CRYPTOGRAPHY

Annu James

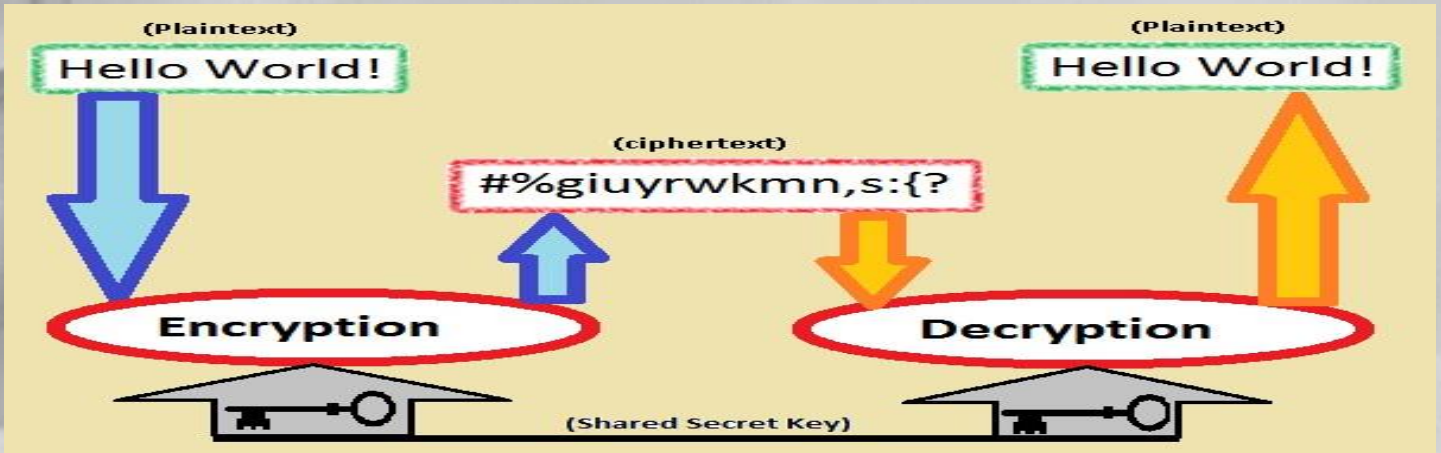
- Security has become a crucial issue in industry, business etc. due to the rapid growth of digital communication.
- One essential aspect for secure communications is

  “ CRYPTOGRAPHY “ means secret writing
- It provides essential techniques for securing information and protecting data.
- The classic cryptography deals with problem of secure communication.
- Modern cryptography deals with all adversarial threats facing parties who wish to carry some task in a network.
- The main aim is to provide secure solutions to a set of parties who wish to carry out a distributed task.

WHAT IS CRYPTOGRAPHY ?

- **Cryptography** is the practice and study of techniques for secure communication in the presence of third parties called adversaries.
- It is the science of using mathematics to encrypt and decrypt data.
- It enables us to store sensitive information or transmit it across insecure networks.
- It cannot be read by anyone except the intended recipient.
- It is constructing and analyzing protocols that overcome the influence of adversaries.
- They are related to various aspects in information security.
- Application of cryptography include ATM cards, computer passwords, and electronic commerce.
- The conversion of information from a readable state to apparent nonsense which means the content is non-understandable.
- The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients.

- Modern cryptography is heavily based on mathematical theory and computer science practice.
- Cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.
- Schemes are therefore termed computationally secure and theoretical advances,
- Improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted.



CRYPTOGRAPHY COMPONENTS

1. **Cryptography :-**

   Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

2. **Plaintext and Ciphertext :-**

- The original message, before being transformed, is called plaintext.
- After the message is transformed, it is called ciphertext.
- An encryption algorithm transforms the plaintext into ciphertext; a decryption algorithm transforms the ciphertext back into plaintext.

3. **Cipher :-**

- Here encryption and decryption algorithms is referred as ciphers.
- The term cipher is also used to refer to different categories of algorithms in cryptography.

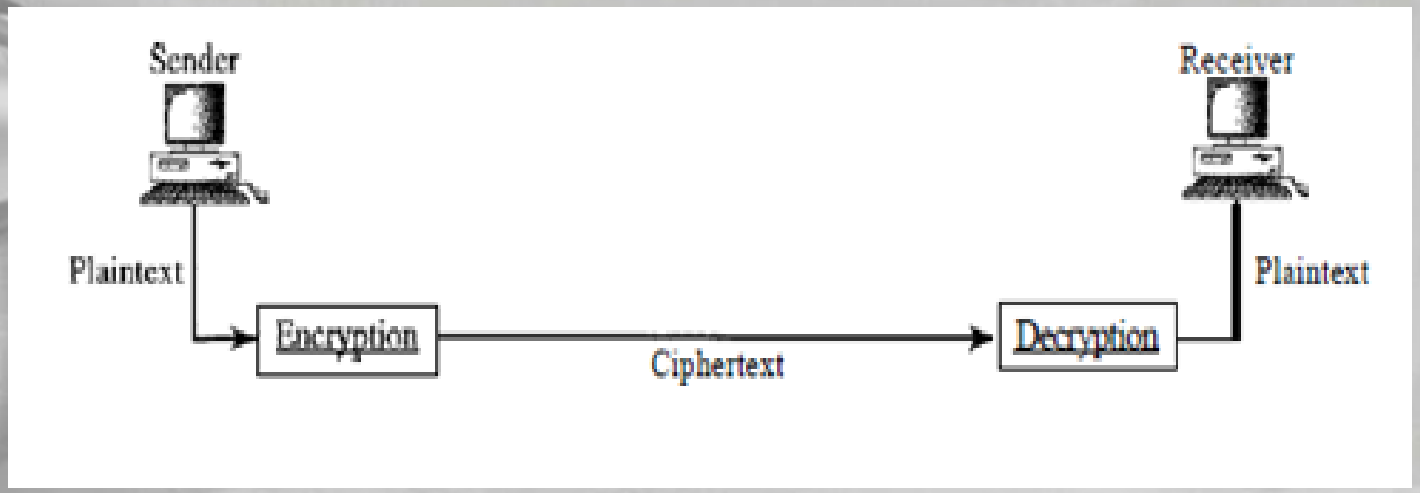
4. **KEY :-**

- A key is a number that the cipher, as an algorithm, operates on.
- To encrypt a message, we need an encryption algorithm, an encryption key, and the plaintext.

5. Alice, Bob, Eve :-

In cryptography, three characters are used in an information exchange scenario; they are Alice, Bob, and Eve.

- Alice - person who needs to send secure data.
- Bob - recipient of the data.
- Eve - person who somehow disturbs the communication between Alice and Bob by intercepting messages to uncover the data or by sending her own disguised messages.



Types of Cryptography :-

The Cryptography algorithm (ciphers)are mainly divided into two groups :- symmetric key (secret-key) cryptography algorithms and asymmetric (public-key) cryptography algorithms.

- **Symmetric-key Cryptography :-**

- In symmetric-key cryptography, the same key is used by both parties.
- The sender uses the key for an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.
- In symmetric·key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption).
- The key is shared.

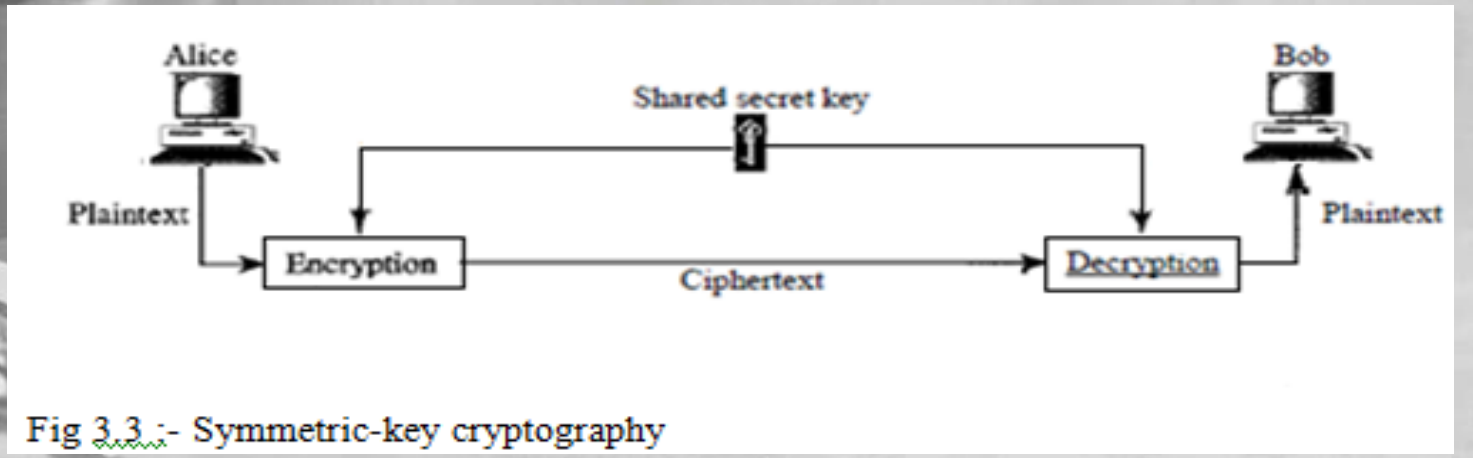


Fig 3.3 :- Symmetric-key cryptography

- **Asymmetric-key Cryptography :-**

- In asymmetric or public-key cryptography, there are two keys: a private key and a public key.
- The private key is kept by the receiver. The public key is announced to the public.
- In public-key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption.
- The public key is available to the public; the private key is available only to an individual.

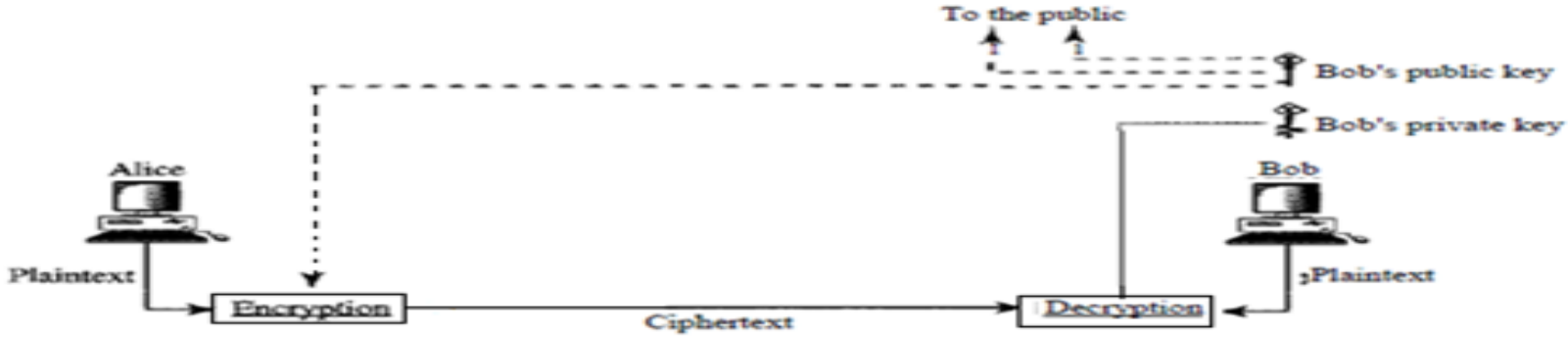
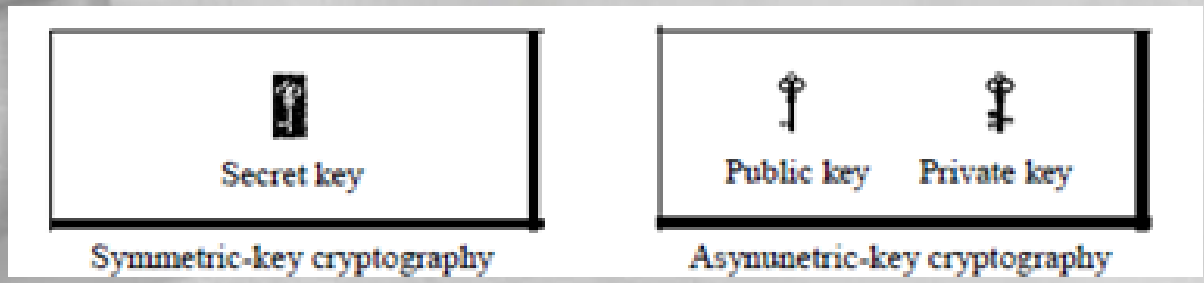


Fig 3.4 :- Asymmetric-key cryptography

Three types of keys :-

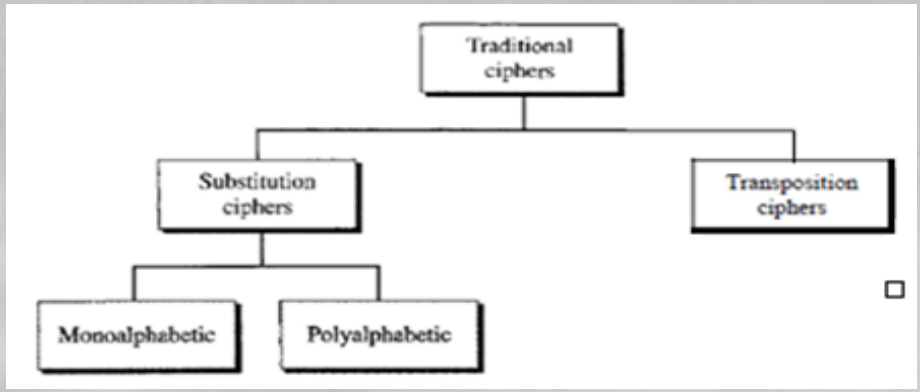
- There are three types of keys involved in cryptography and they are the secret key , the public key and the private key.
- The first, the secret key, is the shared key used in symmetric-key cryptography.
- The second and the third are the public and private keys used in asymmetric-key cryptography.



SYMMETRIC-KEY CRYPTOGRPHY

- The symmetric-key cryptography is mainly used in our network security.
- Today's ciphers are much more complex.

  Traditional algorithms is discussed first, which are character-oriented and secondly modern ones are discussed which are bit-oriented.



- **Traditional Ciphers :-**

->Traditional ciphers are introduced which are character-oriented.

->Traditional symmetric-key ciphers are mainly divided into two categories , substitution ciphers and transposition ciphers.

- **Substitution Cipher :-**

-> A substitution cipher substitutes one symbol with another.

-> If the symbols in the plaintext are alphabetic characters, we replace one character with another.

Eg :- We can replace character A with D, and character T with Z. If the symbols are digits (0 to 9), we can replace 3 with 7, and 2 with 6.

-> Substitution ciphers can be categorized as either monoalphabetic or polyalphabetic ciphers.

❖ **Monoalphabetic Cipher :-**

-> A character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position in the text.

Eg :- If the algorithm says that character A in the plaintext is changed to character D, every character A is changed to character D.

-> The relationship between characters in the plaintext and the ciphertext is a one-to-one relationship.

❖ **Polyalphabetic Cipher** :-

-> Each occurrence of a character can have a different substitute.

->The relationship between a character in the plaintext to a character in the ciphertext is a one-to-many relationship.

Eg :- Character A could be changed to D in the beginning of the text, but it could be changed to N at the middle.

-> If the relationship between plaintext characters and ciphertext characters is one-to many, the key must tell us which of the many possible characters can be chosen for encryption.

->To achieve this goal, we need to divide the text into groups of characters and use a set of keys.

Eg :- We can divide the text "THISISANEASYTASK" into groups of 3 characters and then apply the encryption using a set of 3 keys.

We then repeat the procedure for the next 3 characters.

Shift Cipher :- The simplest monoalphabetic cipher is probably the shift cipher.

-> It is assumed that the plaintext and ciphertext consist of uppercase letters (A to Z) only.

-> In this cipher, the encryption algorithm is "shift key characters down," with key equal to some number and the decryption algorithm is "shift key characters up."

Eg :- If the key is 5, the encryption algorithm is "shift 5 characters down" (toward the end of the alphabet), the decryption algorithm is "shift 5 characters up" (toward the beginning of the alphabet).

If the end or beginning of the alphabet is reached, it is wrap around.

-> The shift cipher is sometimes referred to as the **Caesar cipher**.

- **Alphabet**
- **ABCD……..XYZ**
- Cipher
- DEFG……..ABC

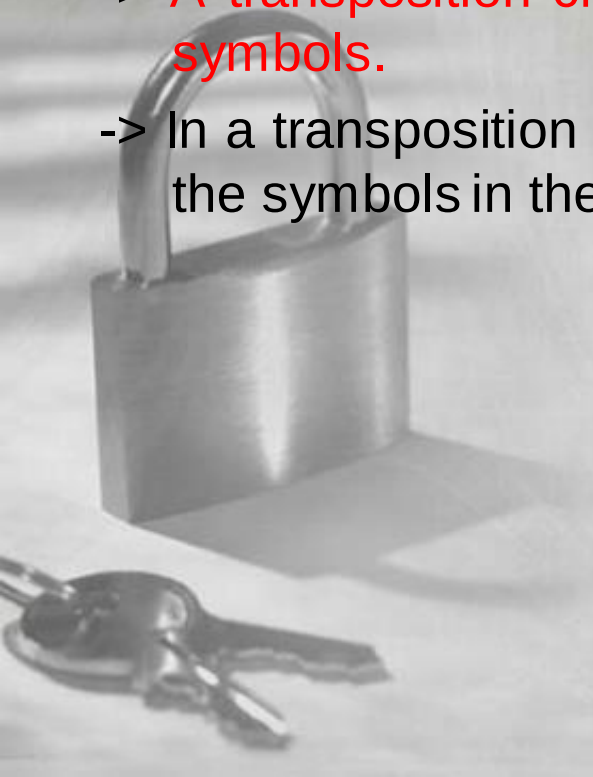
- **Transpostion Cipher :-**

-> In a transposition cipher, there is no substitution of characters; instead, their locations change.

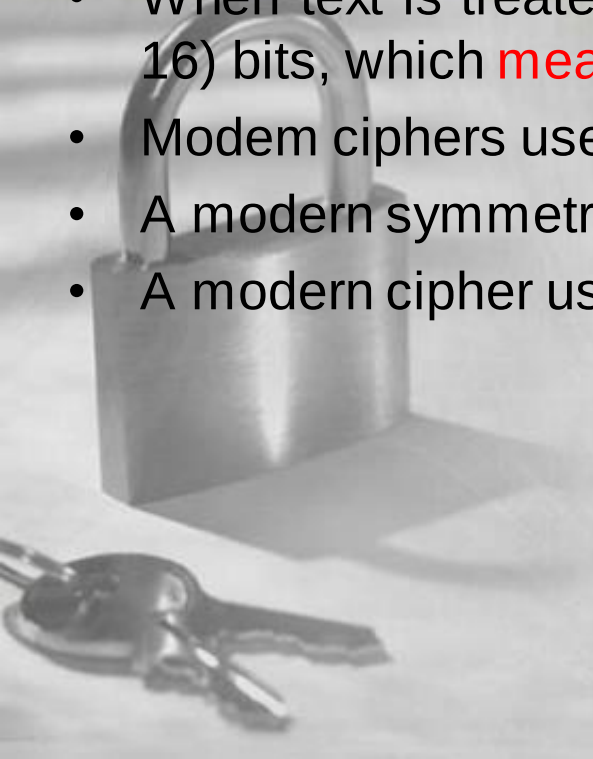
-> A character in the first position of the plaintext may appear in the tenth position of the ciphertext. A character in the eighth position may appear in the first position.

-> A transposition cipher reorders (permutes) the symbols in a block of symbols.

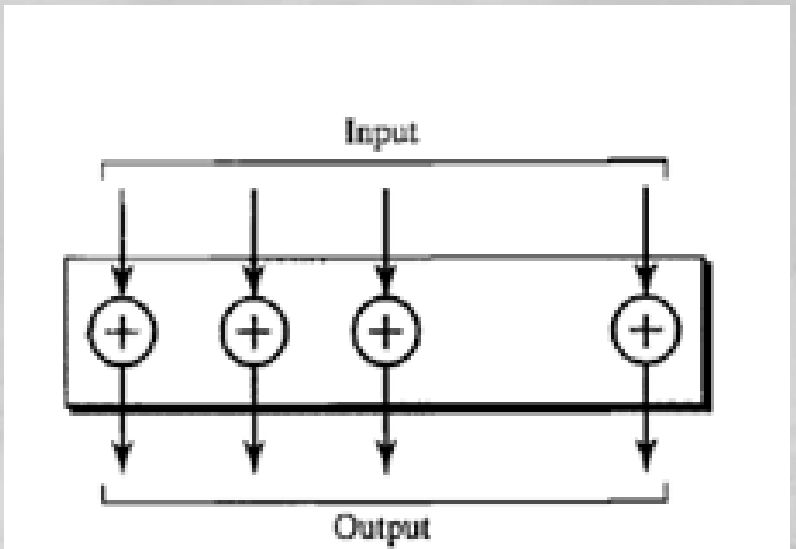
-> In a transposition cipher, the key is a mapping between the position of the symbols in the plaintext and cipher text.



- **Simple modern Ciphers :-**
- With the advent of the computer, ciphers need to be bit-oriented.
- This is because the information to be encrypted is not just text; it can also consist of numbers, graphics, audio, and video data.
- It is convenient to convert these types of data into a stream of bits, encrypt the stream, and then send the encrypted stream.
- When text is treated at the bit level, each character is replaced by 8 (or 16) bits, which means the number of symbols becomes 8 (or 16).
- Modem ciphers use a different strategy than the traditional ones.
- A modern symmetric cipher is a combination of simple ciphers.
- A modern cipher uses several simple ciphers to achieve its goal.

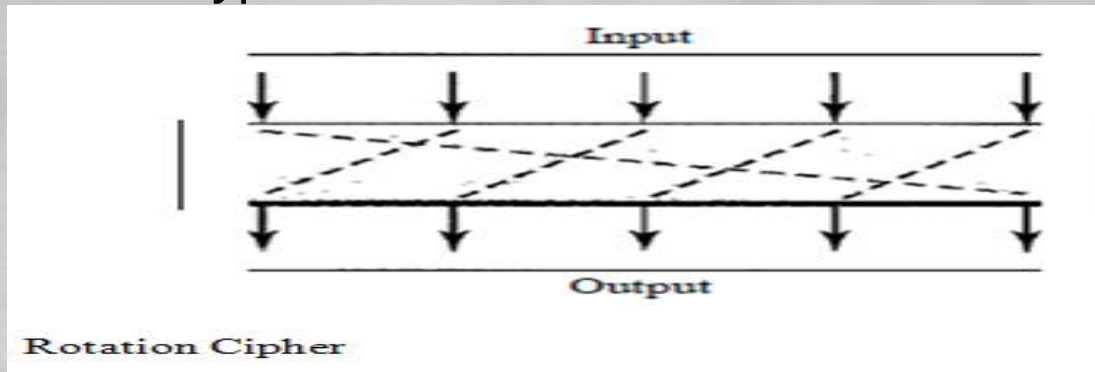


- **XOR Cipher :-**
- Modern ciphers are made of a set of **simple ciphers.**
- They are simple predefined functions in mathematics or computer science.
- The first one discussed here is called the **XOR cipher.**
- Its because uses the exclusive-or operation as defined in computer science.
- An XOR operation needs two data inputs plaintext.
- One of the inputs is the block to be the encrypted, the other input is a key; the result is the encrypted block.
- In an XOR cipher, the size of the key, the plaintext, and the ciphertext are all the same.
- XOR ciphers have a very interesting property: the encryption and decryption are the same.



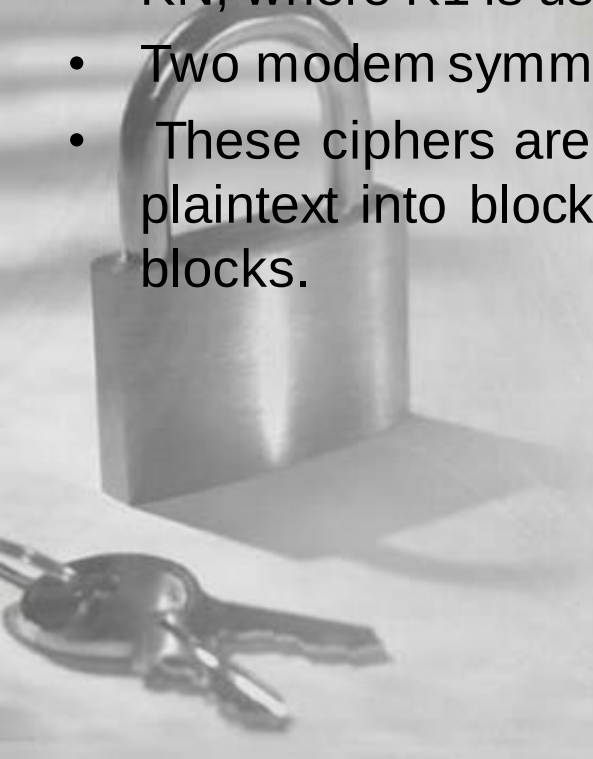
- **Rotation Cipher**
- In rotation cipher, the input bits are rotated to the left or right. The rotation cipher can be keyed or keyless.
- In keyed rotation, the value of the key defines the number of rotations; in keyless rotation the number of rotations is fixed.
- The rotation cipher can be considered a special case of the transpositional cipher using bits instead of characters.
- The rotation cipher has an interesting property that if the length of the original stream is N, after N rotations, we get the original input stream.
- This means that it is useless to apply more than N - 1 rotations.
- The number of rotations must be between 1 and N-1
- The decryption algorithm for the rotation cipher uses the same key and the opposite rotation direction.

  If a right rotation is used in the encryption, a left rotation is used in a decryption and vice versa.

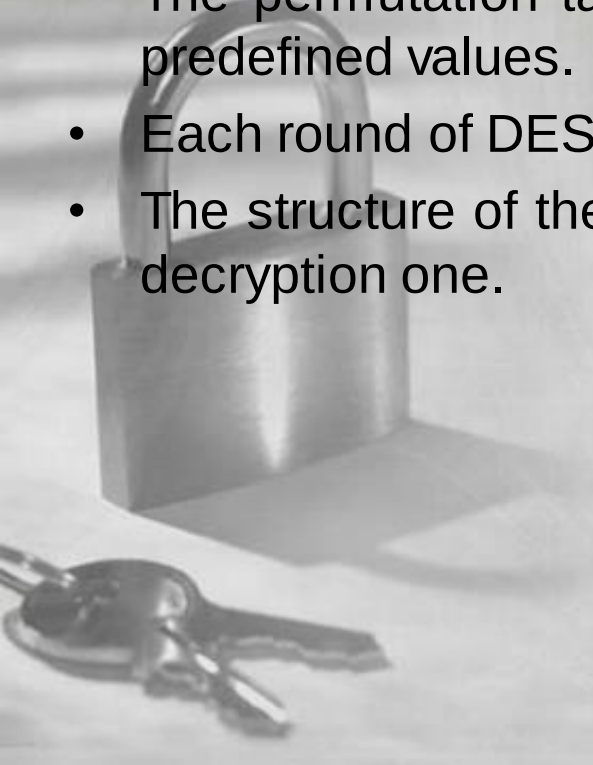


Rotation Cipher

- **Modern Round Ciphers**
- **Round ciphers** involve multiple **rounds,** where each round is a complex cipher made up of the simple ciphers that are previously described.
- The key used in each round is a subset or variation of the general key called the round key.
- If the cipher has N rounds, a key generator produces N keys, K1, K2, ..., KN, where K1 is used in round 1, K2 in round 2, and so on.
- Two modem symmetric-key ciphers are introduced here : DES and AES.
- These ciphers are referred to as block ciphers because they divide the plaintext into blocks and use the same key to encrypt and decrypt the blocks.

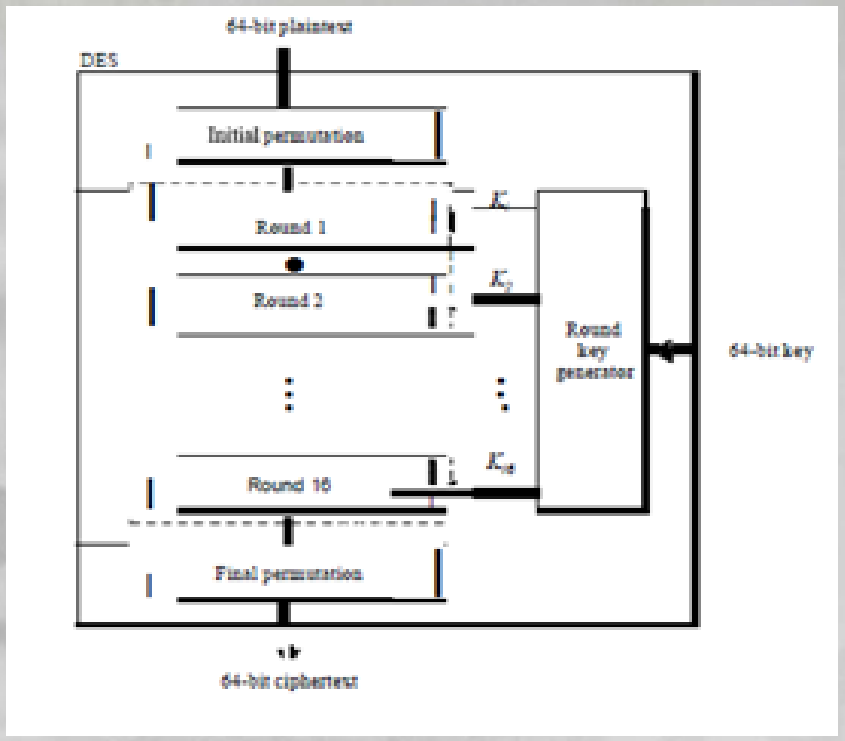


- **Data Encryption Standard (DES)**
- The algorithm encrypts a 64-bit plaintext block using a 64-bit key.
- DES has two transposition blocks (P-boxes) and 16 complex round ciphers (they are repeated).
- The 16 iteration round ciphers are conceptually the same, each uses a different key derived from the original key.
- The initial and final permutations are keyless straight permutations that are the inverse of each other.
- The permutation takes a 64-bit input and permutes them according to predefined values.
- Each round of DES is a complex round cipher.
- The structure of the encryption round ciphers is different from that of the decryption one.



DES function :-

- The heart of DES is the **DES function.**
- The DES function applies a 48-bit key to the rightmost 32 bits Ri to produce a 32-bit output.
- This function is made up of four operations: an XOR, an expansion permutation, a group of S-boxes, and a straight permutation

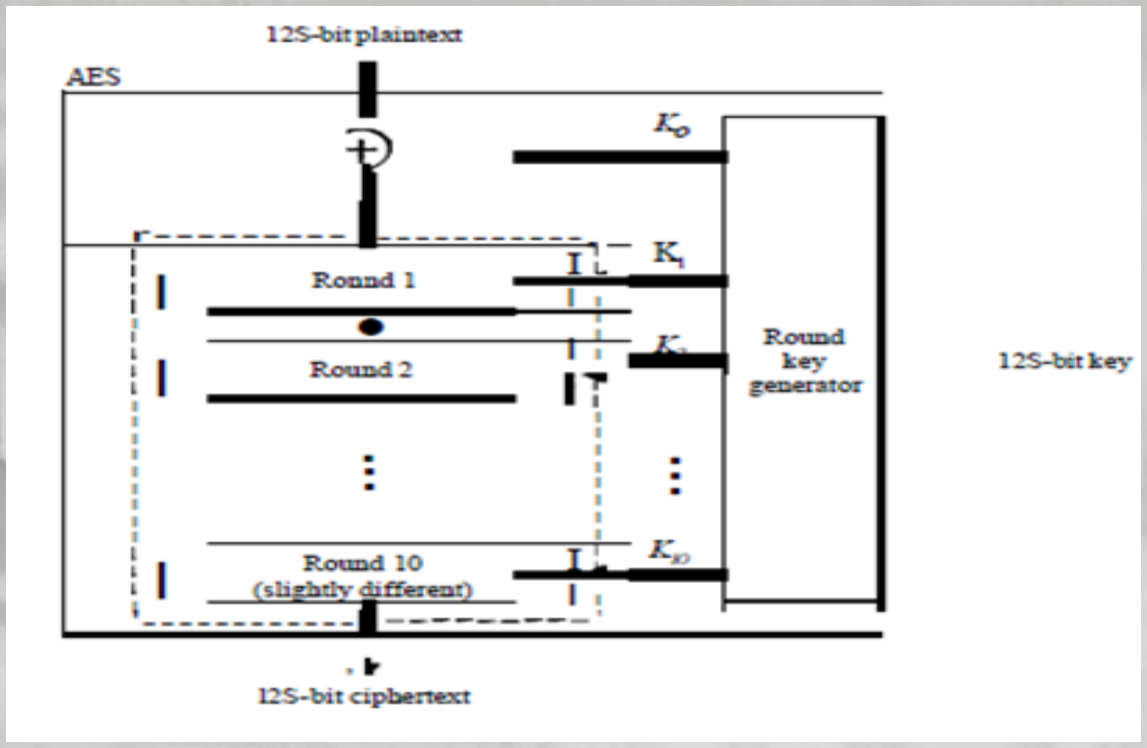


- **Advanced Encryption Standards (AES) :-**
- The Advanced Encryption Standard (AES) was designed because DES's key was too small.
- AES is a very complex round cipher.
- AES is designed with three key sizes: 128, 192, or 256 bits.
- AES has three different configurations with respect to the number of rounds and key size.
- Table below shows the AES configration.
- The structure and operation of the other configurations are similar.
- The difference lies in the key generation.
- There is an initial XOR operation followed by 10 round ciphers.

Size of Data Block	*Number of Rounds*	*Key Size*
128 bits	10	128 bits
	12	192 bits
	14	256 bits

- The last round is slightly different from the preceding rounds; it is missing one operation.
- The 10 iteration blocks are almost identical, each uses a different key derived from the original key.

- The figure below shows the basic structure of AES.

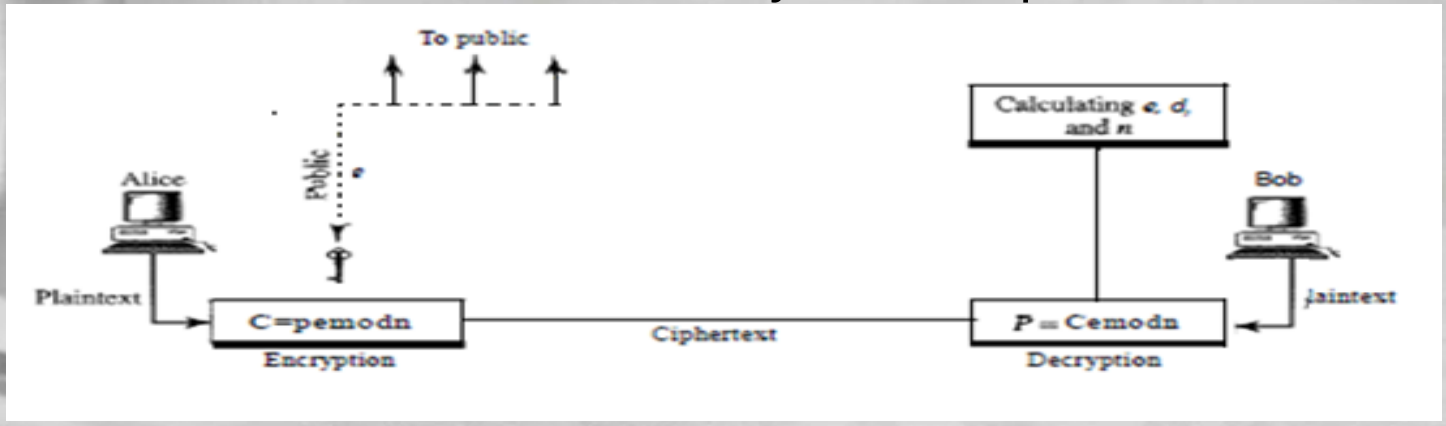


ASYMMETRIC-KEY CRYPTOGRAPHY

- Also called public key cryptography
- An asymmetric-key (or public-key) cipher uses two keys :-one private and one public.
- Here two algorithms are introduced and they are RSA and Diffie-Hellman algorithm.

➢ **RSA**

- RSA is named for its inventors Rivest, Shamir, and Adleman (RSA).
- It uses two numbers, e and d, as the public and private keys.
- The two keys, e and d, have a special relationship to each other but here is shown how to calculate the keys without proof.



- **Selecting Keys :-**

  Bob use the following steps to select the private and public keys :-

1. Bob chooses two very large prime numbers p and q.

   Note :- A prime number is one that can be divided evenly only by 1 and itself.

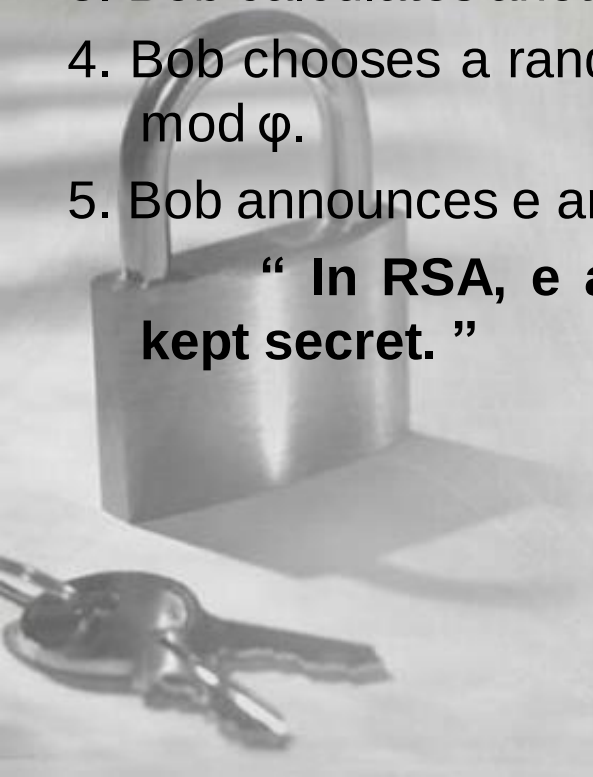
2. Bob multiplies the above two primes to find n, the modulus for encryption and decryption. ie, $n = p \times q$.

3. Bob calculates another number $\varphi = (p - 1) \times (q - 1)$.

4. Bob chooses a random integer e. He then calculates d so that $d \times e = 1 \mod \varphi$.

5. Bob announces e and n to the public; he keeps φ and d secret.

   " In RSA, e and n are announced to the public; d and φ are kept secret. "



- **Encryption :-**
- Anyone who needs to send a message to Bob can use n and e.
- Eg :- If Alice needs to send a message to Bob, she can change the message, usually a short one, to an integer. This is the plaintext.

  She then calculates the ciphertext, using e and n.

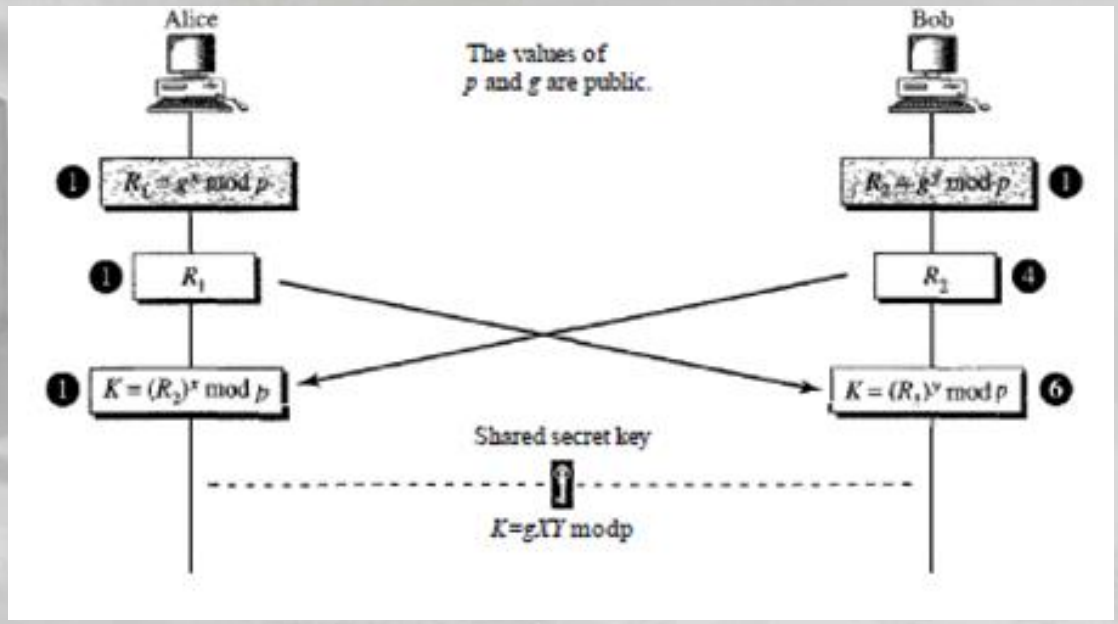
  "$C=p^e(\mathrm{mod} n)$, Alice sends C, the ciphertext, to Bob
- **Decryption :-**
- Bob keeps p and d as private.
- When he receives the ciphertext, he uses his private key d to decrypt the message :-

  $P= C^d(\mathrm{mod} n)$

- There is a restriction for RSA to work, the value of P must be less than the value of n.
- If P is a large number, the plaintext needs to be divided into blocks to make P less than n.

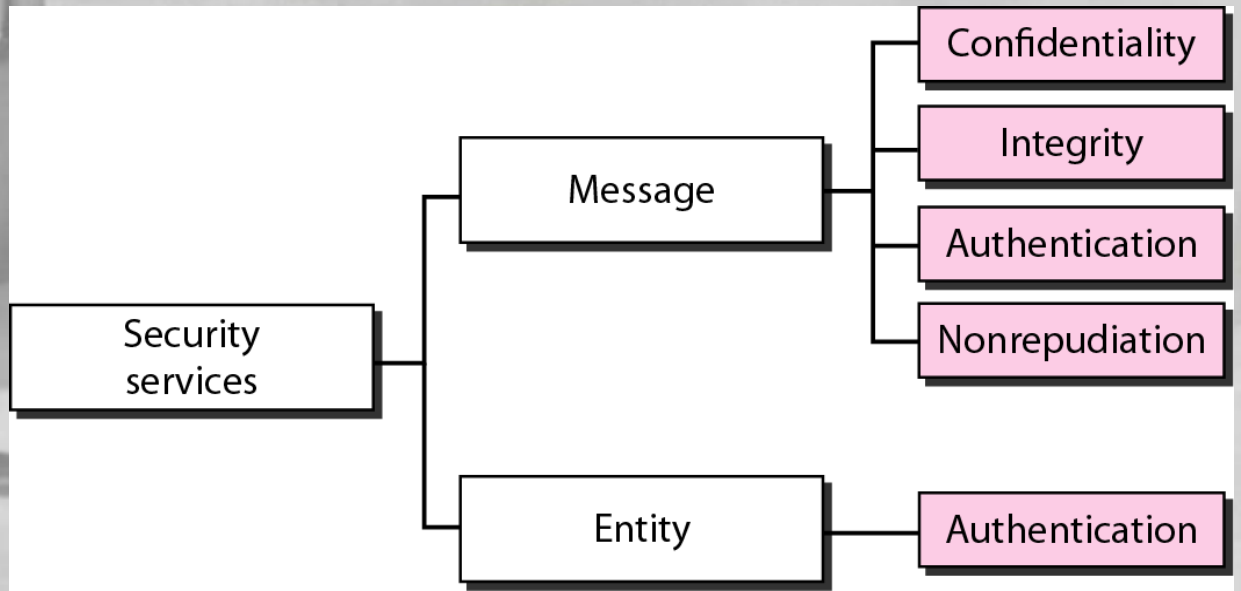
➢ DIFFIE-HELLMAN

- Diffie-Hellman was originally designed for key exchange.
- In the **Diffie-Hellman** cryptography, two parties create a symmetric session key to exchange data without having to remember or store the key for future use.
- They do not have to meet to agree on the key; it can be done through the Internet.



SECURITY SERVICES

- Network security can provide one of the five services.
- Four of these services are related to the message exchanged using the network.
- They are message confidentiality, integrity, authentication, and nonrepudiation.
- The fifth service provides entity authentication or identification.



➢ MESSAGE CONFIDENTIALITY :-

- Message confidentiality or privacy means that the sender and the receiver expect confidentiality.
- The transmitted message must make sense to only the intended receiver.
- To all others, the message must be garbage.
- Eg :- when a customer communicates with her bank, she expects that the communication is totally confidential.

➢ MESSAGE INTEGRITY :-

- Message integrity means that the data must arrive at the receiver exactly as they were sent.
- There must be no changes during the transmission, neither accidentally nor maliciously.
- As more and more monetary exchanges occur over the Internet, integrity is crucial.
- Eg :- It would be disastrous if a request for transferring $100 changed to a request for $10,000 or $100,000.
- The integrity of the message must be preserved in a secure communication.

➢ MESSAGE AUTHENTICATION :-

- Message authentication is a service beyond message integrity.
- In message authentication the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.

➢ MESSAGE NON - REPUDIATION :-

- Message nonrepudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send.
- The burden of proof falls on the receiver.
- Eg :- When a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.

➢ **ENTITY AUTHENTICATION :-**

- In entity authentication (or user identification) the entity or user is verified prior to access to the system resources (files, for example).
- Eg :- A student who needs to access her university resources needs to be authenticated during the logging process. This is to protect the interests of the university and the student.

Asymmetric(public) Cryptography

- Also known as Public key cryptosystem.
- Uses, public key and private key.
- Encodes messages using mathematically related keys.
- RSA was he first public key crypto system
- Public key: Known to all parties engaged. Freely distributed to public. It is used to encrypt message.
- Private key: Known only to the owner and is kept secret.
- The owner uses private key to decrypt all the messages.
- Encryption can be done with any of these.
- Decryption is allowed only with the corresponding key pair.
- Eg: If Anil want to communicate with Bindu, he obtains Bindu's public key. Then he encrypts the message using the public key

WORKING

- Sender A (PKA, PRKA)

  PKA-Public key of A, PRKA-Private key of A

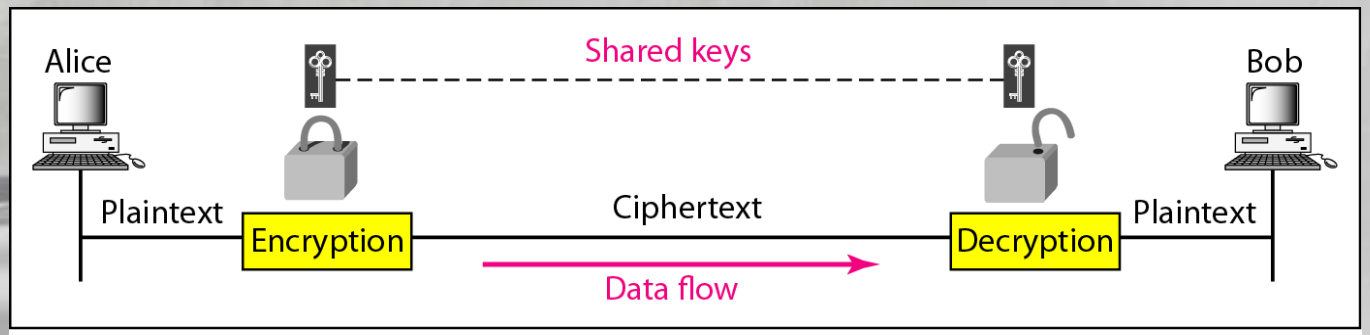
- Receiver B (PKB,PRKB)
- If A wants to send a confidential/secret message to B,

  A will encrypt it with PKB. So that the message can be decrypted only by the private key of B, PRKB, which is known only to B
- If A wants to send an authenticated message to B, A will encrypt it with its private key, PRKA. So anyone can decrypt it using PKA, the public key of A.
- If A wants to send a secret ,authenticated message to B?

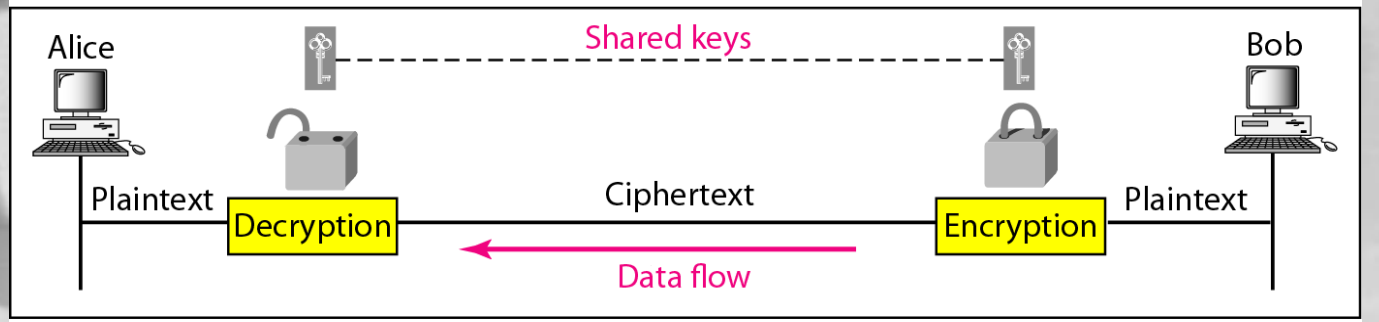
  Encrypt message with PRKA, then encrypt it with PKB. Send it. Receiver B will decrypt it with PRKB first and then with the PKA.

MESSAGE CONFIDENTIALITY

- Confidentiality with Symmetric-Key Cryptography

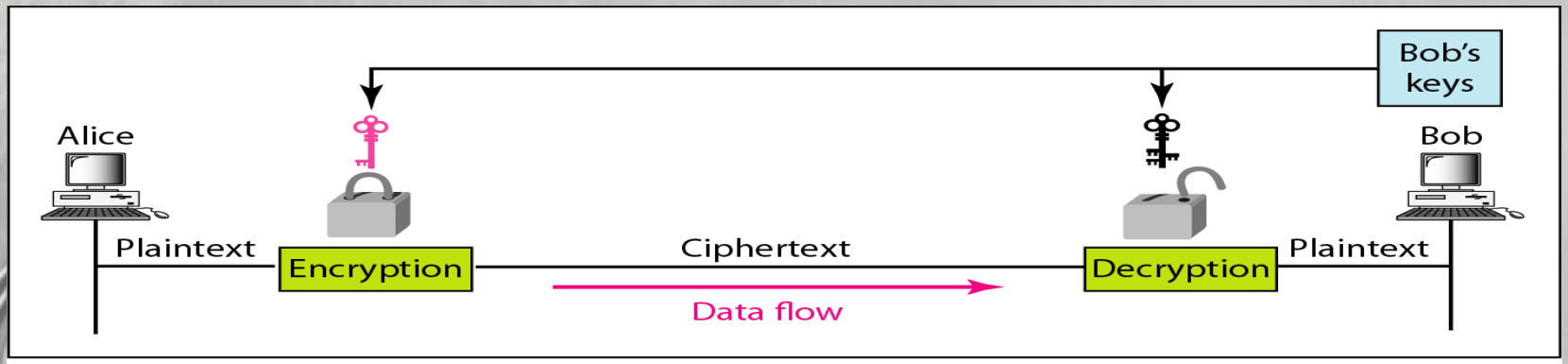


a. A shared secret key can be used in Alice-Bob communication

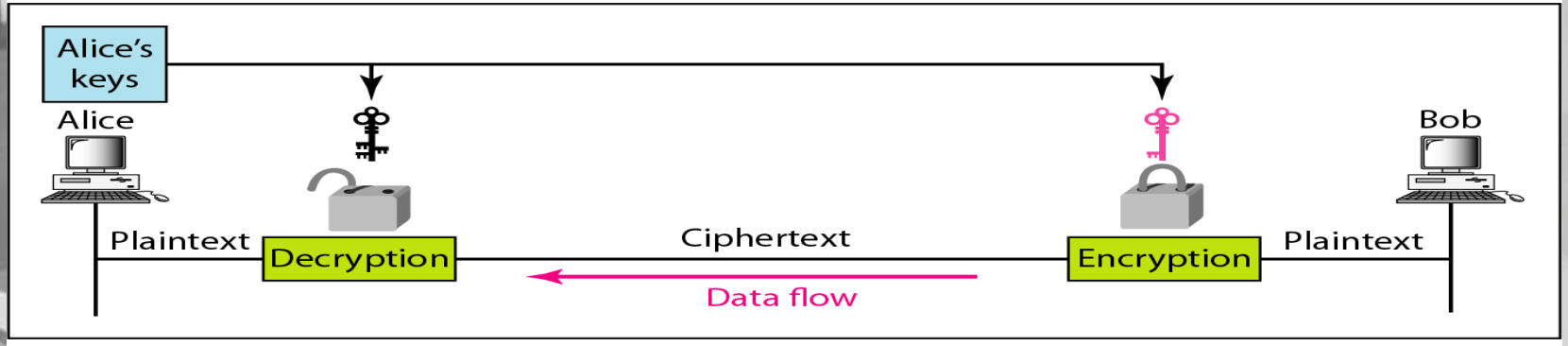


b. A different shared secret key is recommended in Bob-Alice communication

- Confidentiality with Asymmetric-Key Cryptography



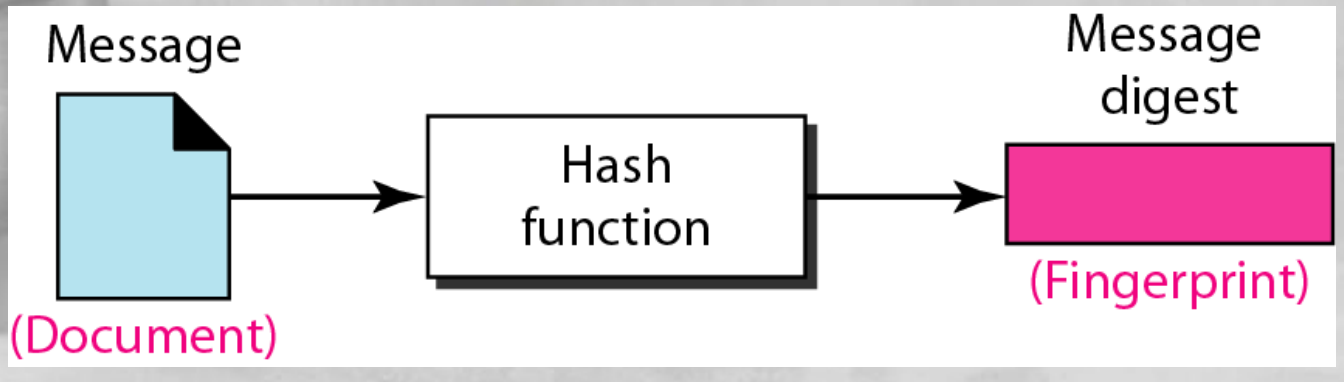
a. Bob's keys are used in Alice-Bob communication



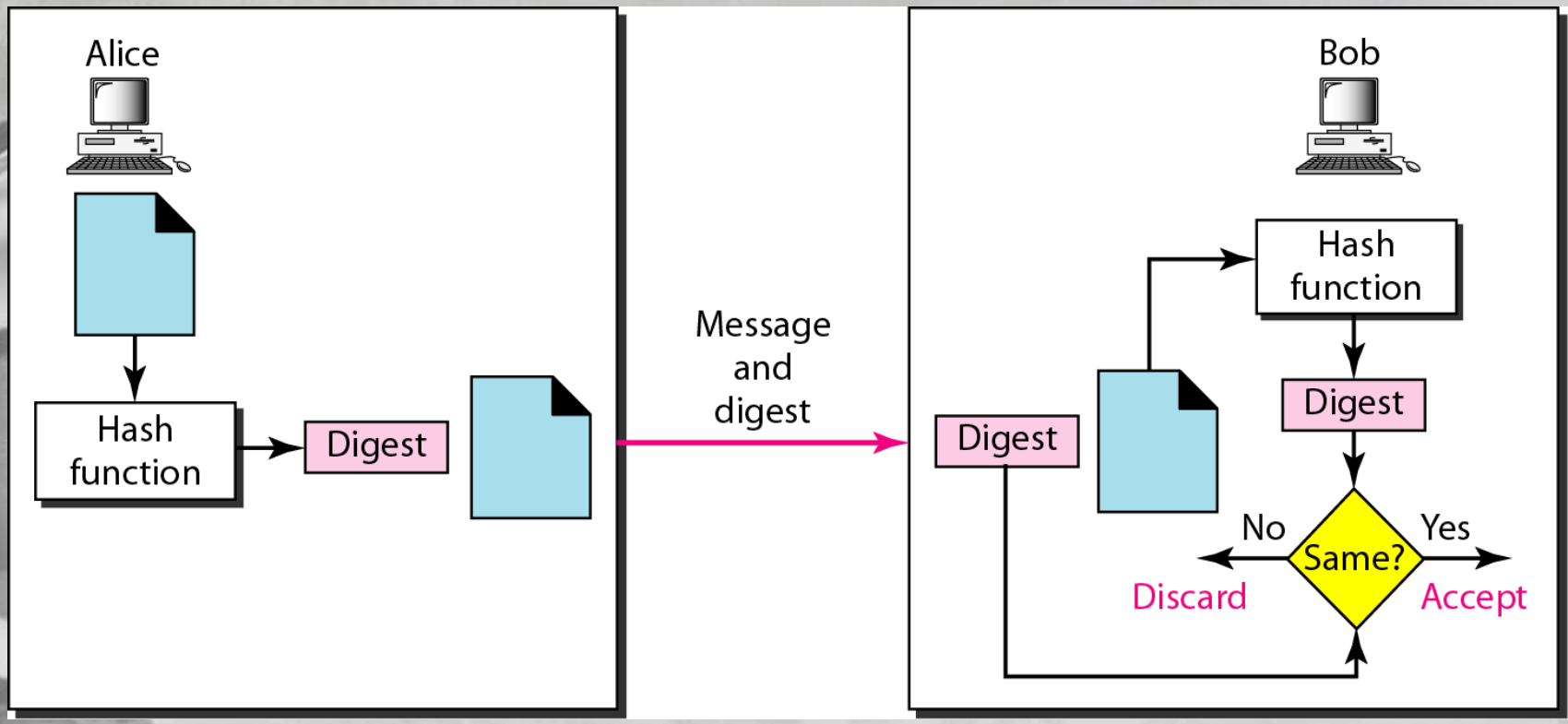
b. Alice's keys are used in Bob-Alice communication

MESSAGE INTEGRITY

- One way to preserve the integrity of a document is through the use of a fingerprint. If Alice needs to be sure that the contents of her document will not be illegally changed
- To preserve the integrity of a document, both the document and the fingerprint are needed
- Message and Message Digest



- ACreating and Checking the Digest

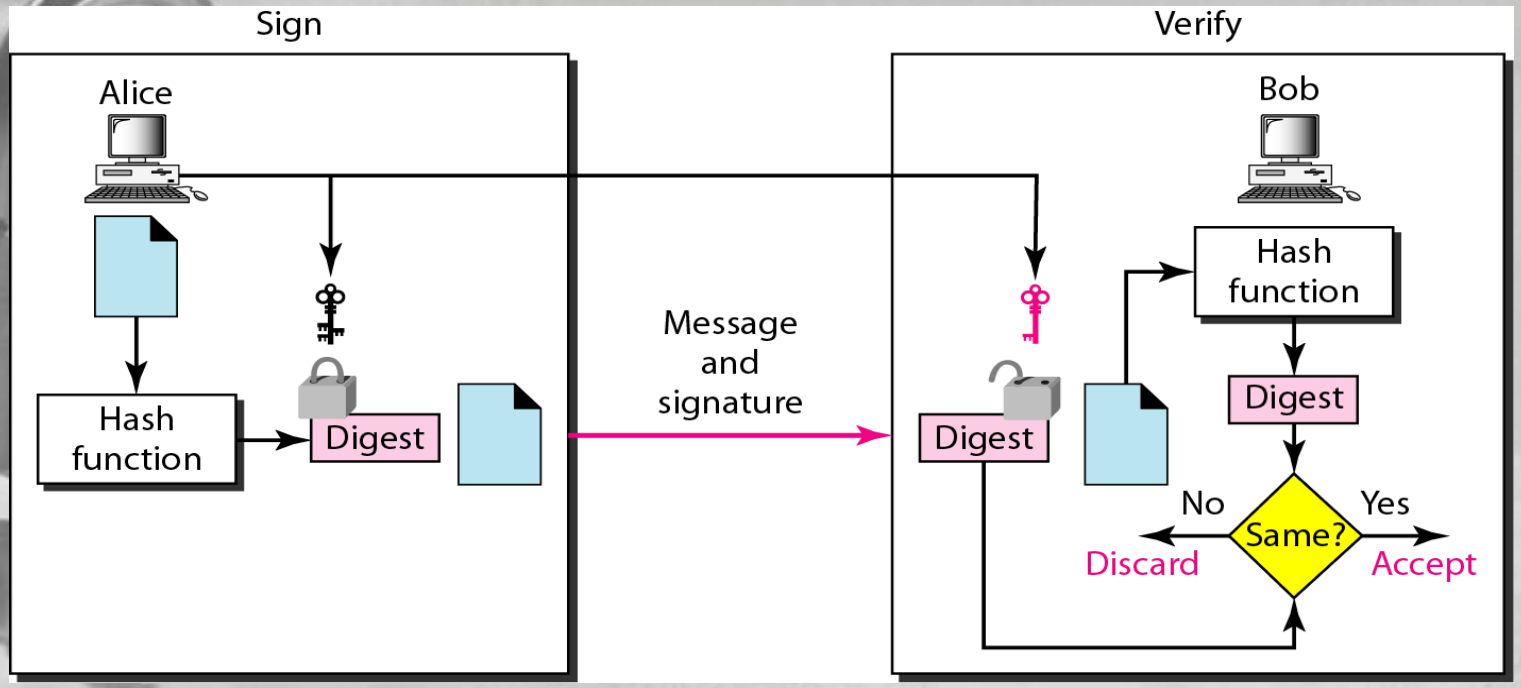


- MESSAGE AUTHENTICATION
- A hash function guarantees the integrity of a message. It guarantees that the message has not been changed. A hash function, however, does not authenticate the sender of the message.
- When Alice sends a message to Bob, Bob needs to know if the message is coming from Alice or Eve. To provide message authentication. The digest created by a hash function is normally called a modification detection code (MDC).
- MAC
- To provide message authentication, we need to change a modification detection code to a message authentication code (MAC). An MDC uses a keyless hash function. A MAC uses a keyed hash function. A keyed hash function includes the symmetric keybetween the sender and receiver when creating the digest. Figure shows how Alice uses a keyed hash function to authenticate her message and how Bob can verify the authenticity of the message.

DIGITAL SIGNATURE

- A digital signature needs a public-key system.
- An electronic signature can prove the authenticity of Alice as the sender of the message. We refer to this type of signature as a digital signature.
- A digital signature needs a public-key system.
- In a cryptosystem, we use the private and public keys of the receiver;
- in digital signature, we use the private and public keys of the sender.

- Services
- A digital signature today provides message integrity.
- Digital signature provides message authentication.
- Nonrepudiation can be provided using a trusted party s



THANK YOU