((security))

1) computer security: generic name for the collection of tools, designed to protect data and to thwart hackers.
(اسم عام لمجموعة الأدوات التي تعمل على حماية البيانات واحباط المتسللين)
2) network security: measures to protect data in networked systems.
(تدابير لحماية بيانات الأنظمة الشبكية)
3) internet security: measures to protect data during their transmission over the Internet.
(تدابير لحماية البيانات التي يتم تقلها عبر الانترنت)

((the NIST computer security))

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources” (includes hardware, software, firmware, information/data, and telecommunications.

((key security))

1) confidentiality: preserving authorized restrictions on information access and disclosure including means for protecting personal privacy and proprietary information.
(الحفاظ على القيود المصرح لها من الوصول الى المعلومات والكشف عن المعلومات الشخصية)
2) integrity: guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.
(الحماية من التعديل على البيانيات او استخدامها بكل خاطئ)
3) Availability: ensuring timely and reliable access to and use of information.(ضمان الدخول الى المعلومات للأشخاص المخول لهم فقط)

((The CIA triad))

1) Confidentiality: This term covers two related concepts:
   Data confidentiality. (ضمان عدم الكشف عن المعلومات للأفراد)
   Privacy. (ان يتحكم الفرد بالمعلومات وحفظها وتخزينها)
2) Integrity: This term covers two related concepts:
   Data integrity.(يضمن عدم تغير المعلومات الا للمخول لهم)
   System integrity. (يضمن ان النظام يؤدي مهامه بطريقة صحيحة)
3) Availability: assure that systems works promptly, and service is not denied to authorized users.
   (تضمن وصول المعلومات الى المستخدم بطريقة صحيحة)

((addition key))

1) Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
   (هذه الخاصية لها القدرة على معرفة المرسل والمكان والمرسل اليه والتأكد من المصدر)
2) **A**ccountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
   (هي احد الأهداف الأمنية التي تنشئ متطلبات ليتم تقصيها بشكل كبير)

((levels of impact))

Low: the loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Moderate: the loss could be expected to have a serious adverse effect on organizational operations, organizational assets

((computer security challenges))

- Computer security is not as simple as it might first appear to the novice.
  ((أمان الكمبيوتر ليس بهذه البساطة كما قد يبدو لأول مرة للمبتدئين))
- Potential attacks on the security features must be considered.
  ((يجب النظر في الهجمات المحتملة على ميزات الأمان))
- Procedures used to provide services are often counterintuitive.
  ((غالبًا ما تكون الإجراءات المستخدمة لتقديم الخدمات غير منطقية))
- Physical and logical placement needs to be determined.
  ((يجب تحديد الوضع المادي والمنطقي))
- Additional algorithms or protocols may be involved.
  ((قد يتم تضمين خوارزميات أو بروتوكولات إضافية))
- Attackers only need to find a single weakness; the developer needs to find all weaknesses.
  ((يحتاج المهاجمون فقط إلى إيجاد نقطة ضعف واحدة؛ المطور يحتاج إلى إيجاد كل نقاط الضعف))
- Users and system managers tend to not see the benefits of security until a failure occurs.
  ((يميل المستخدمون ومديرو النظام إلى عدم رؤية فوائد الأمان حتى حدوث الفشل))
- Security requires regular and constant monitoring.
  ((يتطلب الأمن مراقبة منتظمة ومستمرة))
- Is often an afterthought to be incorporated into a system after the design is complete.
  ((غالبًا ما تكون فكرة لاحقة يتم دمجها في نظام بعد اكتمال التصميم))
- Thought of as an impediment to efficient and user-friendly operation.
  ((يعتقد أنه عائق أمام التشغيل الفعال وسهل الاستخدام))

((computer security terminology))

Adversary (threat agent): an entity that attacks, or is a threat, a system.

((**الخصم (وكيل التهديد):** كيان يهاجم، أو يمثل تهديدًا، نظامًا))

Attack: an assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

((**هجوم:** اعتداء على أمن النظام ينبع من تهديد ذكي؛ أي فعل ذكي هو محاولة متعمدة (خاصة بمعنى طريقة أو تقنية) للتهرب من الخدمات الأمنية وانتهاك السياسة الأمنية للنظام))

Countermeasure: an action, device, procedure, or technique that a vulnerability, or an attack by eliminating or preventing it, by minimzing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

((**هجوم:** اعتداء على أمن النظام ينبع من تهديد ذكي؛ أي فعل ذكي هو محاولة متعمدة (خاصة بمعنى طريقة أو تقنية) للتهرب من الخدمات الأمنية وانتهاك السياسة الأمنية للنظام))

Risk: an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with particular result.

((المخاطرة: توقع للخسارة يتم التعبير عنه على أنه احتمال أن يستغل تهديد معين نقطة ضعف معينة مع نتيجة معينة))

Security policy: a set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

((سياسة الأمان: مجموعة من القواعد والممارسات التي تحدد أو تنظم كيفية قيام نظام أو مؤسسة بتقديم خدمات أمنية لحماية موارد النظام الحساسة والحاسمة))

System resource(asset): data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., system component—hardware, firmware, software, or documentation); or a facility that houses system operations equipment.

((موارد النظام (الأصول): البيانات الواردة في نظام المعلومات؛ أو خدمة يقدمها نظام؛ أو قدرة النظام، مثل قدرة المعالجة أو عرض النطاق الترددي للاتصالات؛ أو عنصر من معدات النظام (على سبيل المثال، مكون النظام - الأجهزة أو البرامج الثابتة أو البرامج أو الوثائق)؛ أو منشأة تحتوي على معدات عمليات النظام))

Threat: a potential for security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

((**التهديد:** احتمال للأمن، وهو موجود عندما يكون هناك ظرف أو قدرة أو فعل أو حدث يمكن أن ينتهك الأمن ويسبب ضررًا. أي أن التهديد هو خطر محتمل قد يستغل إحدى نقاط الضعف))

Vulnerability: a flaw or weakness in a system's design, or operation and management that could be exploited to violate the system security policy.

((**الثغرات الأمنية:** عيب أو ضعف في تصميم النظام، أو التشغيل والإدارة التي يمكن استغلالها لانتهاك سياسة أمان النظام))

((Vulnerbilities,thereats And attacks))

Categories of vulnerabilities:

- Corrupted (loss of integrity)
- Leaky (loss of confidentiality)
- Unavailable or very slow (loss of availability)

Threats:

- Capable of exploiting vulnerabilities
- Represent potential security harm to an asset

Attacks (threats carried out):

- Passive – attempt to learn or make use of information from the system that does not affect system resources
- Active – attempt to alter system resources or affect their operation
- Insider – initiated by an entity inside the security parameter
- Outsider – initiated from outside the perimeter

ATTACKS

• Inside attack: Initiated by an entity inside the security perimeter (an “insider”). The insider is authorized to access system resources but uses them in a way not approved by those who granted the authorization.

(الهجوم الداخلي: بدأه كيان داخل المحيط الأمني ("المطلع"). يحق للمُطّلع من الداخل الوصول إلى موارد النظام ولكنه يستخدمها بطريقة لم يوافق عليها أولئك الذين منحوا التفويض.)

• Outside attack: Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an “outsider”). On the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

(الهجوم الخارجي: بدأ من خارج المحيط، بواسطة مستخدم غير مصرح له أو غير شرعي للنظام ("خارجي"). على الإنترنت، يتراوح المهاجمون الخارجيون المحتملون من المخادعين الهواة إلى المجرمين المنظمين والإرهابيين الدوليين والحكومات المعادية.
)

Passive and active attack

Passive attack:

- Attempts to learn or make use of information from the system but does not affect system resources

  (محاولات التعلم أو الاستفادة من المعلومات من النظام ولكنها لا تؤثر على موارد النظام.

- Eavesdropping on, or monitoring of, transmissions

  (التنصت على الإرسال أو مراقبته).

- Goal of attacker is to obtain information that is being transmitted

(• هدف المهاجم هو الحصول على المعلومات التي يتم نقلها).

- Two types:

Release of message contents

Traffic analysis

Active attack:

- Attempts to alter system resources or affect their operation

(• محاولات لتغيير موارد النظام أو التأثير على تشغيلها).

- Involve some modification of the data stream or the creation of a false stream

(• قم بإدخال بعض التعديلات على تدفق البيانات أو إنشاء تدفق زائف).

- Four categories:

Replay

Masquerade

Modification of messages

Denial of service

Symmetric encreption

- The universal technique for providing confidentiality for transmitted or stored data

(التقنية العالمية لتوفير السرية للبيانات المرسلة أو المخزنة)

- Also referred to as conventional encryption or single-key encryption

(التقنية العالمية لتوفير السرية للبيانات المرسلة أو المخزنة)

- Two requirements for secure use:
  - Need a strong encryption algorithm

    (تحتاج الى خوارزمية للتشفير)
  - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure

    (يجب أن يكون المرسل والمتلقي قد حصلوا على نسخ من المفتاح السري
    بطريقة آمنة ويجب أن يحافظوا على تأمين المفتاح)

Plaintext: This is the original message or data that is fed into the algorithm as input.

(**الرسالة الاصلية:** وهي الرسالة الغير مشفرة التي يتم ارسالها من المرسل).

Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

(**خوارزمية التشفير:** هي العمليات التي يتم استعمالها لعميلة التشفير)

Secret key: The secret key is also input to the encryption algorithm. The exact substitutions and transformations performed by the algorithm depend on the key

(**المفتاح:** وهو أيضا يكون مدخل للعملية التشفيرية مع الرسالة الاصلية).

Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.

(**الرسالة المشفرة:** وهي الرسالة الناتجة عن عملية التشفير وتتم ببعض العمليات بين الرسالة الاصلية والمفتاح).

Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

(فك التشفير: وهي العملية العكسية لعملية التشفير حيث تتم بنفس العمليات باستعمال نفس الأمور لكن بطريقة معاكسة).

Attacking Symmetric Encryption

Cryptanalytic attacks:

- Rely on:
  - Nature of the algorithm. (طبيعة الخوارزمية)
  - Some knowledge of the general characteristics of the plaintext. (بعض المعرفة بالخصائص العامة للنص الاصلي)
  - Some sample plaintext-ciphertext pairs

    (بعض النصوص المشفرة)
- Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used

  (يستغل خصائص الخوارزمية لمحاولة استنتاج نص عادي محدد أو المفتاح المستخدم)

  If successful, all future and past messages encrypted with that key are compromised

Symmetric Block Encryption Algorithms

The most used symmetric encryption algorithms are block ciphers.

(أكثر خوارزميات التشفير المتماثل استخدامًا هي الأصفار الكتلية).

A block cipher processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block.

(يعالج تشفير الكتلة إدخال النص العادي في كتل ذات حجم ثابت وينتج كتلة من نص مشفر متساوي الحجم لكل كتلة نص عادي).

The algorithm processes longer plaintext amounts as a series of fixed-size blocks.

(تعالج الخوارزمية كميات نص عادي أطول كسلسلة من الكتل ذات الحجم الثابت).

The most important symmetric algorithms, all of which are block ciphers, are the Data Encryption Standard (DES), triple DES, and the Advanced Encryption Standard (AES).

(أهم الخوارزميات المتماثلة، وجميعها عبارة عن أصفار كتلة، هي

(معيار تشفير البيانات DES) (وثلاثي DES)

(ومعيار التشفير المتقدم AES))

Block cipher

Processes the input one block of element at the time.

(يعالج إدخال كتلة واحدة من العنصر في ذلك الوقت).

Produces an output block for each input block.

(ينتج كتلة إخراج لكل كتلة إدخال)

Can reuse key.

(تستطيع إعادة استخدام المفتاح).

More common. (مشترك أكثر)

Stream cipher

Processes the input elements continusly.

(يعالج عناصر الإدخال بشكل مستمر).

Processes output one element at time.

(تنتج العمليات عنصرًا واحدًا في كل مرة).

Primary advantage that they are almost always faster and use for less code.

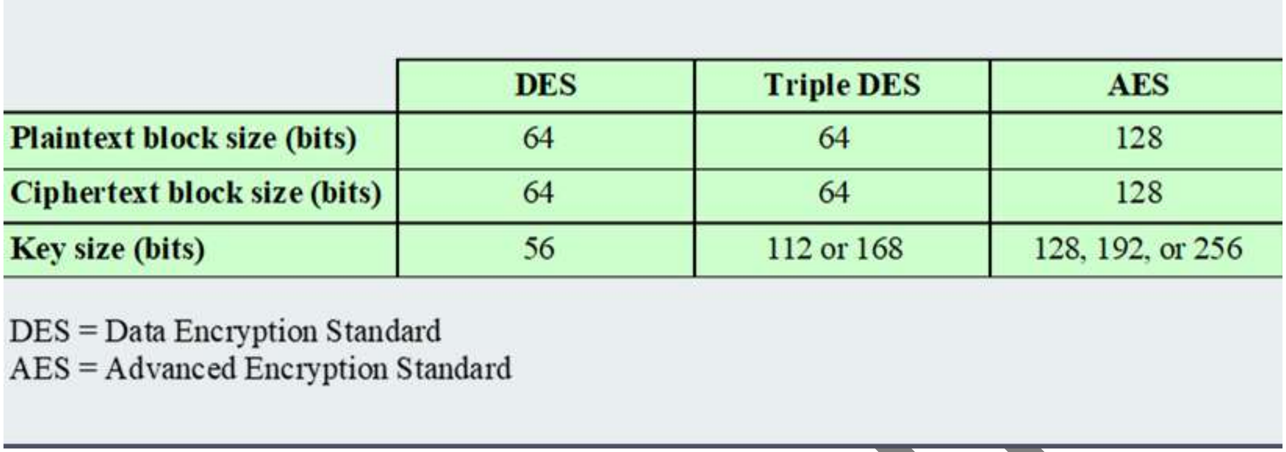
(الميزة الأساسية أنها دائمًا ما تكون أسرع وتستخدم لرمز أقل).

Encrypts plaintext one byte at time.

(يشفر نص عادي بايت واحد في كل مرة)

Pseudorandom stream is one that is unpredictable without knowledge of the input key.

(الدفق العشوائي الزائف هو الذي لا يمكن التنبؤ به دون معرفة مفتاح الإدخال).



	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

Feistel Cipher Structure

- ***The inputs to the encryption algorithm are a plaintext block of length 2w bits and a key K.***
- ***The plaintext block is divided into two halves, L0 and R0.***
- ***The two halves of the data pass through n rounds of processing and then combine to produce the ciphertext block.***
- ***Each round i has as inputs Li-1 and Ri-1, derived from the previous round, as well as a subkey Ki, derived from the overall K.***
- ***In general, the subkeys Ki are different from K and from each other and are generated from the key by a subkey generation algorithm.***
- ***All rounds have the same structure.***
- ***A substitution is performed on the left half of the data.***

- ***This is done by applying a round function F to the right half of the data and then taking the exclusive-OR (XOR) of the output of that function and the left half of the data.***
- ***The round function has the same general structure for each round but is parameterized by the round subkey Ki.***
-

Following this substitution, a permutation is performed that consists of the interchange of the two halves of the data.

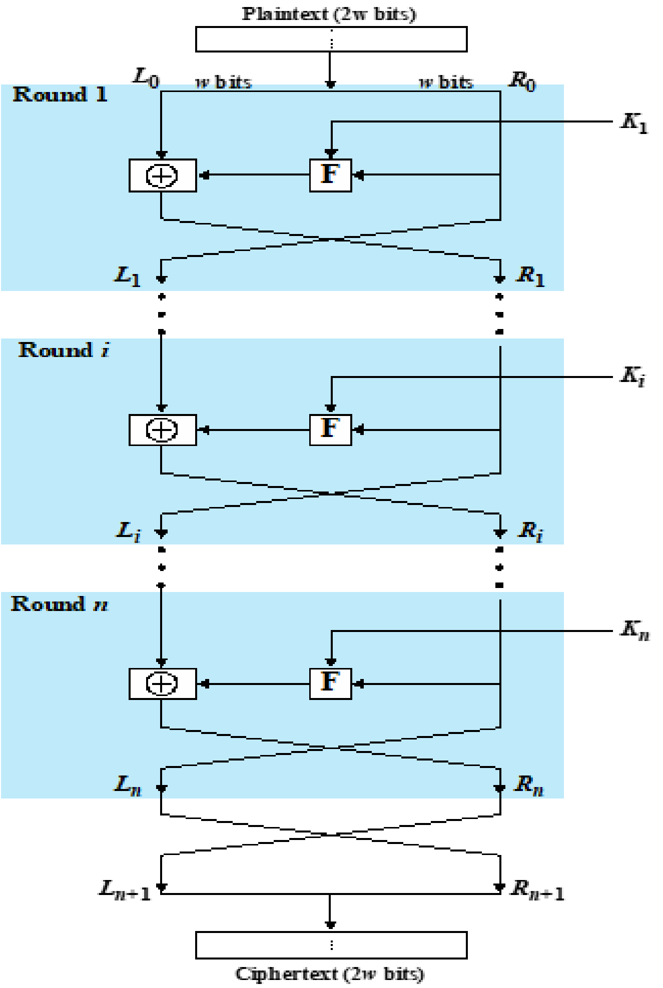


Figure 20.1 Classical Feistel Network

DES

- The most used symmetric encryption algorithms are block ciphers. A block cipher processes the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block.
- The plaintext is 64 bits in length and the key is 56 bits in length; longer plaintext amounts are processed in 64-bit blocks.
- The DES structure is a minor variation of the Feistel.
- There are 16 rounds of processing. From the original 56-bit key, 16 subkeys are generated, one of which is used for each round.
- The process of decryption with DES is essentially the same as the encryption process.
- The rule is as follows: Use the ciphertext as input to the DES algorithm, but use the subkeys *Ki* in reverse order.

That is, use K16 on the first iteration, K15 on the second iteration, and so on until K1 is used on the sixteenth and last iteration.

DES has two part:

1- key round generation algorithm: where 16 subkey (K1…..K16) each sub key has 48 bit will be generated from the original key (64 bit) as a key for each round.

2- plaintext encryption algorithm: message of 64 bits will go through 16 rounds to produce ciphertext of 64 bits.

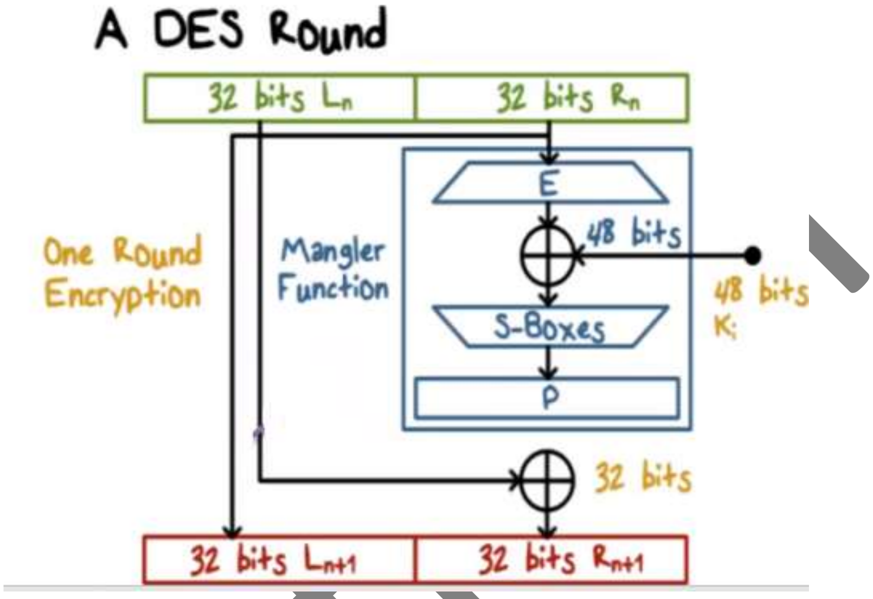
key round generation algorithm

- The key (k) has 64 bits
- Converted to binary
- This algorithm has five steps:
- 1- permutation choice1 (PC1) for the K to generate permutated key (kp) has 56 bits by excluding the parity check bits
- 2- dividing the kp into two equal parts C0 and D0 each part has 28 bits.
- 3- Left circular shift (16 times) to generate (C1 and D1), (C2 and D2),…..(C16 and D16)
- 4- concatenate the two parts C and D as C0D0, C1D1…C16D16 to generate 16 subkey (56 bits)
- 5- permutation choice 2 (PC2) to generate 16 round key K1, K2…k16 each one has 48 bits.

DES Message encryption

- Block data 64 bit
- Initial permutation (IP)
- Divide into two equal parts L0 and R0 each part has 32 bit
- Expansion permutation on R0 (32 bit) to produce E(R0) 48 bit
- K1 XOR E(R0)
- Enter each the 8 blocks (Bn 6bits) of R0 (48 bits) into s-box as Sn(Bn) =4 bits to produce S1(B1)…S8(B8)=32 bit
- Swap R16 and L16

- Concatenate (inverse) R16 L16
- Apply inverse permutation IP-1 on the concatenation R16 L16 to produce the ciphertext



location of Symmetric encryption Devices

we need to decide what to encrypt and where the encryption gear should be located. There are two fundamental alternatives:

link encryption and end-to-end encryption; these are illustrated in use over a frame network in Figure

link encryption

- With link encryption, each vulnerable communications link is equipped on both ends with an encryption device.
- Thus, all traffic over all communications links is secured.
- Although this requires a lot of encryption devices in a large network,
- it provides a high level of security.
- One disadvantage of this approach is that the message must be decrypted each time it enters a frame switch; this is necessary because
  the switch must read the address (connection identifier) in the frame header to route the frame.
- Thus, the message is vulnerable at each switch.

If this is a public frame-relay network, the user has no control over the security of the nodes.

end-to-end encryption

- 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.
- The destination shares a key with the source and so is able to decrypt the data.

- This approach would seem to secure the transmission against attacks on the network links or switches.
- There is, however, still a weak spot.
- Consider the following situation. A host connects to a frame relay network, sets up a logical data link connection to another host, and is prepared to transfer data to that other host using end-to-end encryption.
- Data are transmitted over such a network in the form of frames, consisting of a header and some user data.
- What part of each frame will the host encrypt? Suppose that the host encrypts the entire frame, including the header. This will not work because, remember, only the other host can perform the decryption.
- The frame relay node will receive an encrypted frame and be unable to read the header.
- Therefore, it will not be able to route the frame.

It follows that the host may only encrypt the user data portion of the frame and must leave the header in the clear, so that it can be read by the network.

- Thus, with end-to-end encryption, the user data are secure. However, the traffic pattern is not, because frame headers are transmitted in the clear.
- To achieve greater security, both link and end-to-end encryption are needed, as shown in Figure.

- To summarize, when both forms are employed, the host encrypts the user data
  portion of a frame using an end-to-end encryption key.
- The entire frame is then encrypted using a link encryption key.
- As the frame traverses the network, each switch decrypts the frame using a link encryption key to read the header and then encrypts the entire frame again for sending it out on the next link.

Now the entire frame is secure except for the time that the frame is actually in the memory of a frame switch, at which time the frame header is in the clear

Key distribution

- For symmetric encryption to work, the two parties to an exchange must share the
  same key, and that key must be protected from access by others.
- Furthermore, frequent key changes are usually desirable to limit the amount of data compromised if an attacker learns the key.
- Therefore, the strength of any cryptographic system rests with the key distribution technique,
- a term that refers to the means of delivering a key to two parties that wish to exchange data, without allowing others to see the key.
- Key distribution can be achieved in a number of ways.
- For two parties A and B:

1. A key could be selected by A and physically delivered to B.

2. A third party could select the key and physically deliver it to A and B.

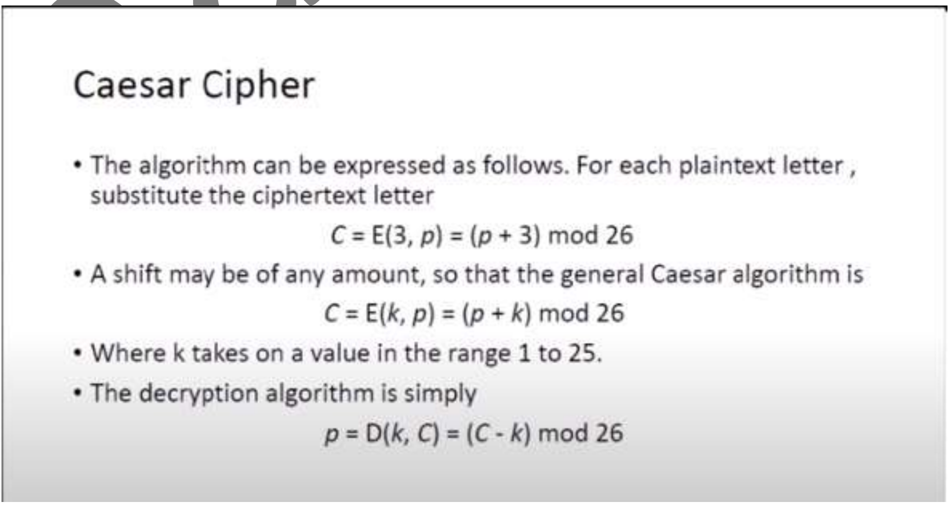
3. If A and B have previously and recently used a key, one party could transmit the new key to the other, encrypted using the old key.

4. If A and B each have an encrypted connection to a third-party C, C could deliver a key on the encrypted links to A and B.

Classical Substitution Ciphers

• Substitution
 Where letters of plaintext are replaced by other
letters, or numbers, or symbols

• Transposition
 The plaintext is encrypted by changing the
positions of the letters and/or symbols, by some
sort of permutation



Caesar Cipher

- The algorithm can be expressed as follows. For each plaintext letter , substitute the ciphertext letter

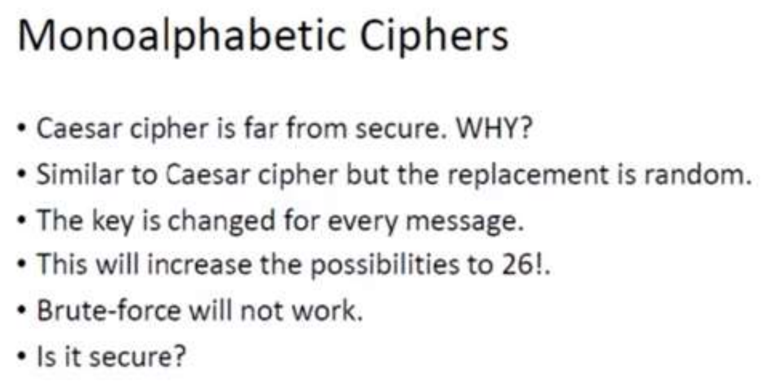
$$C = \mathrm{E}(3, p) = (p + 3) \bmod 26$$

- A shift may be of any amount, so that the general Caesar algorithm is

$$C = \mathrm{E}(k, p) = (p + k) \bmod 26$$

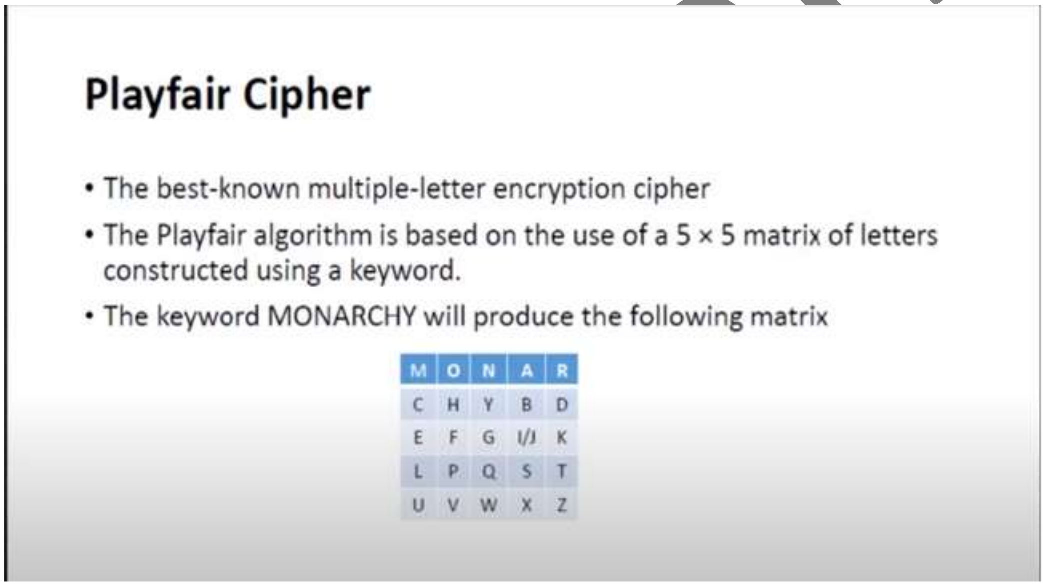
- Where k takes on a value in the range 1 to 25.
- The decryption algorithm is simply

$$p = \mathrm{D}(k, C) = (C - k) \bmod 26$$



Monoalphabetic Ciphers

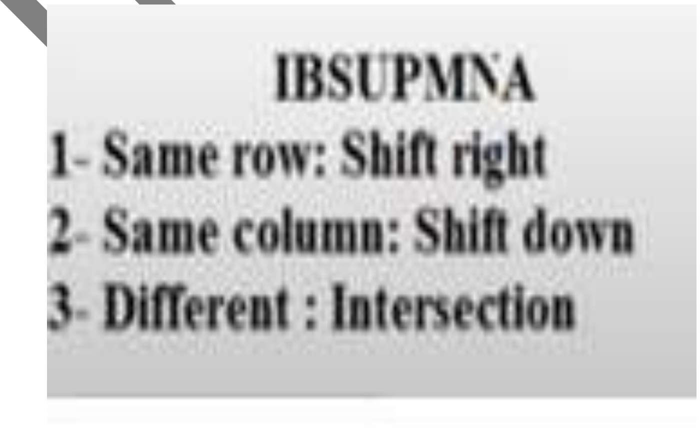
- Caesar cipher is far from secure. WHY?
- Similar to Caesar cipher but the replacement is random.
- The key is changed for every message.
- This will increase the possibilities to 26!.
- Brute-force will not work.
- Is it secure?



Playfair Cipher

- The best-known multiple-letter encryption cipher
- The Playfair algorithm is based on the use of a 5 × 5 matrix of letters constructed using a keyword.
- The keyword MONARCHY will produce the following matrix

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

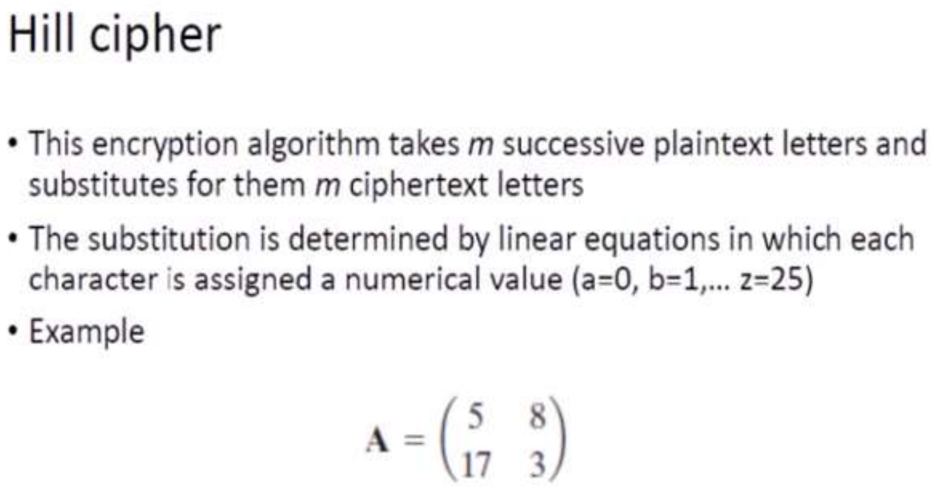


IBSUPMNA

1- Same row: Shift right

2- Same column: Shift down

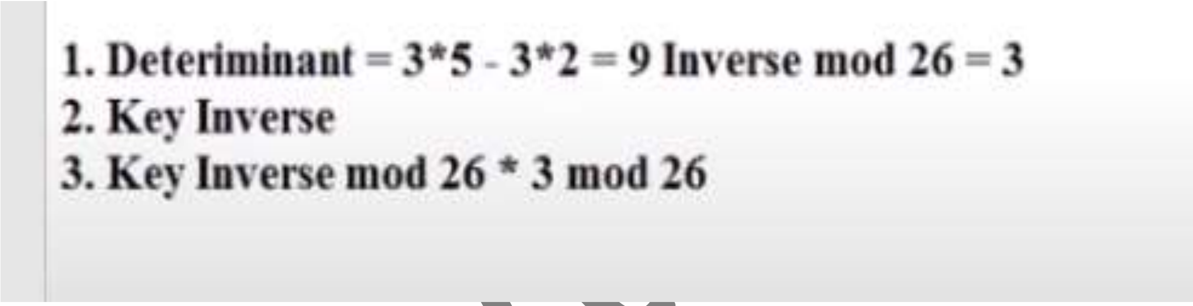
3- Different : Intersection



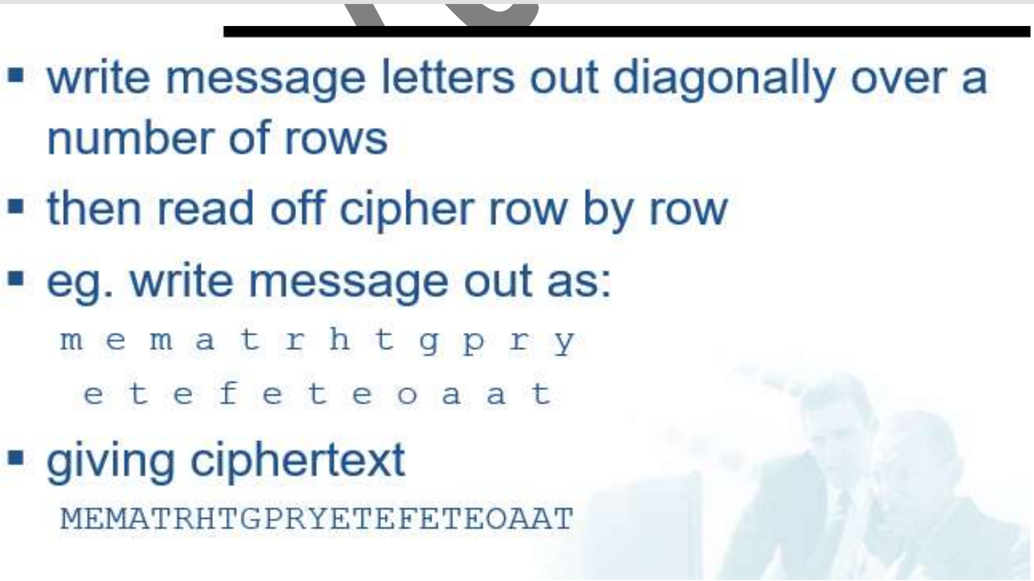
Hill cipher

- This encryption algorithm takes *m* successive plaintext letters and substitutes for them *m* ciphertext letters
- The substitution is determined by linear equations in which each character is assigned a numerical value (a=0, b=1,... z=25)
- Example

$$\mathbf{A} = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$$



1. **Deteriminant = 3*5 - 3*2 = 9 Inverse mod 26 = 3**
2. **Key Inverse**
3. **Key Inverse mod 26 * 3 mod 26**

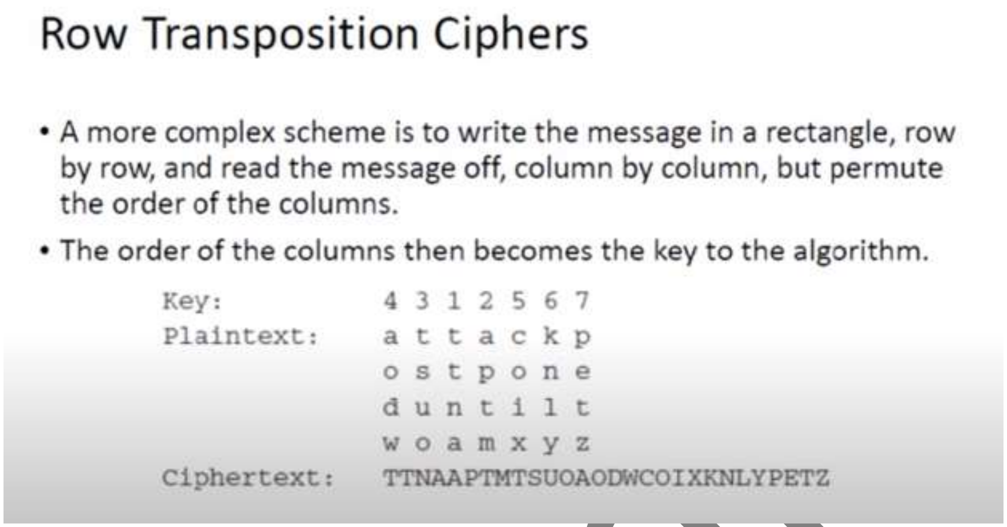


- write message letters out diagonally over a number of rows
- then read off cipher row by row
- eg. write message out as:

```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

- giving ciphertext

```
MEMATRHTGPRYETEFETEOAAT
```



Row Transposition Ciphers

- A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.
- The order of the columns then becomes the key to the algorithm.

```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Public key

probably most significant advance in the 3000 year history of cryptography

uses **two** keys – a public & a private key

asymmetric since parties are **not** equal

uses clever application of number theoretic concepts to function

complements **rather than** replaces private key crypto

public-key/two-key/asymmetric cryptography involves the use of **two** keys:

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

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

is **asymmetric** because

those who encrypt messages or verify signatures **cannot** decrypt messages or create signatures

Why Public-Key Cryptography?

developed to address two key issues:

key distribution – how to have secure communications in general without having to trust a KDC with your key

digital signatures – how to verify a message comes intact from the claimed sender

public invention due to Whitfield Diffie & Martin Hellman at Stanford Uni in 1976

Public-Key Characteristics

- Public-Key algorithms rely on two keys with the characteristics that it is:
  - computationally infeasible to find decryption key knowing only algorithm & encryption key
  - computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known
  - either of the two related keys can be used for encryption, with the other used for decryption (in some schemes)

Security of Public Key Schemes

like private key schemes brute force **exhaustive search** attack is always theoretically possible

but keys used are too large (>512bits)

security relies on a **large enough** difference in difficulty between **easy** (en/decrypt) and **hard** (cryptanalyse) problems

more generally the **hard** problem is known, its just made too hard to do in practise

requires the use of **very large numbers**

hence is **slow** compared to private key schemes

Number of used keys: just two does not matter the number of involved users but symmetric needs more since each two users need their own private keys

Public-Key Applications:

can classify uses into 3 categories:

encryption/decryption (provide secrecy)

digital signatures (provide authentication)

key exchange (of session keys)

some algorithms are suitable for all uses, others are specific to one

RSA

by Rivest, Shamir & Adleman of MIT in 1977

best known & widely used public-key scheme

based on exponentiation in a finite (Galois) field over integers modulo a prime

nb. exponentiation takes $O((\log n)^3)$ operations (easy)

uses large integers (eg. 1024 bits)

security due to cost of factoring large numbers

nb. factorization takes $O(e^{\log n \log \log n})$ operations (hard)

each user generates a public/private key pair by:

selecting two large primes at random - p, q

computing their system modulus N=p.q

note ø(N)=(p-1)(q-1)

selecting at random the encryption key e

where 1<e<ø(N), gcd(e,ø(N))=1

solve following equation to find decryption key d

$e.d=1 \bmod \o(N)$ and $0 \le d \le N$

(what is the number if multiplied by e the product will divide ø(N) and remainder=1)

publish their public encryption key: KU={e,N}

keep secret private decryption key: KR={d,p,q}

1. gcd $(e,\Phi)=(47,152)$
2. $152 \bmod 47 = 11$
3. $47 \bmod 11 = 3$
4. $11 \bmod 3 =2$
5. $3 \bmod 2 =1$
6. $\gcd(47,152)=1$, or
7. $\gcd(152,47)= 152/47=47/11=11/3=3/2=1$

Key Distribution

Proposed in 1979 (Diffie, Hellman, and Merkle)
§ **A** generates a new temporary pair of public/private keys

§ **A** sends **B** the public key and his identity

§ **B** generates a session key **K,** encrypts it using the supplied
public key, and then sends the encrypted key to **A**

§ **A** decrypts the ciphertext using the private key, and gets the key **K**

A public-key distribution scheme can help to establish a common key known only to the two participants

Diffie-Hellman scheme of key exchange

§ Key exchange is implemented by operations over a finite

field (or called Galois field)

§ Security relies on the difficulty of computing ***discrete logarithms*** (similar to factoring)

– It is hard

MAC

Generated by an algorithm that creates a small fixed sized block

§ Depending on both message and a key

§ Like encryption (though need not be reversible)

• Appended to message, which is called a MAC

• Receiver performs same computation on message and checks whether it matches the MAC

• Provides assurance that message is unaltered and comes from sender

Hash Functions:

- To condense arbitrary message to fixed size
- Hash functions can be public and not keyed
- Hash functions are used

- to detect changes to message, and

- to authenticate identity, etc.

- Usually used with other techniques (such as, digital signature)