Established as per the Section 2(f) of the UGC Act, 1956
Approved by AICTE, COA and BCI, New Delhi

QS I-GAUGE GOLD

nirf

MHRD'S INNOVATION CELL (GOVERNMENT OF INDIA)

INSTITUTION'S INNOVATION COUNCIL (Ministry of HRD Initiative)

Lecture 1.5

Computer Security Concepts

School of Computing and Information Technology

Mr. K.Jeevan pradeep

Introduction Class

Recap of previous Lecture

The picture can't be displayed.

TOPICS TO BE DISCUSSED

Block Ciphers and the Data Encryption, Block Cipher Design Principles

The Data Encryption Standard, A DES Example

Advanced Encryption Standard. Public-Key Cryptosystems

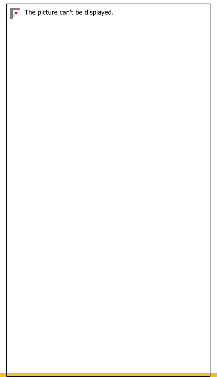
The RSA Algorithm, Diffie-Hellman Key Exchange

The picture can't be displayed.

BLOCK CIPHER DESIGN PRINCIPLES

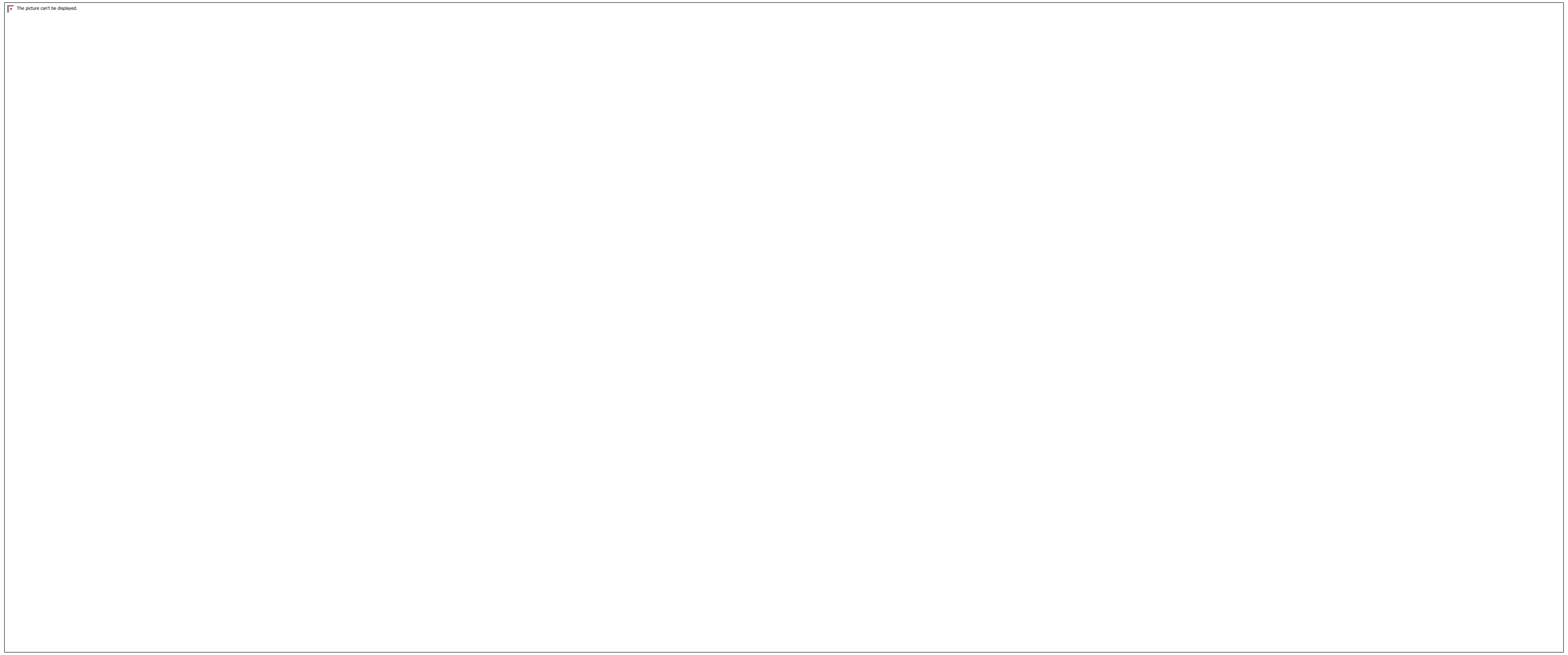
✓ In Modern ciphers, digital data is represented in strings of binary digits (bits) unlike alphabets. Modern cryptosystems need to process these binary strings to convert into another binary string. Based on how these binary strings are processed, a symmetric encryption scheme can be classified into stream cipher and block cipher.

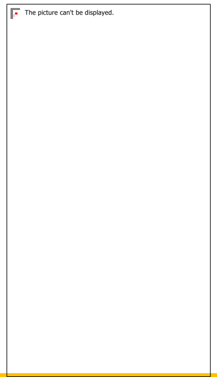
✓ Stream cipher: A stream cipher is the mechanism that encrypts a digital data stream one bit or one byte at a time. In this scheme, the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations are performed on it to generate one bit of ciphertext.



BLOCK CIPHER DESIGN PRINCIPLES

For practical reasons, the bit-stream generator must be implemented as an algorithmic procedure, so that the cryptographic bit stream can be produced by both users. in this approach, the bit-stream generator is a key-controlled algorithm and must produce a bit stream that is cryptographically strong. that is, it must be computationally impractical to predict future portions of the bit stream based on previous portions of the bit stream. the two users need only share the generating key, and each can produce the keystream.





BLOCK CIPHER DESIGN PRINCIPLES

- ✓ Block Cipher: A block cipher is the mechanism in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length. The number of bits in a block is fixed. Typically, a block size of 64 or 128 bits is used. As with a stream cipher, the two users share a symmetric encryption key.
- ✓ The basic scheme of a block cipher is depicted as follows:

The picture can't be displayed.

The picture can't be displayed.

BLOCK CIPHER DESIGN PRINCIPLES

1

The picture can't be displayed.

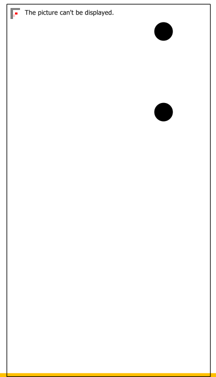
The picture can't be displayed.

DATA ENCRYPTION STANDARD (DES)

- The Data Encryption Standard (DES) is a symmetric-key block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. The block size is 64-bit.

- Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

- Most widely used block cipher in world
- Adopted in 1977 by NBS (now NIST)
- Encrypts 64-bit data using 56-bit key
- Has widespread use
- Has considerable controversy over its security



DATA ENCRYPTION STANDARD (DES)
DES HISTORY

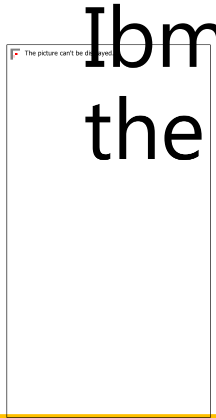
Ibm developed lucifer cipher

- By team led by feistel in late 60’s
- Used 64-bit data blocks with 128-bit key

Then redeveloped as a commercial cipher with input from nsa and others

In 1973 nbs issued request for proposals for a national cipher standard

Ibm submitted their revised lucifer which was eventually accepted as the des



DATA ENCRYPTION STANDARD (DES)

Figure ***Encryption and decryption with DES***

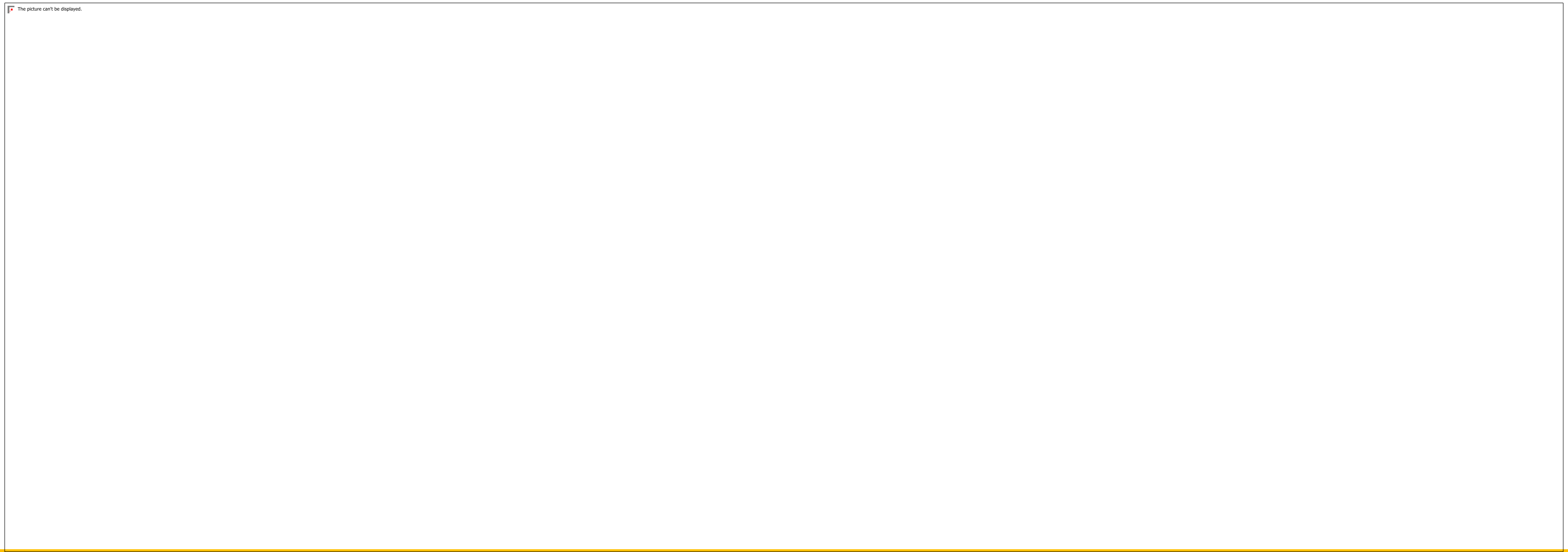
- ✓ *The encryption process is made of two permutations (P-boxes), which we call initial and final permutations, and sixteen Feistel rounds.*
- ✓ *Topics discussed in this section*

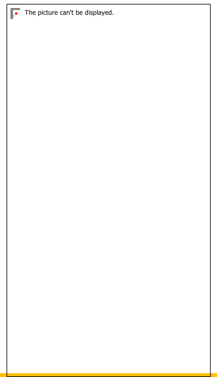
○ Initial and Final Permutations

○ Rounds

○ Cipher and Reverse Cipher

○ Examples





DATA ENCRYPTION STANDARD (DES)

Figure : ***General structure of DES***

The picture can't be displayed.

The picture can't be displayed.

DATA ENCRYPTION STANDARD (DES)

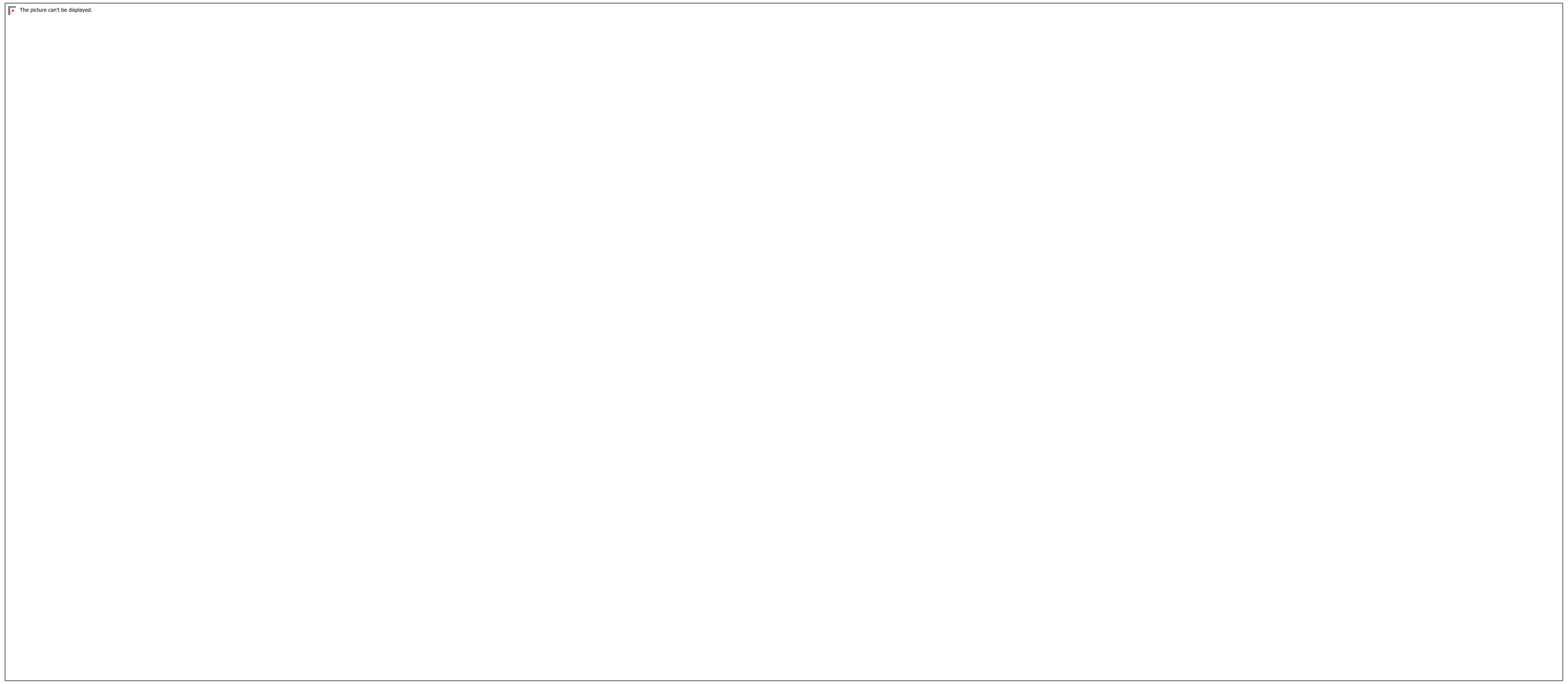
Figure : ***Initial and final permutation steps in DES***

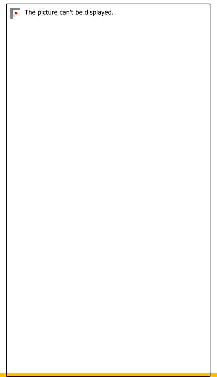
The picture can't be displayed.

The picture can't be displayed.

DATA ENCRYPTION STANDARD (DES)

Table : ***Initial and final permutation tables***





Note:The initial and final permutations are straight P-boxes that are inverses of each other.

They have no cryptography significance in DES.

DATA ENCRYPTION STANDARD (DES)

The picture can't be displayed.

The picture can't be displayed.

DATA ENCRYPTION STANDARD (DES)

The picture can't be displayed.

The picture can't be displayed.

DATA ENCRYPTION STANDARD (DES)

The heart of DES is the DES function. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

Figure: *DES function*

The picture can't be displayed.

Figure:

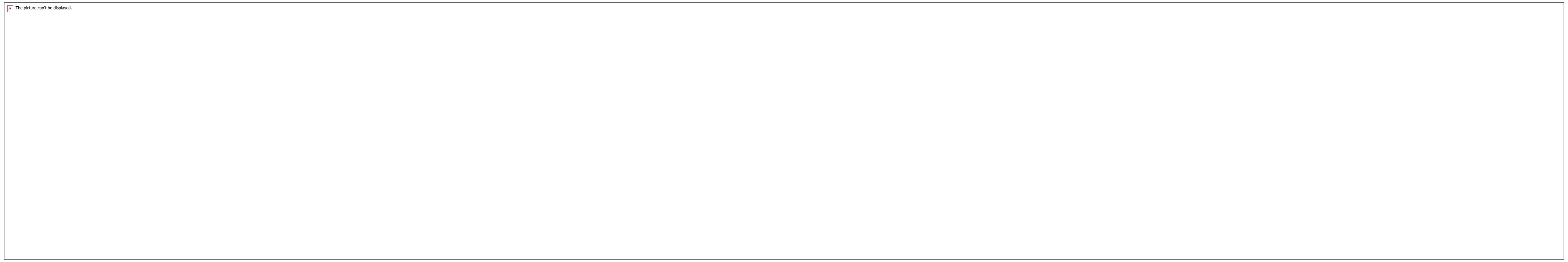
The picture can't be displayed.

DATA ENCRYPTION STANDARD (DES)

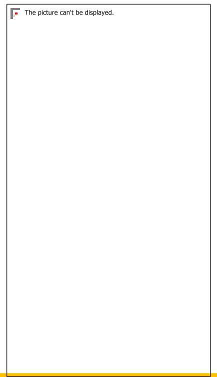
Expansion P-box

Since R_{I-1} is a 32-bit input and K_I is a 48-bit key, we first need to expand R_{I-1} to 48 bits.

Figure: ***Expansion permutation***

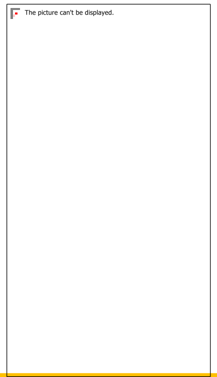


The S-boxes do the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.



ADVANCED ENCRYPTION STANDARD (AES)

- 1997 --National Institute of Standards and Technology (NIST) issues a call for proposals.
- 2001--AES issues as a federal information processing standards (FIPS 197)
- Security Strength Equal to or Better than 3DES
- Significantly More Efficient than 3DES
- Symmetric Block Cipher
- Block Length = 128 bits
- Support for Key Lengths of 128, 192, and 256 bits
- SECURITY
- COST
- IMPLEMENTATION



ADVANCED ENCRYPTION STANDARD (AES)

AES has defined three versions, with 10, 12, and 14 rounds.
Each version uses a different cipher key size (128, 192, or 256),
but the round keys are always 128 bits

The picture can't be displayed.

The picture can't be displayed.

AES STRUCTURE

The picture can't be displayed.

The picture can't be displayed.

The picture can't be displayed.

The picture can't be displayed.

AES ENCRYPTION PROCESS

The picture can't be displayed.

The picture can't be displayed.

DATA UNITS USED IN AES

The picture can't be displayed.

The picture can't be displayed.

PLAINTEXT TO STATE

The picture can't be displayed.

The picture can't be displayed.

STRUCTURE OF EACH ROUND

The picture can't be displayed.

The picture can't be displayed.

SHIFT ROWS

The picture can't be displayed.

The picture can't be displayed.

The picture can't be displayed.

The picture can't be displayed.

MIX COLUMNS

- each column is processed separately
- each byte is replaced by a value dependent on all 4 bytes in the column

The picture can't be displayed.

The picture can't be displayed.

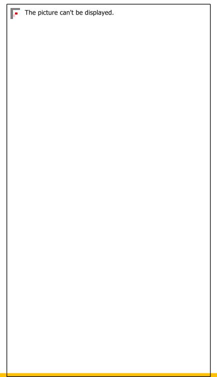
ADD ROUND KEY

The picture can't be displayed.

The picture can't be displayed.

TRANSPOSITION TECHNIQUES

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. For the type of columnar transposition just shown, cryptanalysis is fairly straightforward and involves laying out the ciphertext in a matrix and playing around with column positions. Digram and trigram frequency tables can be useful



PUBLIC-KEY CRYPTOSYSTEMS

- It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key.

In addition, some algorithms, such as RSA, also exhibit the following characteristic.

- Either of the two related keys can be used for encryption, with the other used for decryption

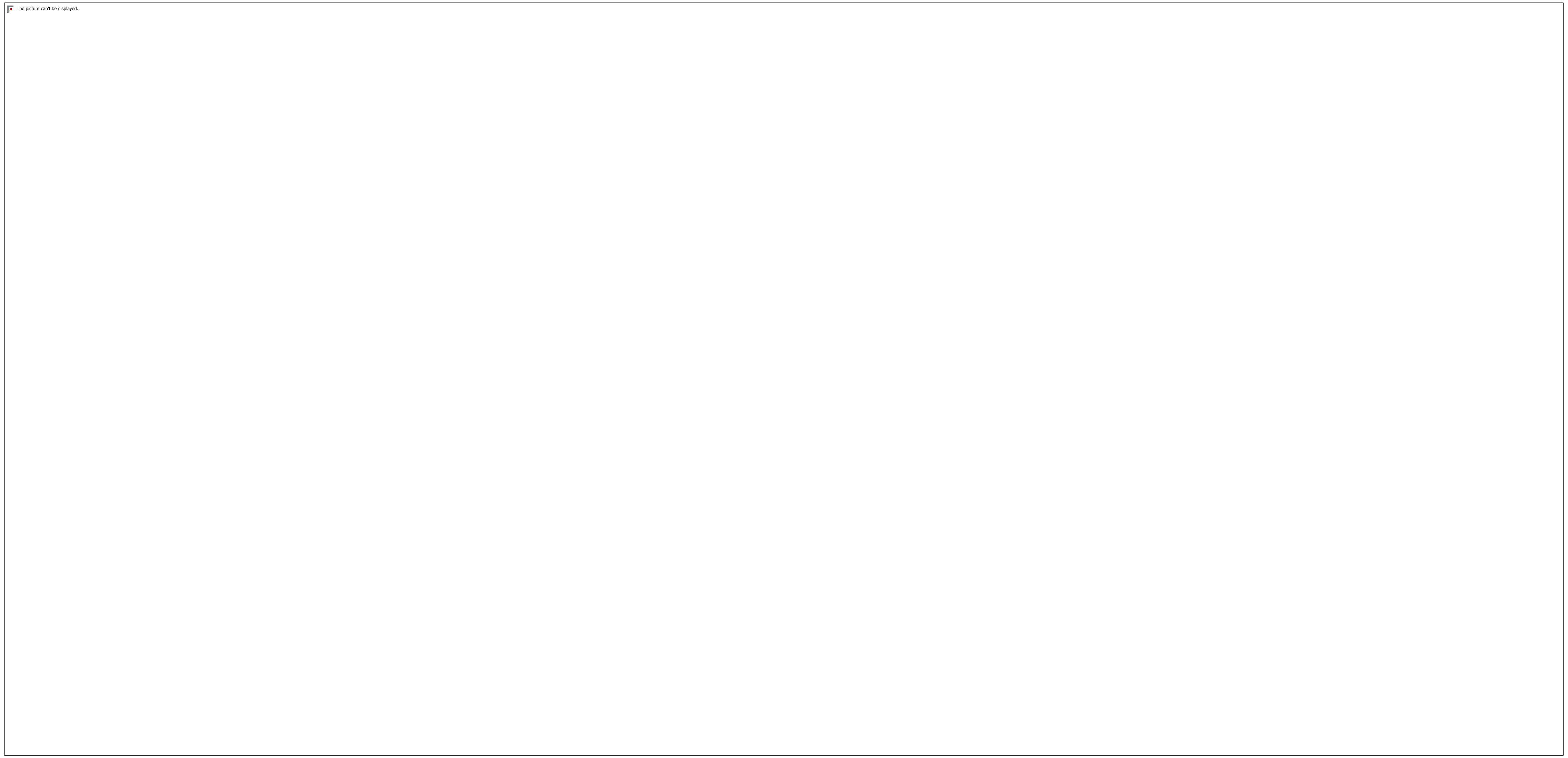
The picture can't be displayed.

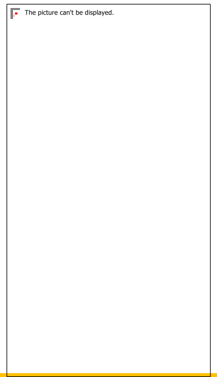
The picture can't be displayed.

PUBLIC-KEY CRYPTOSYSTEMS

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

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



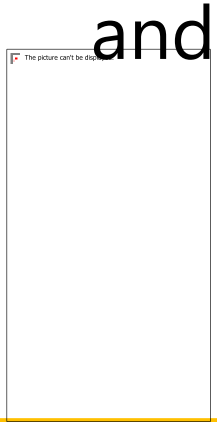


PUBLIC-KEY CRYPTOSYSTEMS

- Public and private keys: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption.The exact transformations performed by the algorithm depend on the public or private key that is provided as input.

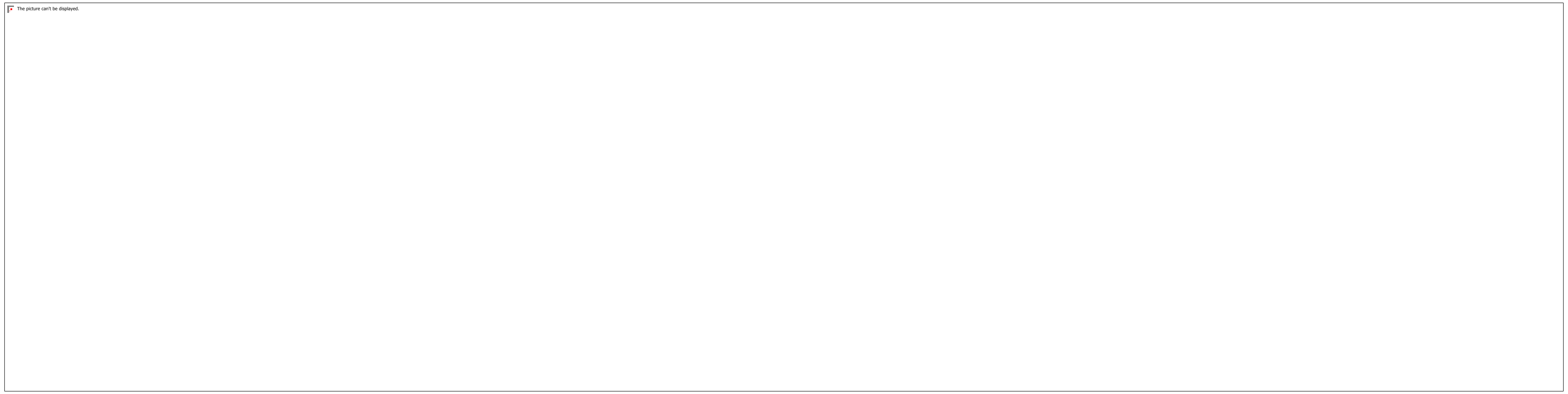
- Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.

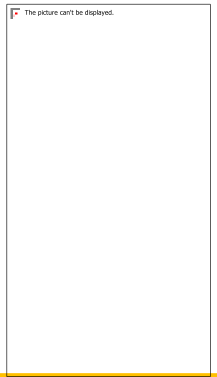
- Decryption algorithm: This algorithm accepts the ciphertext and the matching key and produces the original plaintext



THE RSA ALGORITHM

- The **RSA algorithm** is an asymmetric cryptography algorithm; this means that it uses a public key and a private key (i.e two different, mathematically linked keys).
- As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.
- The RSA algorithm is named after those who invented it in 1978: Ron Rivest, Adi Shamir, and Leonard Adleman.





THE RSA ALGORITHM

- RSA is the most common public-key algorithm, named after its inventors **Rivest, Shamir, and Adelman (RSA).**

The picture can't be displayed.

The picture can't be displayed.

THE RSA ALGORITHM

The picture can't be displayed.

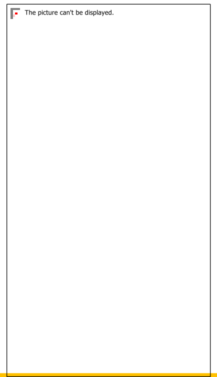
-

The picture can't be displayed.

THE RSA ALGORITHM

- **Advantages-**
  - The advantages of public key cryptography are-
  - It is more robust.
  - It is less susceptible to third-party security breach attempts.

- **Disadvantages-**
  - It involves high computational requirements.
  - It is slower than symmetric key cryptography.



THE RSA ALGORITHM

Example

The picture can't be displayed.

The picture can't be displayed.

DIFFIE-HELLMAN KEY EXCHANGE

- **Introduction to Diffie Hellman Key Exchange Algorithm**

➢ Whitefield Diffie and Martin Hellman develop Diffie Hellman key exchange Algorithms in 1976 to overcome the problem of key agreement and exchange.

➢ It enables the two parties who want to communicate with each other to agree on a symmetric key, a key that can be used for encrypting and decryption, note that Diffie Hellman key exchange algorithm can be used for only key exchange, not for encryption and decryption process.

➢ The algorithm is based on mathematical principles.

DIFFIE-HELLMAN KEY EXCHANGE

The simple idea of understanding to the DH Algorithm is the following.

1. The first party picks two prime numbers, α and q and tells them to the second party.

2. The second party then picks a secret number (let's call it X_A), and then it computes $\alpha^{X_A} \bmod q$ and sends the result back to the first party; let's call the result Y_A. Keep in mind that the secret number is not sent to anyone, only the result is.

3. Then the first party does the same; it selects a secret number X_B and calculates the result Y_B similor to the
4. step 2. Then, this result is sent to the second party.
5. The second party takes the received number Y_B and calculates $Y_B^{X_A} \bmod q$

The picture can't be displayed.

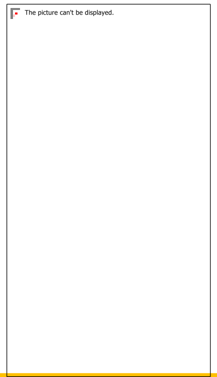
DIFFIE-HELLMAN KEY EXCHANGE

The simple idea of understanding to the DH Algorithm is the following.

5 .The first party takes the received number Y_A and calculates $Y_A^{X_B} \mod q$

6. This is where it gets interesting the answer in step 5 is the same as the answer in step 4. This means both parties will get the same answer no matter the order of exponentiation.

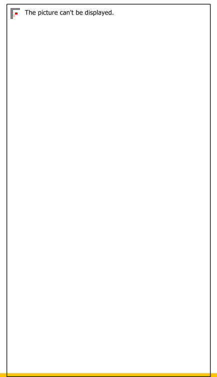
7. The number we came within steps 4 and 5 will be taken as the shared secret key. This key can be used to do any encryption of data that will be transmitted



DIFFIE-HELLMAN KEY EXCHANGE

-

The picture can't be displayed.



The picture can't be displayed.

DIFFIE-HELLMAN KEY EXCHANGE

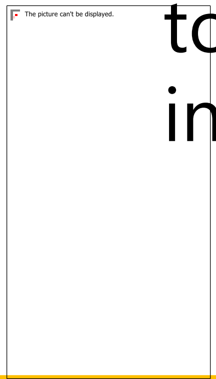
Key Exchange Protocols

✓ Figure 10.2 shows a simple protocol that makes use of the Diffie-Hellman calculation.

✓ Suppose that user A wishes to set up a connection with user B and use a secret key to encrypt messages on that connection.

✓ User A can generate a one-time private key , calculate , and send that to user B. User B responds by generating a private value , calculating , and sending to user A.

✓ Both users can now calculate the key. The necessary public values and would need to be known ahead of time. Alternatively, user A could pick values for and and include those in the first message



DIFFIE-HELLMAN KEY EXCHANGE

Key Exchange Protocols

The picture can't be displayed.

The picture can't be displayed.

DIFFIE-HELLMAN KEY EXCHANGE

Example

✓

The picture can't be displayed.

The picture can't be displayed.

The picture can't be displayed.

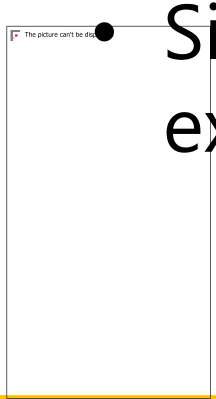
DIFFIE-HELLMAN KEY EXCHANGE

Advantages of the Diffie Hellman Algorithm

- The sender and receiver don’t need any prior knowledge of each other.
- Once the keys are exchanged, the communication of data can be done through an insecure channel.
- The sharing of the secret key is safe.

Disadvantages of the Diffie Hellman Algorithm

- The algorithm can not be sued for any asymmetric key exchange.
- Similarly, it can not be used for signing digital signatures.
- Since it doesn’t authenticate any party in the transmission, the Diffie Hellman key exchange is susceptible to a man-in-the-middle attack.



MAN-IN-THE-MIDDLE ATTACK

The protocol depicted in Figure 10.2 is insecure against a man-in-the-middle attack. Suppose Alice and Bob wish to exchange keys, and Darth is the adversary. The attack proceeds as follows

1. Darth prepares for the attack by generating two random private keys and and then computing the corresponding public keys and .

2. Alice transmits to Bob.

3. Darth intercepts and transmits to Bob. Darth also calculates

$$K2 = (YA) XD2 \text{ mod } q$$

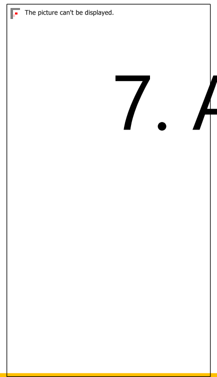
4. Bob receives and calculates .

5. Bob transmits to Alice.

6. Darth intercepts and transmits to Alice. Darth calculates .

$$K1 = (YB) XD1 \text{ mod } q$$

7. Alice receives and calculates .



MAN-IN-THE-MIDDLE ATTACK

At this point, Bob and Alice think that they share a secret key, but instead Bob and Darth share secret key and Alice and Darth share secret key . All future communication between Bob and Alice is compromised in the following way

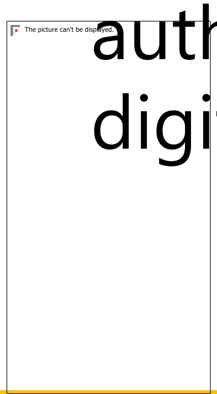
1. Alice sends an encrypted message .

2. Darth intercepts the encrypted message and decrypts it to recover .

3. Darth sends Bob ,

where is any message. In the first case, Darth simply wants to eavesdrop on the communication without altering it. In the second case, Darth wants to modify the message going to Bob

The key exchange protocol is vulnerable to such an attack because it does not authenticate the participants. This vulnerability can be overcome with the use of digital signatures and public-key certificates.



SUMMARY OF THE LECTURE

Computer Security Concepts: The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms

A Model for Network Security Symmetric Ciphers, Classical Encryption Techniques : Substitution Techniques,

Transposition Techniques, Steganography, Block Ciphers and the Data Encryption, The Data Encryption Standard, A DES Example

Block Cipher Design Principles,AES, Public-Key Cryptosystems, The RSA Algorithm, Diffie-Hellman Key Exchange

DISCUSSION

The picture can't be displayed.