CRYPTOGRAPHY

Cryptography:
The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form

From Ancient Greek 'CRYPTO' means Secret 'Graphy' means Writing

CRYPTOGRAPHY-'Secret Writing'

Computer data often transfers from one computer to another, leaving its secure physical environment.
People with ill intentions might change or fabricate your data once it has gotten out of hand, either for entertainment or for their own gain.

The data can be reformatted and transformed using cryptography, making the journey between computers safer.
The technique is built on the fundamentals of secret codes, which are enhanced by contemporary mathematics to provide effective protection for our data.

Computer Security: a generic name for a group of techniques aimed at protecting data and preventing hackers

Network Security: Mechanisms to safeguard data during transmission

Internet Security - measures to protect data during their transmission over a collection of interconnected networks

Security Attacks, Services and Mechanisms:

Security Attack: Any activity that compromises the security of an organization's information.

Security mechanism – A mechanism that is designed to detect, prevent or recover from a security attack.

Security Services: A service that improves the security of an organization's data processing systems and information exchanges. The services are designed to thwart security assaults, and they employ one or more security measures to do so.

Basic Terminologies:

- **Plain Text:** The original message was understandable.
- **Cipher text** : The transformed message
- **Cipher:** An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods
- **Key** :Some critical information used by the cipher, known only to the sender & receiver
- **Encipher (encode) :**The process of converting plaintext to cipher text using a cipher and a key
- **Decipher (decode):** The process of converting ciphertext back into plaintext using a cipher and a key
- **Cryptanalysis:** The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called code breaking
- **Cryptology:** Both cryptography and cryptanalysis
- **Threat**: A potential for violation of 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.

- **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.

Characteristics of Cryptography:

Cryptographic systems are generally classified along 3 independent dimensions:

1.Type of operations : used for transforming plain text to cipher text

All the encryption algorithms are based on two general principles:

Substitution, in which each element in the plaintext is mapped into another element, and **Transposition**, in which elements in the plaintext are rearranged.

2.The number of keys used: If the sender and receiver uses same key then it is said to be **symmetric key** (or) **single key (or) conventional encryption.**

If the sender and receiver use different keys then it is said to be **public key encryption.**

3. The way in which the plain text is processed:

A block cipher processes the input and block of elements at a time, producing output blocks for each input block.

A stream cipher processes the input elements continuously, producing output elements one at a time, as it goes along.

Cryptanalysis:

Cryptanalysis is the process of attempting to discover X, K, or both. The cryptanalyst's strategy is determined by the nature of the encryption system and the information accessible to it**.**

Cryptanalytic attacks based on the amount of information known to the cryptanalyst.

Cipher text only – A copy of cipher text alone is known to the cryptanalyst.

Known plaintext – The cryptanalyst has a copy of the cipher text and the corresponding plaintext.

Chosen plaintext – The cryptanalysts gains temporary access to the encryption machine. They cannot open it to find the key, however; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key.

Chosen cipher text – The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several string of symbols, and tries to use the results to deduce the key.

SECURITY SERVICES:

Confidentiality: Ensures that only authorised parties have access to the information stored in a computer system and sent information.

E.g. Printing, displaying and other forms of disclosure

Authentication: Ensures that the message or electronic document's origin is accurately identified, with the guarantee that the identification is not fake.

Integrity: Only authorized parties are allowed to make changes to computer system assets and sent data. Writing, altering status, deleting, generating, and delaying or replaying sent messages are all examples of modification.

Non repudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.

Access control: Requires that access to information resources may be controlled by or the target system.
Availability: Requires that computer system assets be available to authorized parties when needed.

SECURITY ATTACKS:

There are four different types of attacks, as described below:

Interruption: A system asset is destroyed, rendered unavailable, or rendered useless. This is a type of availability attack in which a piece of hardware is destroyed, a communication line is severed, or a file management system is disabled.

Interception: An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or a computer. e.g., wire tapping to capture data in the network, illicit copying of files

Modification: An unauthorized person not only obtains access to an asset, but also tampers with it. This is a violation of trust. Changing the contents of messages being broadcast over a network, for example, changing the values in a data file, updating a program.

Fabrication: Counterfeit items are introduced into the system by an unauthorized person. This is a smear campaign against truthfulness. Inserting a false message into a network or adding records to a file are two examples.

Cryptographic Attacks:

It is classified into **Passive attacks** and **Active Attacks**

Passive Attacks: Eavesdropping or monitoring communications are examples of passive attacks. The opponent's objective is to intercept the information being transmitted. There are two forms of passive attacks:

1. **Release of message contents**
2. **Traffic analysis**

Passive attacks are very difficult to detect because they do not involve any alteration of data

Active attacks: These attacks include some form of data stream manipulation or the construction of a fake stream.

These attacks can be classified in to four categories:

Masquerade – One entity pretends to be a different entity.

Replay – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.

Modification of messages – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.

Denial of service – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance

Security Services:

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

Model for Network security

1.6 A MODEL FOR NETWORK SECURITY

A model for much of what we will be discussing is captured, in very general terms, in Figure 1.4. A message is to be transferred from one party to another across some sort of Internet service. The two parties, who are the *principals* in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All of the techniques for providing security have two components:

1. A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.
2. Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.[7]

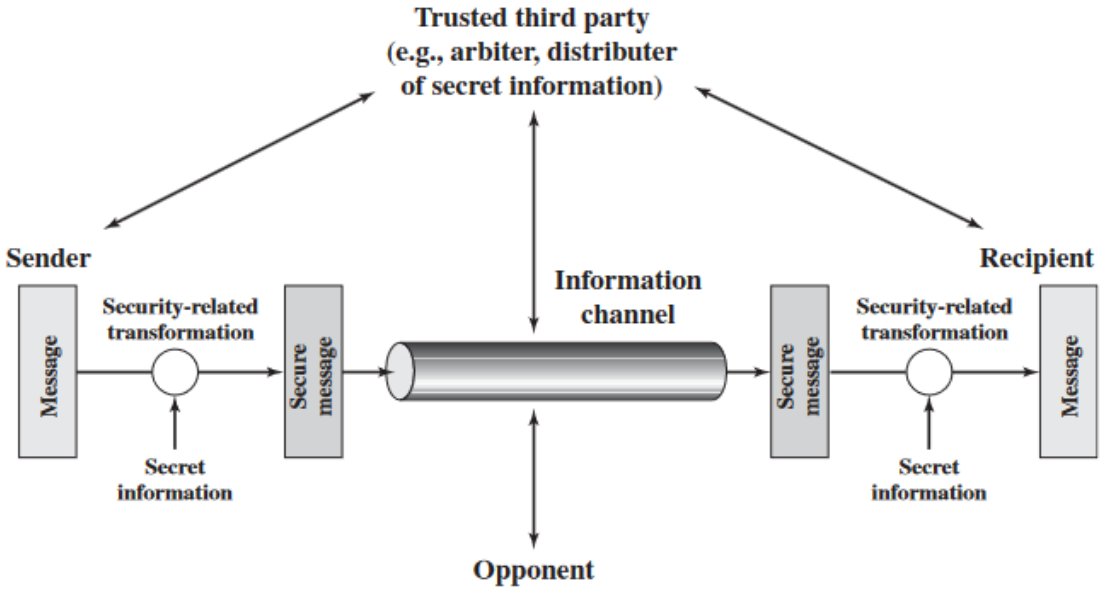


Figure 1.4 Model for Network Security

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

2.1 SYMMETRIC ENCRYPTION PRINCIPLES

A **symmetric encryption** scheme has five ingredients (Figure 2.1):

- **Plaintext:** This is the original message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key:** The secret key is also input to the algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
- **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.
- **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the same secret key and produces the original plaintext.

There are two requirements for secure use of symmetric encryption:

1. We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. This requirement is usually stated in a stronger form: The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.
2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

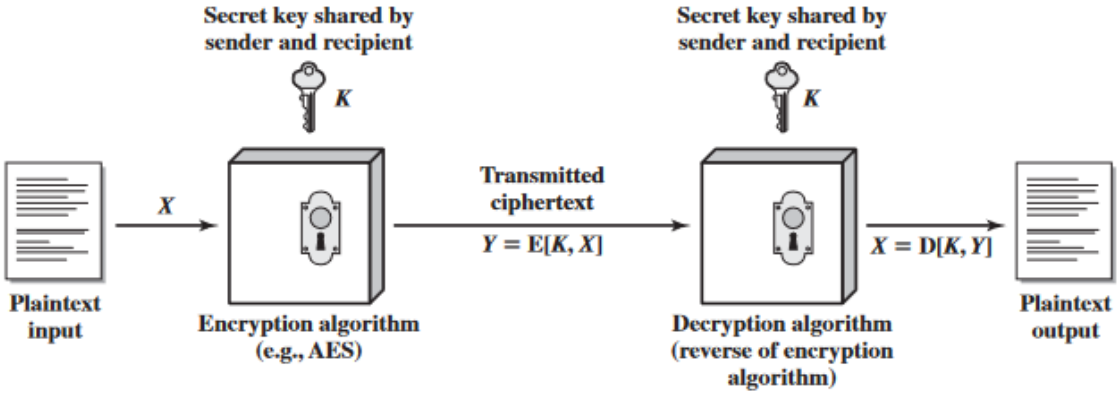


Figure 2.1 Simplified Model of Symmetric Encryption

Public key cryptography:

A public-key encryption scheme has six ingredients (Figure 3.9a).

- **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 and private key:** 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 encryption 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.

As the names suggest, the public key of the pair is made public for others to use, while the private key is known only to its owner. A general-purpose public-key cryptographic algorithm relies on one key for encryption and a different but related key for decryption.

The essential steps are the following:

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private. As Figure 3.9a suggests, each user maintains a collection of public keys obtained from others.
3. If Bob wishes to send a private message to Alice, Bob encrypts the message using Alice's public key.
4. When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

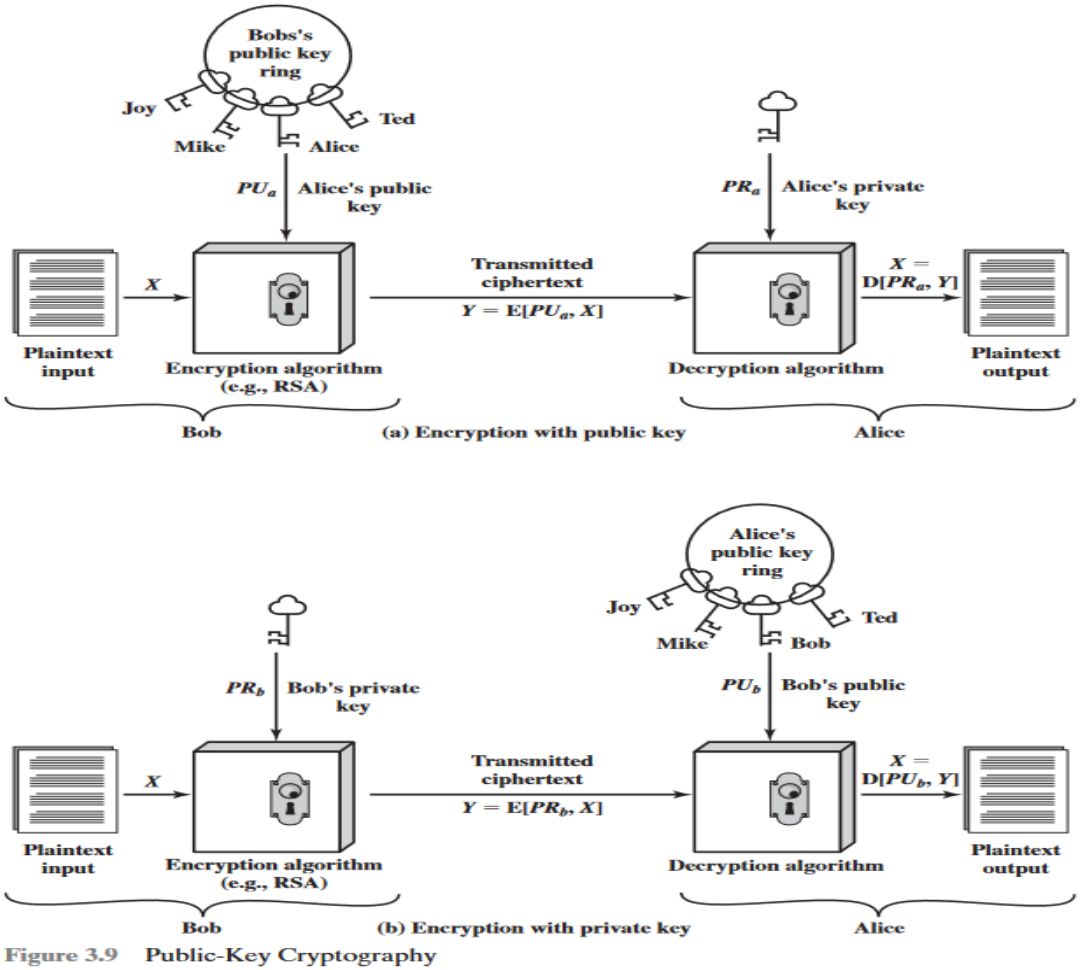
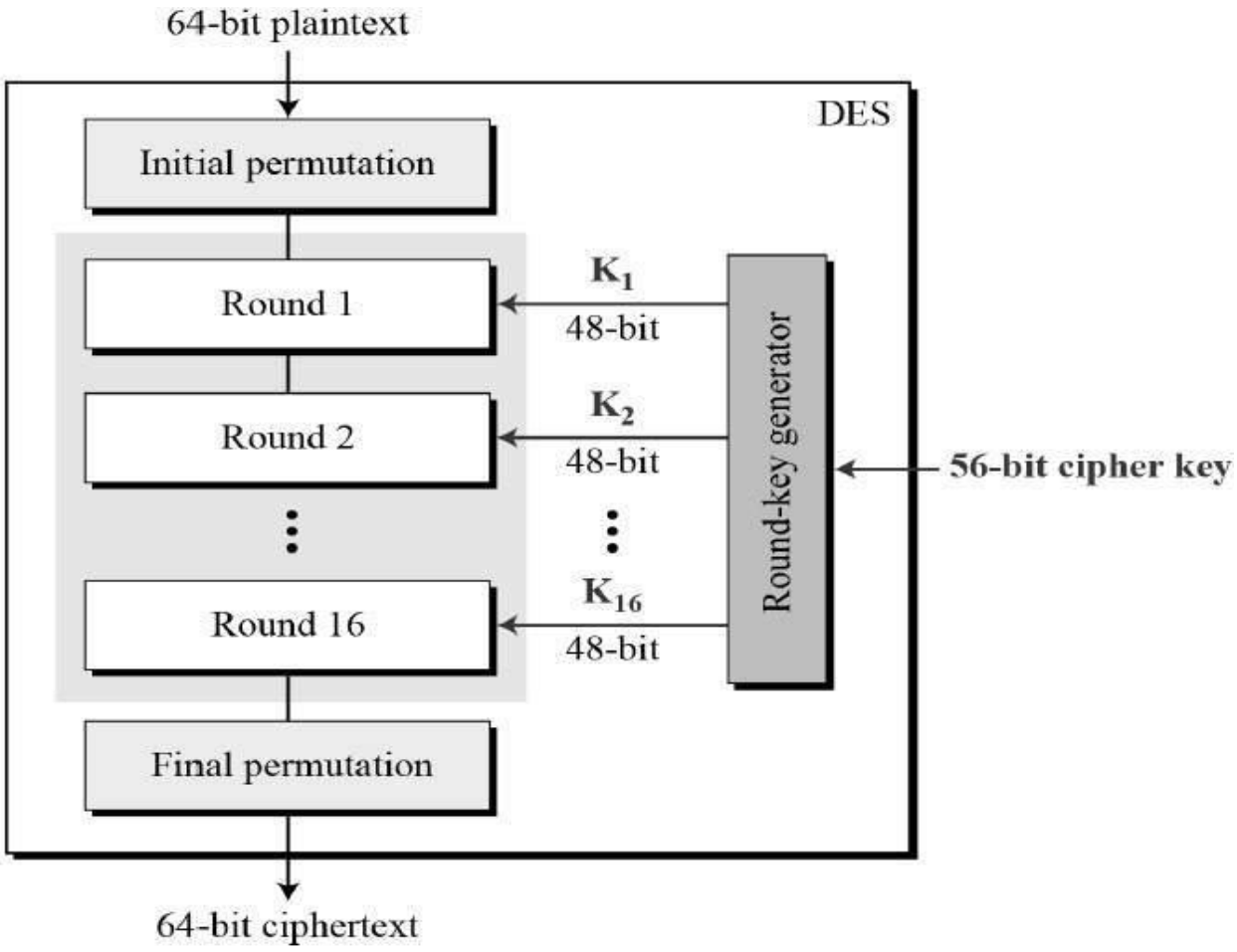


Figure 3.9 Public-Key Cryptography

Data Encryption Standard

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. 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). General Structure of DES is depicted in the following illustration −



Since DES is based on the Feistel Cipher, all that is required to specify DES is −

- Round function
- Key schedule
- Any additional processing − Initial and final permutation

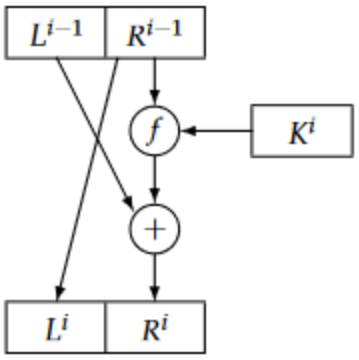


FIGURE 4.5: One round of DES encryption

$$\begin{aligned} L^i &= R^{i-1} \\ R^i &= L^{i-1} \oplus f(R^{i-1}, K^i). \end{aligned}$$

The f function is shown in Figure 4.6. Basically, it consists of a substitution (using an S-box) followed by a (fixed) permutation, denoted **P**. Suppose we denote the first argument of f by A, and the second argument by J. Then, in order to compute $f(A, J)$, the following steps are executed.

1. A is "expanded" to a bitstring of length 48 according to a fixed ***expansion function*** **E**. $\mathbf{E}(A)$ consists of the 32 bits from A, permuted in a certain way, with 16 of the bits appearing twice.

2. Compute $\mathbf{E}(A) \oplus J$ and write the result as the concatenation of eight 6-bit strings $B = B_1B_2B_3B_4B_5B_6B_7B_8$.

3. The next step uses eight S-boxes, denoted $S_1, \ldots, S_8$. Each S-box

$$S_i : \{0,1\}^6 \to \{0,1\}^4$$

maps six bits to four bits. Using these eight S-boxes, we compute $C_j = S_j(B_j)$, $1 \le j \le 8$.

4. The bitstring

$$C = C_1C_2C_3C_4C_5C_6C_7C_8$$

of length 32 is permuted according to the permutation **P**. The resulting bitstring $\mathbf{P}(C)$ is defined to be $f(A, J)$.

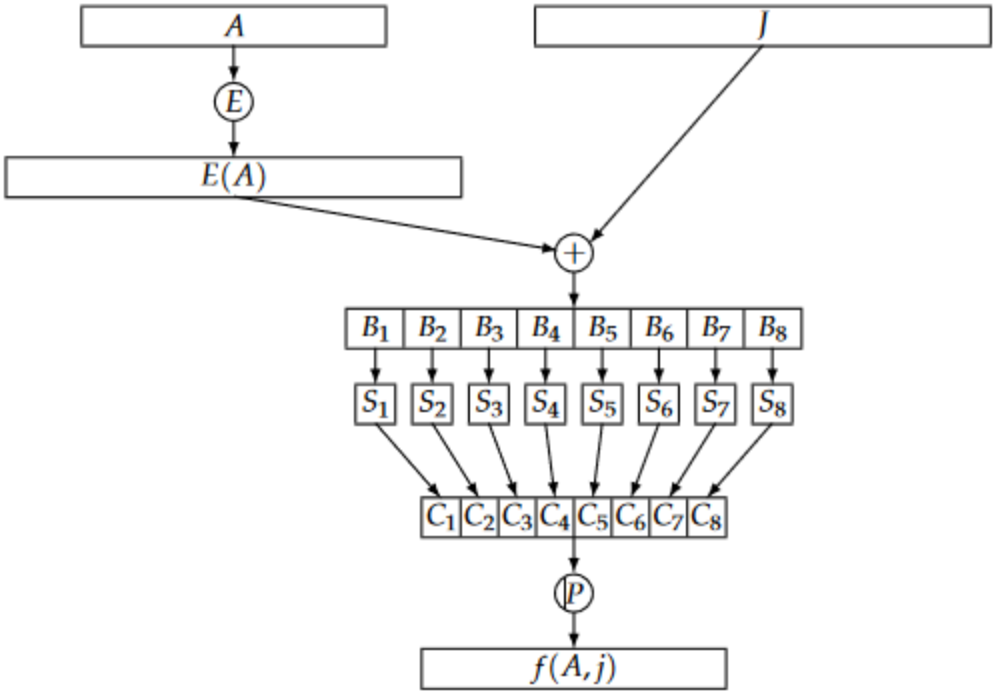
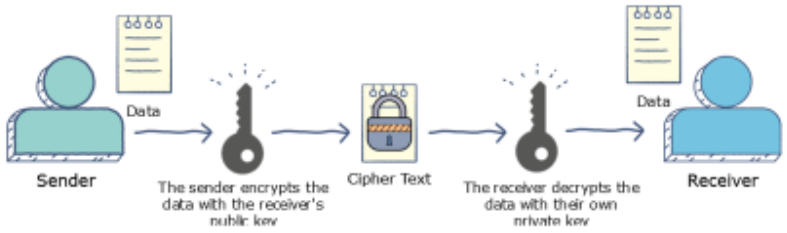


FIGURE 4.6: The DES f function

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.



Key Generation

Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext	$M < n$
Ciphertext	$C = M^e \pmod{n}$

Decryption

Ciphertext	C
Plaintext	$M = C^d \pmod{n}$

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and φ (n) are coprime. Let e = 7
- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$