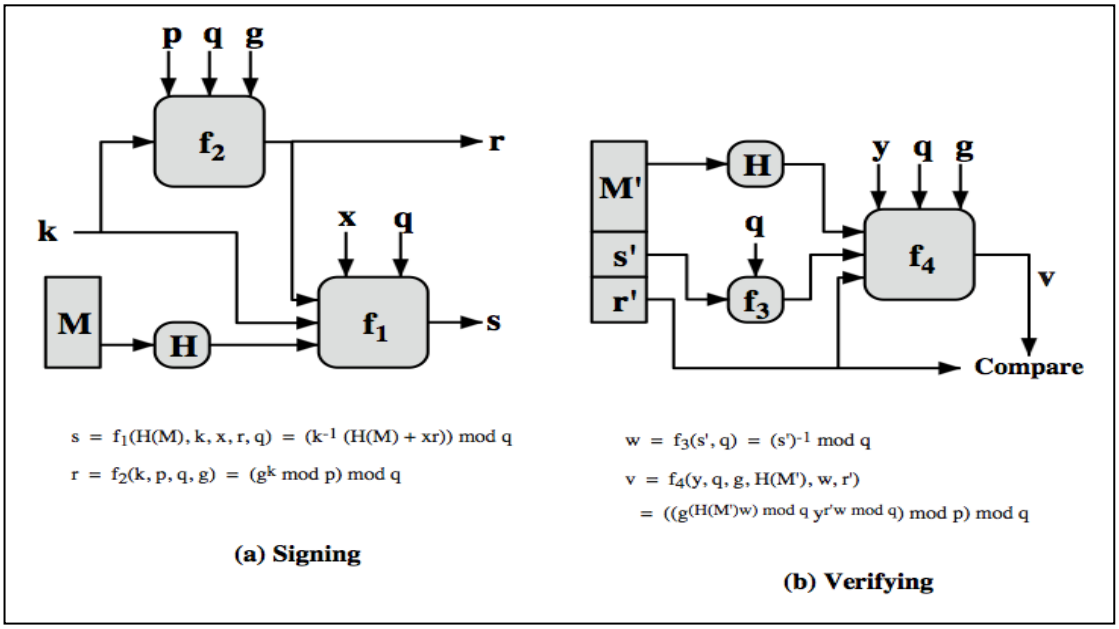
- **مقارنة بين أنظمة التشفير ذات public Key** :

الخوارزمية	تشفير/ فك تشفير	توقيع رقمي	تبادل مفاتيح
RSA	نعم	نعم	نعم
Elliptic curve	نعم	نعم	نعم
Diffie - Helman	لا	لا	نعم
DSS	لا	نعم	لا

*** مقارنة بين خوارزمية DSS و RSA من حيث التوقيع :**



* عملية إنشاء التوقيع والتحقق في DSS :



13.1 List two disputes that can arise in the context of message authentication.

13.1 Suppose that John sends an authenticated message to Mary. The following disputes that could arise: **1.** Mary may forge a different message and claim that it came from John. Mary would simply have to create a message and append an authentication code using the key that John and Mary share. **2.** John can deny sending the message. Because it is possible for Mary to forge a message, there is no way to prove that John did in fact send the message.

13.2 What are the properties a digital signature should have?

13.2 **1.** It must be able to verify the author and the date and time of the signature. **2.** It must be able to authenticate the contents at the time of the signature. **3.** The signature must be verifiable by third parties, to resolve disputes.

.

13.5 In what order should the signature function and the confidentiality function be applied to a message, and why?

13.5 It is important to perform the signature function first and then an outer confidentiality function. In case of dispute, some third party must view the message and its signature. If the signature is calculated on an encrypted message, then the third party also needs access to the decryption key to read the original message. However, if the signature is the inner operation, then the recipient can store the plaintext message and its signature for later use in dispute resolution.

13.6 What are some threats associated with a direct digital signature scheme?

13.6 1. The validity of the scheme depends on the security of the sender's private key. If a sender later wishes to deny sending a particular message, the sender can claim that the private key was lost or stolen and that someone else forged his or her signature. **2.** Another threat is that some private key might actually be stolen from X at time T. The opponent can then send a message signed with X's signature and stamped with a time before or equal to T.

13.7 Give examples of replay attacks.

- Simple replay
- . Repetition that can be logged
- Repetition that cannot be detected
- Backward replay without modification

13.8 List three general approaches to dealing with replay attacks

13.8 1. Attach a sequence number to each message used in an authentication exchange. A new message is accepted only if its sequence number is in the proper order. **2.** Party A accepts a message as fresh only if the message contains a timestamp that, in A's judgment, is close enough to

A's knowledge of current time. This approach requires that clocks among the various participants be synchronized. **3.** Party A, expecting a fresh message from B, first sends B a nonce (challenge) and requires that the subsequent message (response) received from B contain the correct nonce value.

13.9 What is a suppress-replay attack?

13.9 When a sender's clock is ahead of the intended recipient's clock., an opponent can intercept a message from the sender and replay it later when the timestamp in the message becomes current at the recipient's site. This replay could cause unexpected results.

Chapter 15

User Authentication Protocols

Chapter 15

User Authentication Protocols

- **يمكن أن يكون هناك اتصال بين A وB بحيث يتشاركان في المفتاح التشفيري السري (تشفير متماثل) يحصل كالآتي:**

١- يقوم A بإجراء التصافح وإرسال هويته identification بشكل واضح إلى B

٢- يقوم B بعملية التحقق Verification من A .

- **Distinct form Message Authentication :**

إجراء يمسح للاتصال ين الاطراف للتحقق من محتويات الرسالة بأنها لم تعدل.

- **معاني User Authentication :**

كلمات المرور – صوت وإشارة - البصمة والعين - المفاتيح .

- **Authentication Protocols له نوعان :**

١- **متبادل (Mutual) :**

هو إجراء بين مستفيدين لإجراء تبادل المفاتيح واثبات شخصية باستخدام handshaking حيث:

- Confidentiality: لحماية Session Key.

- Timeliness : للحماية من Replay attack .

٢- **One – way Function** :

هو ان المرسل والمستقبل غير متصلين في نفس الوقت .

فمثلا: تخزين جدولا لكلمات المرور في الحاسوب المضيف لكل مستفيد حيث أن استرجاع كلمة المرور لا يمكن لأنه دالة one-way لا يمكن عكسها لاسترجاع كلمة المرور.

- **تعريف إدارة الهوية الموحد (Federated Identity Management) :**

هي السيطرة والتحكم بالمعلومات الخاصة بالمستخدمين على اجهزة الكمبيوتر والسماح للمستخدمين من استعمال خدمات تكنولوجيا المعلومات وغيرها وإدارة الوصول في حماية السرية والسلامة والتأكد من المستخدمين ذوي التصريح للوصول.

- **ماذا نعني بـ Kerberos:**

هو بروتوكول مصادقة الشبكة مصمم لتوفير مصادقة قوية بين العميل والسيرفر باستخدام مفتاح سري للتشفير.

تعتبر شبكات الانترنت بانها مكان غير آمن من حيق معظم البروتوكولات تفتقد للأمان وأقرب مثال كلمة السر تكون في الشبكة بصورة غير مشفرة ومن هنا جاء تصميم **Kerberos فهو :**

١- يسمح للعميل بإثبات هويته للخادم .

٢- تشفير جميع اتصالاتهم لضمان سلامة المعلومات .

- **كيف يعمل الـــ Kerberos:**
  - يعمل عبر نظام تشفير يعتمد على المفاتيح السرية (متماثلة- خاصة) مع خوارزميات DES
  - يشارك كل عميل في الشبكة مفتاحا سريا مع **Kerberos** للتعرف على الهوية .
  - **يقوم على مبدأ التذاكر (Ticket) وخطواته :**
    ١- الحصول على إذن للوصول إلى الخدمة :إرسال المستخدم هويته إلى Authentication Server .
    ٢- يتحقق Authentication Server من الهوية ويرسل تذكرة أولية للمستخدم مشفرة مع المفتاح تحتوي على (مفتاح session + الوصول لخدمة التذاكر للحصول على التذكرة).
    ٣- العميل يقوم بفك شفرة التذكرة الأولية مع المفتاح ويحصل على تذكرة ومفتاح Session .
  - وبفضل التذكرة ومفتاح Session يصبح للعميل إرسال طلب مشفر للخدمة الموجودة في التذكرة قبل أن يحصل على الخدمة التي طلبها.
  - ملاحظة: التعريفات التي يقدمها **Kerberos** **وقتية** لتفادي القرصنة والمحافظة على الموارد .

14.1 What problem was Kerberos designed to address?

14.1 The problem that Kerberos addresses is this: Assume an open distributed environment in which users at workstations wish to access services on servers distributed throughout the network. We would like for servers to be able to restrict access to authorized users and to be able to authenticate requests for service. In this environment, a workstation cannot be trusted to identify its users correctly to network services.

14.2 What are three threats associated with user authentication over a network or Internet?

14.2 **1.** A user may gain access to a particular workstation and pretend to be another user operating from that workstation. **2.** A user may alter the network address of a workstation so that the requests sent from the altered workstation appear to come from the impersonated workstation. **3.** A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations.

14.4 What four requirements were defined for Kerberos?

14.4 **Secure:** A network eavesdropper should not be able to obtain the necessary information to impersonate a user. More generally, Kerberos should be strong enough that a potential opponent does not find it to be the weak link. **Reliable:** For all services that rely on Kerberos for access control, lack of availability of the Kerberos service means lack of availability of the supported services. Hence, Kerberos should be highly reliable and should employ a distributed server architecture, with one system able to back up another. **Transparent:** Ideally, the user should not be aware that authentication is taking place, beyond the requirement to enter a password. **Scalable:** The system should be capable of supporting large numbers of clients and servers. This suggests a modular, distributed architecture.

14.5 What entities constitute a full-service Kerberos environment?

14.5 A full-service Kerberos environment consists of a Kerberos server, a number of clients, and a number of application servers.

14.6 In the context of Kerberos, what is a realm?

14.6 A realm is an environment in which: **1.** The Kerberos server must have the user ID (UID) and hashed password of all participating users in its database. All users are registered with the Kerberos server. **2.** The Kerberos server must share a secret key with each server. All servers are registered with the Kerberos server.

14.7 What are the principal differences between version 4 and version 5 of Kerberos?

14.7 Version 5 overcomes some environmental shortcomings and some technical deficiencies in Version 4.

Chapter 17

Transport-Level Security (TLS)

Chapter 17

Transport-Level Security (TLS)

* تتلخص أهداف خدمات التأمين للشبكات في الآتي:

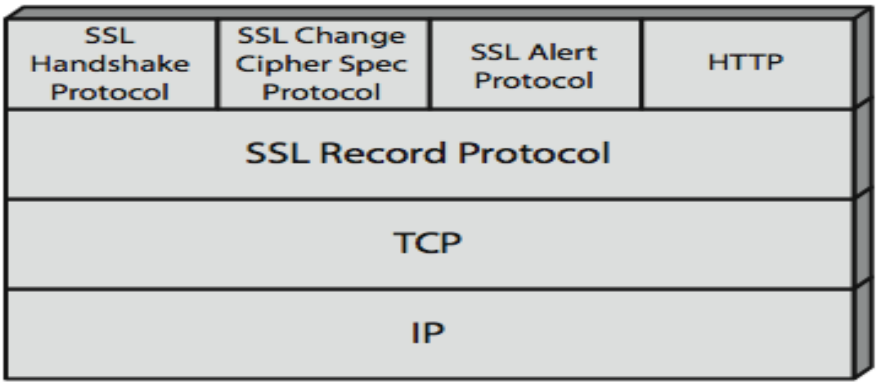
١- الخصوصية أو السرية . ٢- المصداقية.

٣- تكامل البيانات. ٤- الإتاحية.

- الهجمات على طبقة التطبيقات :
تأثر على النظام المستخدم في أجهزة الشبكة + البرامج المستخدمة مثل (الفيروسات والديدان). لذا كان لابد من تأمين هذه الأمور الحساسة كالتجارة الإلكترونية وعمليات كشف الحسابات فتم تطوير تقنية SSL (**Secure Socket Layer**) **.**
- الاتصالات الآمنة الأكثر شيوعا يستخدم بروتوكولي (SSL/TLS) .
١- SSL: بروتوكول طور من قبل شركة Netscape لنقل البيانات بطريقة آمنة عبر الانترنت وتحتاج إلى الشهادة الالكترونية.
٢- TLS: إضافة إلى بروتوكول SSL وهو تقنية محسنة له ويختلف في طريقة اداء العملية. ويسمون معا بمعيار (SSL/TLS) ليضمن الخصوصية (privacy) ودقة البيانات (Data integrity) .
- بشكل عام يتكون SSL/TLS من طبقيتين :
١- بروتوكول مصافحة الأيدي Handshake protocol (TLS) :
ويستخدم لإثبات علاقة بين Server and client للتفاوض في خوارزمية التشفير والمفاتيح قبل السماح بانتقال البيانات بين Server and client.
٢- بروتوكول التسجيل Record protocol (TLS) :
يسمح للـ Server and client بالاتصال فيما بينهم وتبادل البيانات باستخدام التشفير او دون استخدام التشفير حسب الحاجة .
- **أهم ثلاثة طبقات في نظام OSI في عمليات التشفير :**

الطبقة	**البروتوكول الذي يعمل عليها**
التطبيقات	Kerberos + S/MIME
النقل	SSL + TLS
الشبكة	IP/IPsec

- **معمارية SSL:**



- **SSL Change Cipher Spec Protocol**

— a single message consists of a single byte with the value 1.

— that signals the beginning of secure communications between the client and server.

(a) Change Cipher Spec Protocol

SSL Alert Protocol

This protocol sends errors, problems or warnings about the connection between the two parties.

This layer is formed with two fields:

Severity level

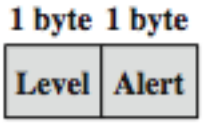
Warning value 1 or fatal value 2

specific alert

fatal: unexpected message, bad record mac, decompression failure, handshake failure, illegal parameter

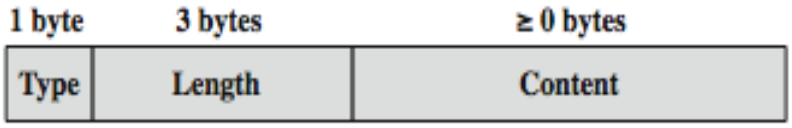
warning: close notify, no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown

compressed & encrypted like all SSL data



(b) Alert Protocol

- **SSL Handshake Protocol**
- Allows server & client to:
  - **authenticate each other**
  - **to negotiate encryption & MAC algorithms**
  - **to negotiate cryptographic keys** to be used to protect data sent in an SSL record.
- is used before any application data is transmitted.
- comprises a series of messages in phases
  - Establish Security Capabilities
  - Server Authentication and Key Exchange
  - Client Authentication and Key Exchange
  - Finish
  - **Type:** Table 16.2
- **Content (bytes):** Table 16.2.



(c) Handshake Protocol

- **Server message block (SMB)** : هي Packet يتم إرسالها بين السيرفر والأجهزة في عملية Sharing والحماية من السرقة للمعلومات بطريقة SMB Signing ويتم بواسطتها إضافة Hash .
- **مشكلة HTTP** :

١- أن بعض البيانات المرسلة (كلمة المرور مثلا) يتم إرسالها بطريقة غير مشفرة.

٢- عدم وجود آلية للتحقق من هوية الموقع الذي يتعامل معه .

- **حل مشكلة HTTP هي استخدام HTTP secure (HTTPS) :**

١- تشفير البيانات المرسلة حيث يستخدم بروتوكول SSL/TLS مع HTTP.
٢- يقوم بروتوكول SSL بالتأكيد من هوية الموقع عن **طريق الشهادة الالكترونية**.

*** Secure Shell (SSH) :**

- **لديها ثلاث بروتوكولات تعمل في طبقة النقل:**

1- SSH user authentication protocol .
2- SSH connection protocol . فتح قناة + نقل بيانات + غلق قناة
3- SSH Transport layer protocol .

- **شرحها باختصار:**

تم عمل هذه الخدمة من أجل استبدال الخدمة السابقة Telnet والتي يتم ارسال البيانات بين المستخدم والسيرفر بشكل مكشوف (clear text) يعني كلمة السر والبيانات المارة بينك وبين الجهة المتصل بها كلها عبارة واضحة لأي شخص قد يعمل على مراقبة الشبكة من خلال برامج مراقبة الشبكة (**SNFFING+ WIRESHARK**)

- **استخدمت SSH طريقة أكثر قوة من خلال تشفير البيانات المارة بينك وبين السيرفر بطرق تشفير قوية للغاية منها: Blowfish + Triple DES+ AES** .
- **خدمة SSH تدعم طرق توثيق authentication مختلفة هي :**

١- Host- key authentication :

وذلك من خلال استخدام اسم مستخدم وكلمة مرور قوية للدخول على السيرفر (طريقة شائعة وعادية).

٢- Public- key authentication :

وذلك من خلال استعمال مفتاح خاص private بك للاتصال بالسيرفر الذي يحمل مفتاح عام public ويكون للمفتاح الخاص كلمة مرور Passphrase (أفضل طريقة وتحتاج إلى جهد وعمل بنسبة ما).

٣- Passphrase – less authentication :

نفس الطريقة السابقة ولكن بدون عمل كلمة مرور للمفتاح الخاص (يتم استخدامها في العمليات الاوتوماتيكية ولكن غير كافية من ناحية السرية).

- **ملاحظة**:

الأمن في طبقة التطبيقات والعرض: وظيفته محدودة (تشفير ما بنيت لأجله) توجد بيانات لا تشفر.
الأمن في طبقة الشبكة : ابتكرت طريقة IPsec لتشفير كل packet حيث يوفر الموثوقية + الصحة + التشفير الكامل.

17.2 What protocols comprise SSL?

17.2 SSL handshake protocol; SSL change cipher spec protocol; SSL alert protocol; SSL record protocol.

17.3 What is the difference between an SSL connection and an SSL session?

17.3 **Connection:** A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session. **Session:** An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

17.4 List and briefly define the parameters that define an SSL session state

17.4 **Session identifier:** An arbitrary byte sequence chosen by the server to identify an active or resumable session state. **Peer certificate:** An X509.v3 certificate of the peer. **Compression method:** The algorithm used to compress data prior to encryption. **Cipher spec:** Specifies the bulk data encryption algorithm (such as null, DES, etc.) and a hash algorithm (such as MD5 or SHA-1) used for MAC calculation. It also defines cryptographic attributes such as the hash_size. **Master secret:** 48-byte secret shared between the client and server. **Is resumable:** A flag indicating whether the session can be used to initiate new connections.

17.5 List and briefly define the parameters that define an SSL session connection

17.5 **Server and client random:** Byte sequences that are chosen by the server and client for each connection. **Server write MAC secret:** The secret key used in MAC operations on data sent by the server. **Client write MAC secret:** The secret key used in MAC operations on data sent by the client. **Server write key:** The conventional encryption key for data encrypted by the server and decrypted by the client. **Client write key:** The conventional encryption key for data encrypted by the client and

decrypted by the server. **Initialization vectors:** When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key. This field is first initialized by the SSL Handshake Protocol. Thereafter the final ciphertext block from each record is preserved for use as the IV with the following record. **Sequence numbers:** Each party maintains separate sequence numbers for transmitted and received messages for each connection. When a party sends or receives a change cipher spec message, the appropriate sequence number is set to zero. Sequence numbers may not exceed $2^{64} - 1$.

17.6 What services are provided by the SSL Record Protocol?

17.6 **Confidentiality:** The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads. **Message Integrity:** The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

17.7 What steps are involved in the SSL Record Protocol transmission?

17.7 Fragmentation; compression; add MAC; encrypt; append SSL record header.

17.1 In SSL and TLS, why is there a separate Change Cipher Spec Protocol, rather than including a change_cipher_spec message in the Handshake Protocol?

17.1 The change cipher spec protocol exists to signal transitions in ciphering strategies, and can be sent independent of the complete handshake protocol exchange

Chapter 18

Electronic Mail Security

Chapter 18
Electronic Mail Security

- **برنامج Pretty Good Privacy (PGP) :**

البرنامج الذي بين أيدينا أثبت جدارته وصموده أمام كثير من محاولات الكسر ولعل أهم ما يميزه أنه يستخدم في التشفير مفتاح بطول 128 bit .

يطلق عليه الخصوصية المتوفقة.

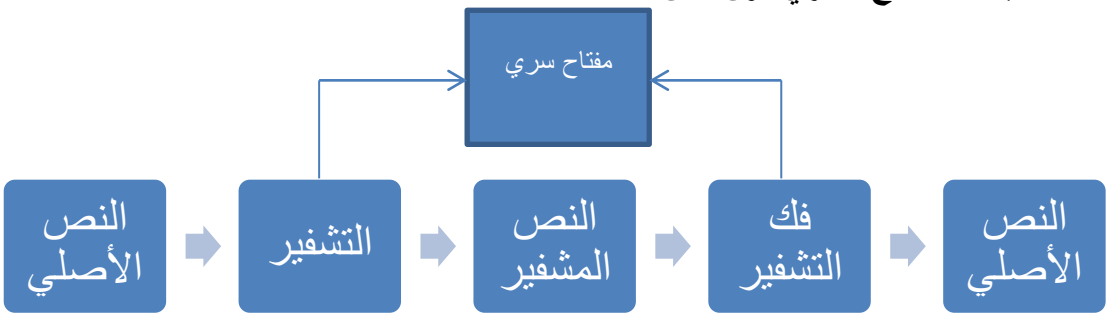
مصمم البرنامج Phil Zimmermann .

- **عادة ما يستند تشفير ملف ما إلى الخوارزمية أما قوة التشفير فترتكز على نقطتين:**

الخوارزمية + طول المفتاح .

- **التشفير المتماثل (مفتاح سري) : DES**

مشكلته **تبادل المفتاح السري دون أمان .**



- **التشفير غير المتماثل(المفتاح العام) :RSA :**

حل مشكلة التشفير المتماثل : استخدام مفتاحين public and private بدلا من مفتاح سري واحد .

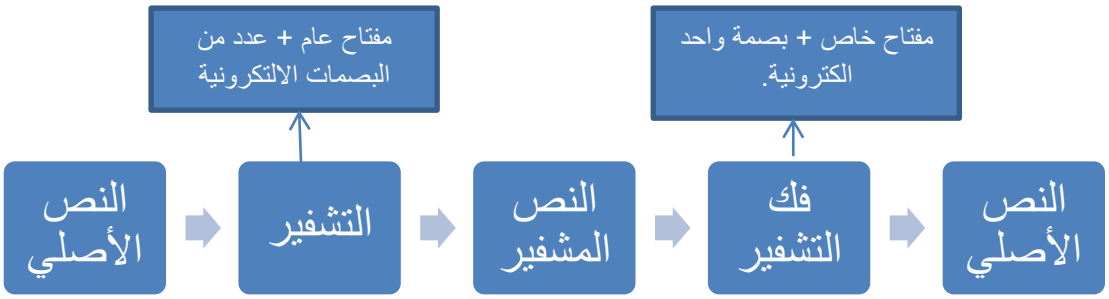
- المفتاح private معروف لدى المرسل (يستخدم لتشفير + فك تشفير).
- المفتاح public معروف لدى جهة أو شخص (يستخدم لفك التشفير + تشفير رسائل مالك المفتاح private .
- لا يمكن فك تشفير رسالة باستخدام مفتاح public رسالة مشفرة من هذا المستخدم باستخدام مفتاح public بل المستخدم الذي لديه المفتاح Private يستطيع فك شفرة تلك الرسالة .

- **نظام RAS أفضل من DES من حيث الأمان ولكن أبطأ من حيث جلسة التشفير وفك التشفير يجب ان تكون متزامنتين تقريبا**

- **لهذا تم تطور PGP الذي يعد نموذجا محسنا من نظام RAS ويستخدم ما يلي:**

١- مفتاح بطول 128 bit .

٢- البصمة الالكترونية للرسالة (Message Digest) .



- PGP Key Ring :

Private Key Ring

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
. . .	. . .	. . .	. . .	. . .
Ti	PU_i mod 2^{64}	PU_i	E(H(P_i), PR_i)	User *i*
. . .	. . .	. . .	. . .	. . .

Public Key Ring

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
Ti	PU_i mod 2^{64}	PU_i	$trust\_flag_i$	User *i*	$trust\_flag_i$		
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .

* = field used to index table

15.1 What are the five principal services provided by PGP?

15.1 Authentication, confidentiality, compression, e-mail compatibility, and segmentation

15.2 What is the utility of a detached signature?

15.2 A detached signature is useful in several contexts. A user may wish to maintain a separate signature log of all messages sent or received. A detached signature of an executable program can detect subsequent virus

infection. Finally, detached signatures can be used when more than one party must sign a document, such as a legal contract. Each person's signature is independent and therefore is applied only to the document. Otherwise, signatures would have to be nested, with the second signer signing both the document and the first signature, and so on.

15.3 Why does PGP generate a signature before applying compression?

15.3 **a.** It is preferable to sign an uncompressed message so that one can store only the uncompressed message together with the signature for future verification. If one signed a compressed document, then it would be necessary either to store a compressed version of the message for later verification or to recompress the message when verification is required.
b. Even if one were willing to generate dynamically a recompressed message for verification, PGP's compression algorithm presents a difficulty. The algorithm is not deterministic; various implementations of the algorithm achieve different tradeoffs in running speed versus compression ratio and, as a result, produce different compressed forms. However, these different compression algorithms are interoperable because any version of the algorithm can correctly decompress the output of any other version. Applying the hash function and signature after compression would constrain all PGP implementations to the same version of the compression algorithm.

15.9 What is MIME?

15.9 MIME is an extension to the RFC 822 framework that is intended to address some of the problems and limitations of the use of SMTP (Simple Mail Transfer Protocol) or some other mail transfer protocol and RFC 822 for electronic mail.

15.10 What is S/MIME?

15.10 S/MIME (Secure/Multipurpose Internet Mail Extension) is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security.

15.4 The first 16 bits of the message digest in a PGP signature are translated in the clear

a. To what extent does this compromise the security of the hash algorithm?

15.4 a. Not at all. The message digest is encrypted with the sender's private key. Therefore, anyone in possession of the public key can decrypt it and recover the entire message digest.

b. To what extent does it in fact perform its intended function, namely, to help determine if the correct RSA key was used to decrypt the digest?

b. The probability that a message digest decrypted with the wrong key would have an exact match in the first 16 bits with the original message digest is 2^{-16}.

Chapter 19

IP Security

Chapter 19

IP Security

- **ما هي IP/ sec :**

هي مجموعة من معايير البروتوكولات والخوارزميات طورت بواسطة اللجنة الخاصة لنظام الانترنت (IETF) واعتمدت كمعايير للإنترنت لتوفر (التحقق من سلامة المعلومات + سريتها).

وذلك يجعلها تعمل في طبقة network حيث تمكن من حماية أي نوع من البيانات تم نقله من خلال IP .

عادة يعبر عن IP/sec بانها : Transport security protocol السبب:

لأن المستخدم والتطبيقات لا يشعرون بوجودها لأنها في تعمل في طبقة Network .

يعمل في البيئات التي تكون سرعة الاتصال بها **سريعة** .

- **بروتوكولات IP/Sec :**

ينقسم إلى ثلاث بروتوكولات هي:

١- **Authentication Header (AH) :**

يستخدم في **توقيع الرسالة** ولا يقوم **بتشفيرها** حيث يحافظ على الآتي:

- صحة البيانات (Data integrity) : لم تعدل أثناء إرسالها
- موثوقية البيانات (Date **Authentication**) : أنها المستخدم نفسه وليست مزورة .
- عدم إعادة الإرسال (Anti-replay) وهي سرقة كلمات المرور وهي مشفرة وترسل للسيرفر وقت آخر .
- الحماية ضد الخداع (Anti-spoofing protection) : عندما يحدد مدير الشركة عناوين معينة للدخول ويقوم المستخدم بتغيير عنوانه وهذا لا يمكن في الـــ IP/Sec .

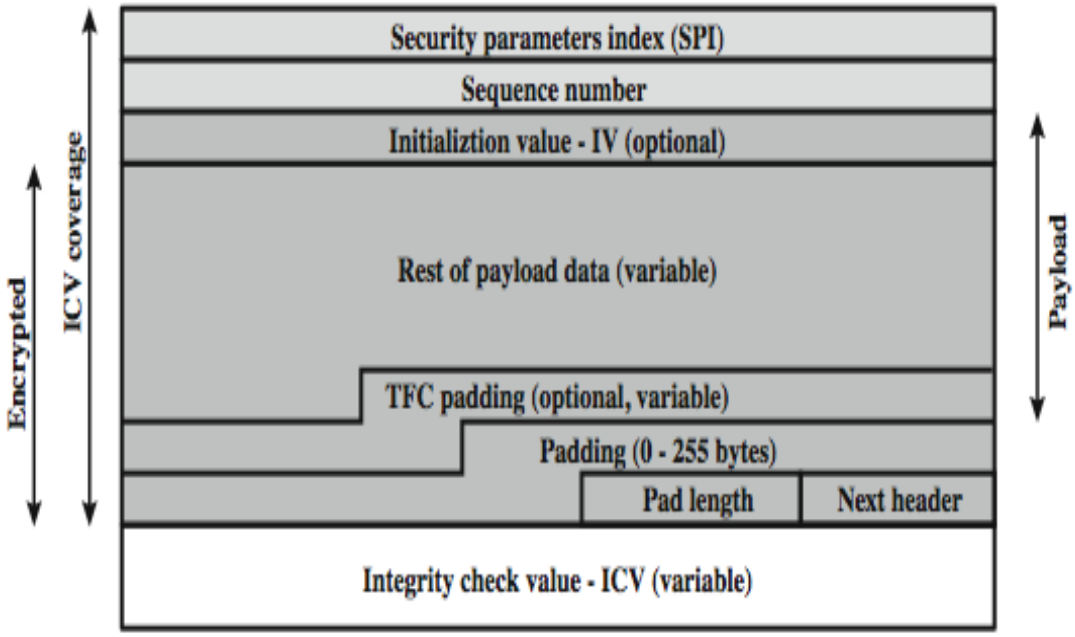
٢- **Encapsulating Security Payload(ESP) :**

يوفر هذا البروتوكول **التشفير والتوقيع للبيانات .**

ويستخدم في كون المعلومات سرية أو عند إرسال المعلومات عن طريق الانترنت.

ويوفر **ESP** المزايا التالية :

- مصداقية المرسل (source Authentication) .
- تشفير البيانات (Data Encryption) .
- عدم إعادة الإرسال (Anti-replay)
- الحماية ضد الخداع (Anti-spoofing protection).



٣- Internet Key Exchange (IKE) :

الوظيفة الأساسية هي :

١- ضمان كيفية وعملية ومشاركة المفاتيح بين مستخدمي IP/Sec .

٢- فهو بروتوكول نقاش Negotiation في نظام IP/sec كما أنه يعمل على تأكيد طريقة الموثوقية والمفاتيح الواجب استخدامها ونوعها.

- **يستخدم الـIp/sec التشفير بخوارزمية 3-DES** وهو عبارة عن زوج من المفاتيح ذاتها يتولد عشوائيا بطرق معقدة ويتم فقط إعطاءه للجهة الثانية ويمنع من توزيعه وهو نوع من أنواع التشفير المتماثل التي تستخدم مفتاح private .
- **أقسام الـIP/sec:**

١- نظام النقل (Transport mode) .

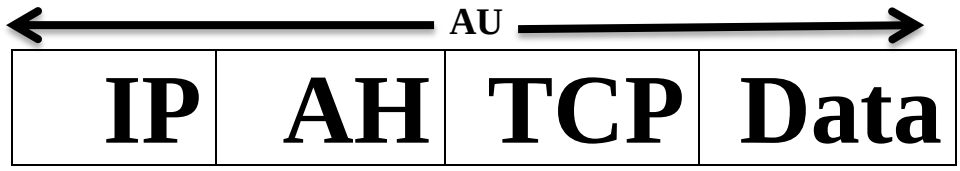
٢- نظام النفق (Tunnel mode).

- **نظام النقل (Transport mode) :**
  - يستخدم داخل شبكة محلية ويقوم بعلمية التشفير للبيانات حسب الـ IP/sec فمثلا استخدام Telnet .
  - يطبق في حالات منها:

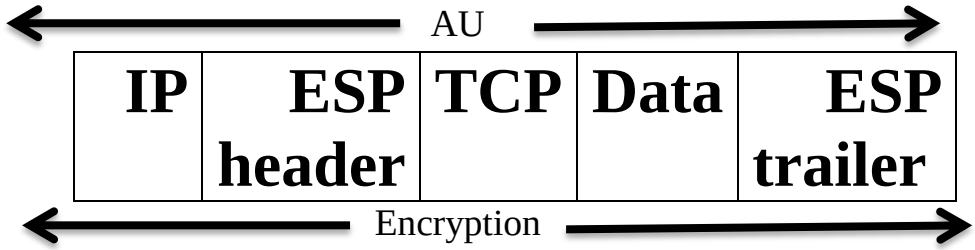
    ١- المحادثة بين الأجهزة في شبكة داخلية.

    ٢- المحادثة بين جهازين ولا يقطع بينها firewall يعمل عملNAT .
- **نظام النفق (Tunnel mode).**
  - يستخدم بين نقطتين تكون بالعادة بين Two Routers بعيدة جغرافيا WAN .
  - يستخدم في حالة مرور البيانات أثناء مروها بطرق غير آمنة مثل الانترنت وكذلك FTP .

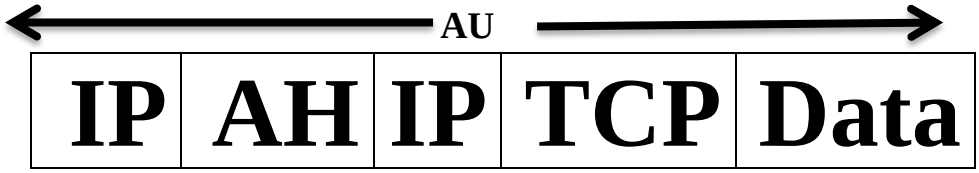
- **مخطط Packet في أقسام IP/sec :**
  - **نظام النقل (Transport mode) :**
  - Authentication :



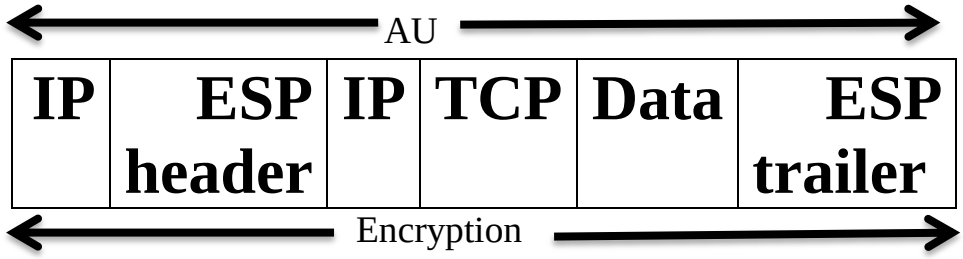
- Encapsulating Security Payload(ESP) :



- **نظام النفق (Tunnel mode).**
- Authentication :



- Encapsulating Security Payload(ESP) :



- **فوائد الـ IP/Sec :**

أنه يوفر حماية كاملة لجميع البروتوكولات التي تعمل على طبقة Network .

- **مميزات الـ IP/Sec :**

أنه Built –in في داخل حزمة الـ IP packet **" لا يحتاج لأي إعدادات لاتصاله عبر الشبكة ولا يحتاج إلى أي أجهزة إضافية"** .

- **كيف يحمي الـ IP/Sec من الهجوم على الشبكة:**
  - هناك هجوم غير فعالة (Passive) مثل مراقبة الشبكة.
  - هناك هجوم فعال (Active) تعديل البيانات .
- **أنواع الهجمات :**

١- التقاط حزم البيانات: تكون غير مستقرة يقوم الـIP/Sec بتشفيرها.
٢- تعديل البيانات : استخدام Hash مع البيانات ثم تشفيرها.
٣- انتحال الشخصية: باستخدام Kerberos + الشهادات الالكترونية+ تشفير كلمة المرور .
٤- رفض الخدمة او حجبها: عن طريق إغلاقه ووضع قواعد للمنافذ المفتوحة.
٥- هجوم الوسط: باستخدام طرق التحقق من الوثوقية .
٦- الهجوم على طبقة التطبيقات : وجود الفلاتر لإسقاط حزم البيانات غير المتطابقة.

- **لماذا يستخدم في Padding field ESP :**

١- توسيع الـPlaintext للحد المطلوب.
٢- ترتيب طول وحقول العنوان Header إلى حد 32bit .
٣- تزويد سرية كسر المرور الجزئية بإخفاء الطول الفعلي لـ Payload

- **مفاهيم أساسية:**
  - **Security Association (SA) :**

هي عبارة عن Argument بين devise عن كيفية حماية المعلومات أثناء الاتصال.

  - **security association database (SAD)** :

يعرف فيها أي traffic ستكون محمية + كيفية حمايتها + من سيحميها.

  - **the security policy database (SPD)** :

تتمتع بالخصائص التالية وتحتوي على :

١- Distention IP address
٢- IP/sec protocol
٣- Security parameter index(SPI)

19.1 Give examples of applications of IPSec .

- Secure branch office connectivity over the Internet
- . Secure remote access over the Internet
- . Establishing extranet and intranet connectivity with partners
- . Enhancing electronic commerce security

19.2 What services are provided by IPSec?

19.2 Access control; connectionless integrity; data origin authentication; rejection of replayed packets (a form of partial sequence integrity); confidentiality (encryption); and limited traffic flow confidentiality

19.4 What is the difference between transport mode and tunnel mode?

19.4 **Transport mode** provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet. **Tunnel mode** provides protection to the entire IP packet.

19.5 What is a replay attack?

19.5 A replay attack is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence.

Chapter 22

Firewalls

Chapter 22

Firewalls

- **ما هي جدر الحماية النارية (Firewalls):**

هي عبارة عن نظام متكامل بين البرمجيات والعتاد للتحكم في تدفق البيانات من خلال شبكة آمنة إلى شبكة غير آمنة أو العكس حيث ان هذه البيانات قد بسمح لها المرور أو الرفض .

- **لماذا نحتاج إلى جدار الحماية الناري:**

١- منع هجمات تعطيل الخدمة حيث يقوم المهاجم بإغراق الشبكة بعدة اتصالات مزيفة بالحزم .
٢- منع تعديل أو الوصول للمعلومات الداخلية في الشبكة.
٣- السماح بالمصرح لهم بالدخول إلى الشبكة الداخلية فقط .
٤- منع المستخدمين داخل الشبكة من الوصول إلى مصادر سيئة خارج الشبكة .

- **ما الذي لا يستطيع جدار الحماية أن يعمله :**

١- منع الفيروسات من الدخول إلى الجهاز إذا قدمت من عنوان ليس له صلاحية في الدخول أن ٩٥% من الفيروسات تأتي من خلال رسائل البريد الالكتروني الحل : تركيب مضاد الفيروسات .
٢- الحماية من المخاطر داخل الشبكة نفسها .
٣- الحماية من الهجمات المعتمدة على البروتوكولات .

- **أنواع جدر الحماية :**

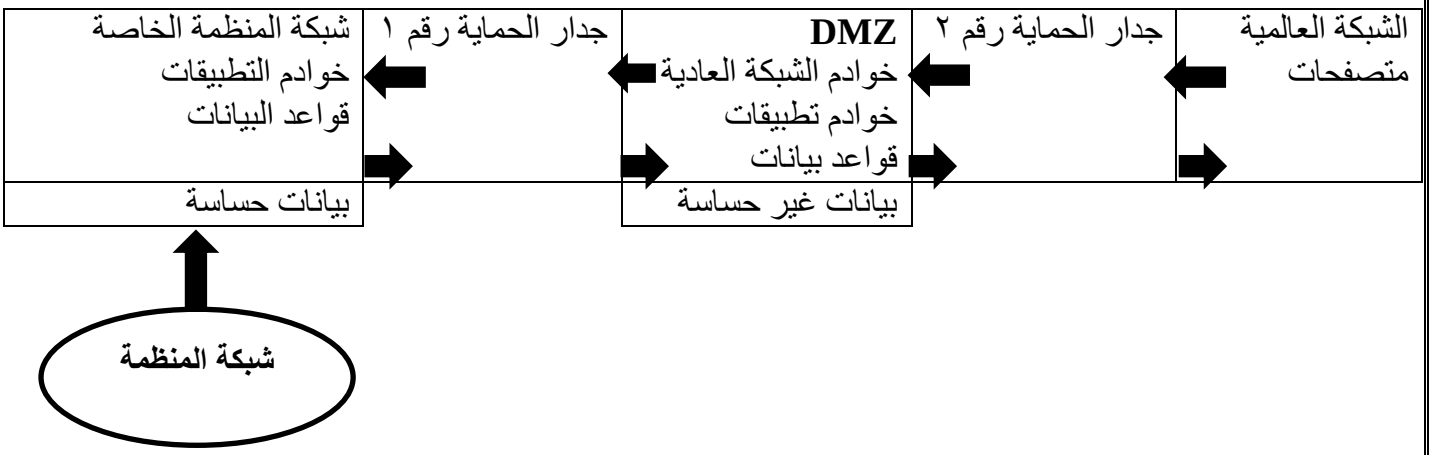
- من خلال وضعها داخل الجهاز أو خارجه إلى قسمين :
  ١- Hardware: مثل router .
  ٢- Software: مثل البرامج المصنعة في نظام التشغيل .
- من خلال التكنولوجيا المستخدمة إلى ثلاثة أنواع :
  ١- فلترة الرسالة (packet filtering) :
  يقوم بفحص عنوان المرسل والمستقبل الموجود في بيانات الرسالة .
  ٢- طبقة التطبيقات ويعرف بـ (proxy firewall) **:**
  يعمل على طريقة الخادم والعميل هذا مفيد في حالة يريد مدير النظام منع موظفين من استخدام تطبيق معين .
  ٣- حالة التفتيش (Stateful Inspection):
  يقوم بتفتيش الرسالة ومعرفة حالتها وهل تم استقبال رسائل من هذا الموقع أم لا.

- **هناك استراتيجيات رئيسية لتوفير الحماية من خلال جدار الحماية :**

١- يجب منع أي رسالة لا يعرفها جدار الحماية.
٢- لا تعتمد على الجدار الناري فقط استخدم الدفاع بعمق (Defense in dept.) وضع عدة مستويات حماية.
٣- التأكد من مرور جميع من في الشبكة من خلال الجدار الناري.
٤- عند توقف الجدار الناري يجبر توقف (قطع) جميع الاتصالات.

- **المنطقة المحايدة demilitarized zone (DMZ) :**

- الهدف منها : حماية الشبكة السلكية سواء كانت محلية أو واسعة من الهجمات التي تتعرض لها من المخترقين من شبكة الانترنت.



- **الهدف من جدار الحماية رقم ٢ :**

حماية الخوادم (مرئية للعالم) من الهجمات القادمة من الشبكة العالمية.
وتكون الحماية على أساس الفلترة (سماح / منع) حيث :
تسمح بمرور HTTP&HTTPS وتمنع TELNET& FTP

- **وقد ظهرت تقنية أوعية العسل (Honey pots) :**

تستخدم في المنطقة المحايدة لإبعاد الاختراقات المحتملة على شبكة المنظمة وهي عبارة عن خوادم مزودة ببرامج وبيانات تظهر كأنها موثوقة وصحيحة لتوجيه أنظار المخترقين إليها وصرفهم عن الخوادم الحقيقية.

20.2 List four techniques used by firewalls to control access and enforce a security policy.

- Service control
- . Direction control
- . User control
- . Behavior control

20.3 What information is used by a typical packet-filtering router?

- Source IP address
- Destination IP address
- Source and destination transport-level address
- IP protocol field
- . Interface

20.5 What is the difference between a packet-filtering router and a stateful inspection firewall?

20.5 A **traditional packet filter** makes filtering decisions on an individual packet basis and does not take into consideration any higher layer context. A **stateful inspection packet filter** tightens up the rules for TCP traffic by creating a directory of outbound TCP connections, as shown in Table 20.2. There is an entry for each currently established connection. The packet filter will now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory

20.6 What is an application-level gateway?

20.6 An application-level gateway, also called a proxy server, acts as a relay of application-level traffic.

20.7 What is a circuit-level gateway

20.7 A circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host. Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents. The security function consists of determining which connections will be allowed.

20.9 In the context of access control, what is the difference between a subject and an object?

20.9 A **subject** is an entity capable of accessing objects

An **object** is anything to which access is controlled

20.10 What is the difference between an access control list and a capability ticket?

20.10 For each object, an **access control list** lists users and their permitted access rights. A **capability ticket** specifies authorized objects and operations for a user.

20.11 What are the two rules that a reference monitor enforces?

20.11 **No read up:** A subject can only read an object of less or equal security level. **No write down:** A subject can only write into an object of greater or equal security level.

20.12 What properties are required of a reference monitor?

- Complete mediation
- Isolation
- Verifiability

20.13 What are the common criteria?

20.13 The Common Criteria (CC) for Information Technology and Security Evaluation is an international initiative by standards bodies in a number of countries to develop international standards for specifying security requirements and defining evaluation criteria.