DATA SECURITY

SECURITY GOALS

EXTC – BE – DATA COMPRESSION AND CRYPTOGRAPHY

Ms. Vandana Sawant

Assistant Professor

Dept. of Electronics & Telecommunication Engineering,

SIES Graduate School of Technology

SIES Graduate School of Technology
RISE WITH EDUCATION

QUESTIONS

- 1. What are the goals of cryptographic systems? Describe various attacks compromising these goals.
- What are the goals of cryptography? Explain anyone in detail.

OBJECTIVES OF LECTURE

- Students should be able to

  - Use various methods of data security.

DATA SECURITY

- Concept building:
- Assets: are something that have value and need to protected.
- Controls: any countermeasures or actions that you take to safeguard an asset are called controls.
- Threat: is a person or an entity that can exploit an asset by passing your controls(if they are weak)n instance of be
- Vulnerability: is of harm occurring to an asset is called risk.
- Exposure: is a instance of being harmed.

DATA SECURITY

- The asset of data security is information or more precisely Digital information.
- There are three tenets (or pillars) of security.
- 1. confidentiality
- 2. Integrity and
- 3. Availability
- These tenets in short called as CIA triad.
- These are also sometimes called goals of security.

DATA SECURITY

- Confidentiality:
- Confidentiality can be defined as, an act of protecting information from unauthorized disclosure to an entity.
- The information should be ;
- 1. Protected at rest
- 2. Protected in motion
- 3. Protected during use

DATA SECURITY

- Integrity:
- Integrity can be defined as, an act of protecting information from unauthorized modification by an entity.
- In terms of digital information integrity is enforced using several mechanisms:
- Hashing
- Access control
- Data classification
- Input and output sanitization.

DATA SECURITY

- Availability :
- Availability can be defined as, an act of protecting nformation from unauthorized destruction by an entity.
- Availability is generally enforced using several mechanisms:

1. Access control
2. Isolation
3. Back up
4. Disaster recovery
5. Business continuity process.

Types of security attacks

- What are active and passive attacks?
- Discuss types of attacks.
- Classify the different types of attacks and explain them with example

Types of security attacks

- I .Active Attacks :
- An active attack is defined as, an attack where the attacker actively participates in the communication or the attack mechanism and disrupts the systems by sending several manipulated inputs.
- Let us expand on some of examples of active attacks
- A. Replay attack:

Types of security attacks

- A. Replay attack:

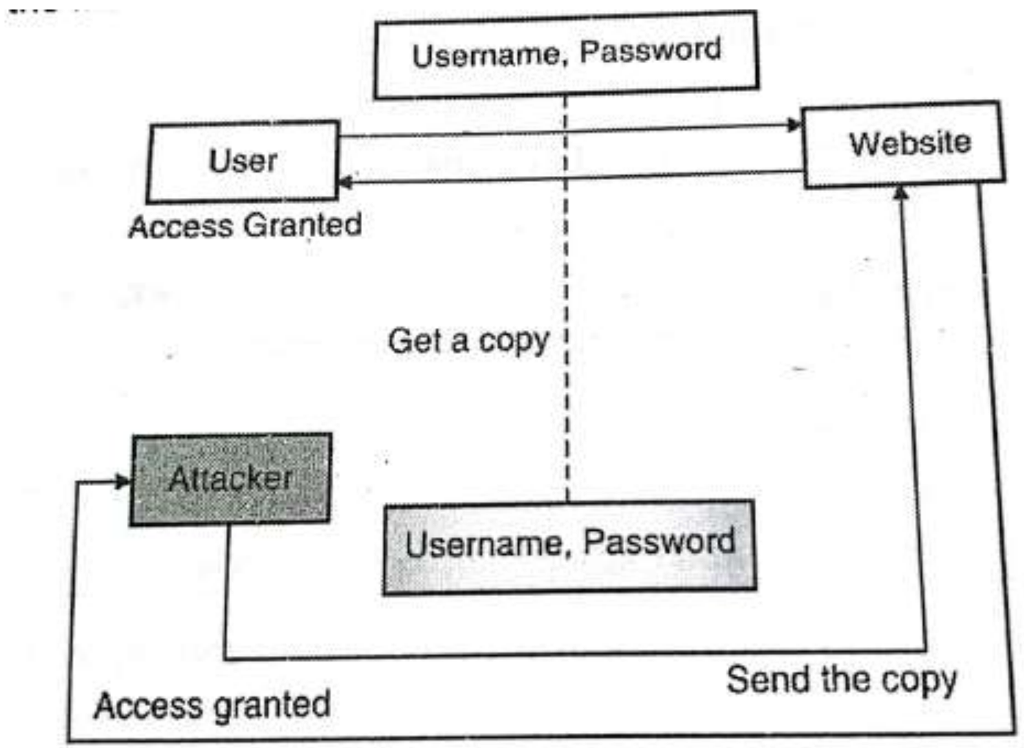


Fig. 4.4.2 : Replay attack

Types of security attacks

- A. Replay attack:
- Countermeasures:
- You can use timestamps and sequence numbers(also called as session ID). If a message comes with a sequence number that is already used previously, it can be rejected,
- Similarly, if a message comes with timestamp that is beyond the estimated threshold, it can be rejected.
- B. Denial of Service(Dos) attack:

Types of security attacks

- B. Denial of Service(Dos) attack:

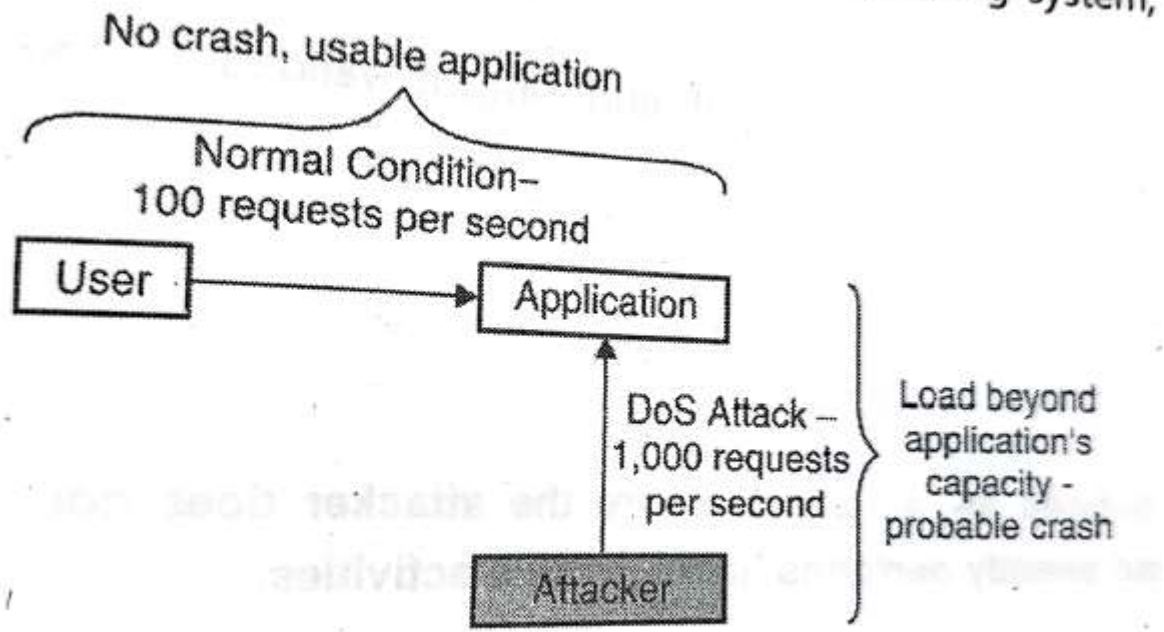


Fig. 4.4.3 : Denial of Service (DoS) attack

Types of security attacks

- B. Denial of Service(Dos) attack:
- Countermeasures:
- Some of the countermeasures to protect from Dos are firewall, application limit, whitelisting networks, etc.
- Firewall can be used to drop network connections that come from a particular location or based on other networking parameters (a list of allowed IP addresses, etc)
- Application limits can protect application from crashing when the rate of requests goes beyond a set limit.

Types of security attacks

- C . Fabrication attack:

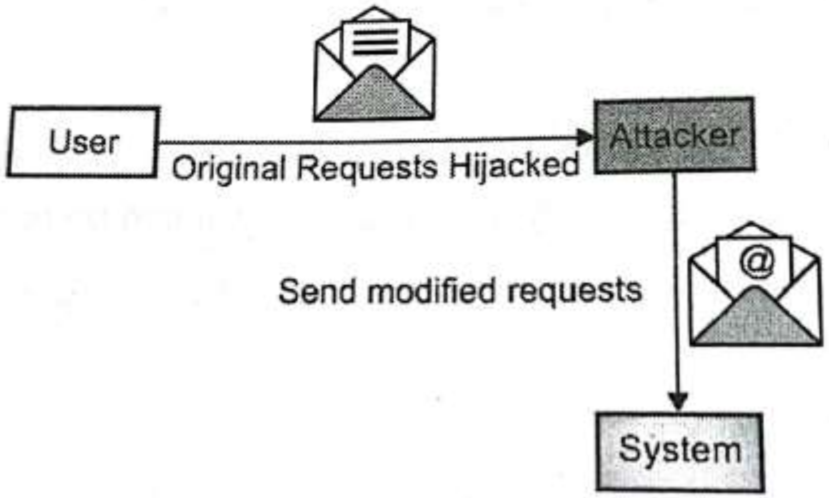


Fig. 4.4.4 : Fabrication attack

Types of security attacks

- C . Fabrication attack:
- Countermeasures:
- Hashing redundancy checks and input and output validation.

Types of security attacks

- II. Passive attack:
- A passive attack is defined as, an attack where the attacker does not alter the behaviour of the information system and silently performs her malicious activities.
- Let us expand on some of the examples of passive attacks
- A . Traffic analysis:

Types of security attacks

- A . Traffic analysis:

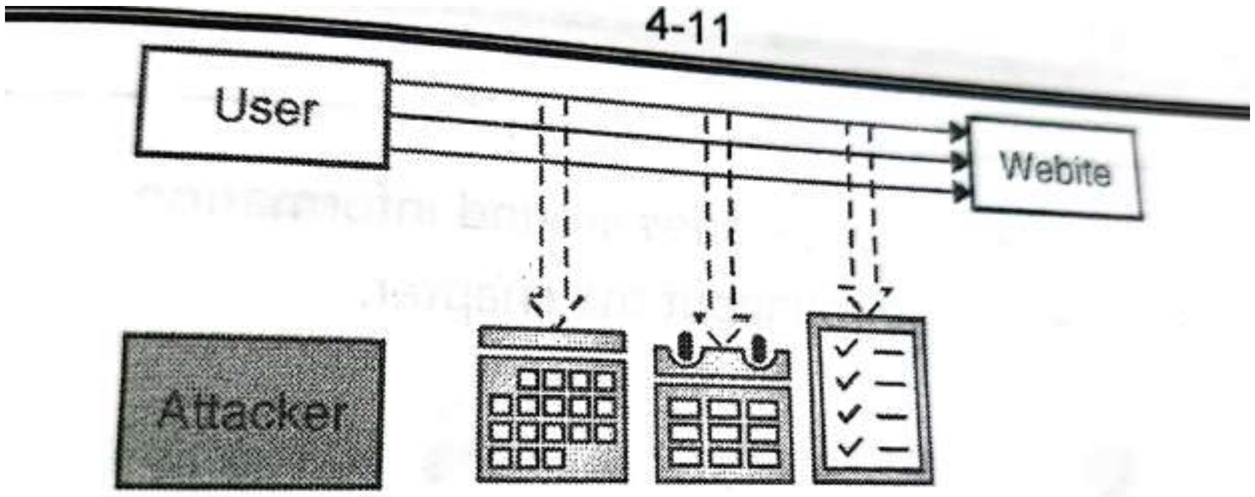


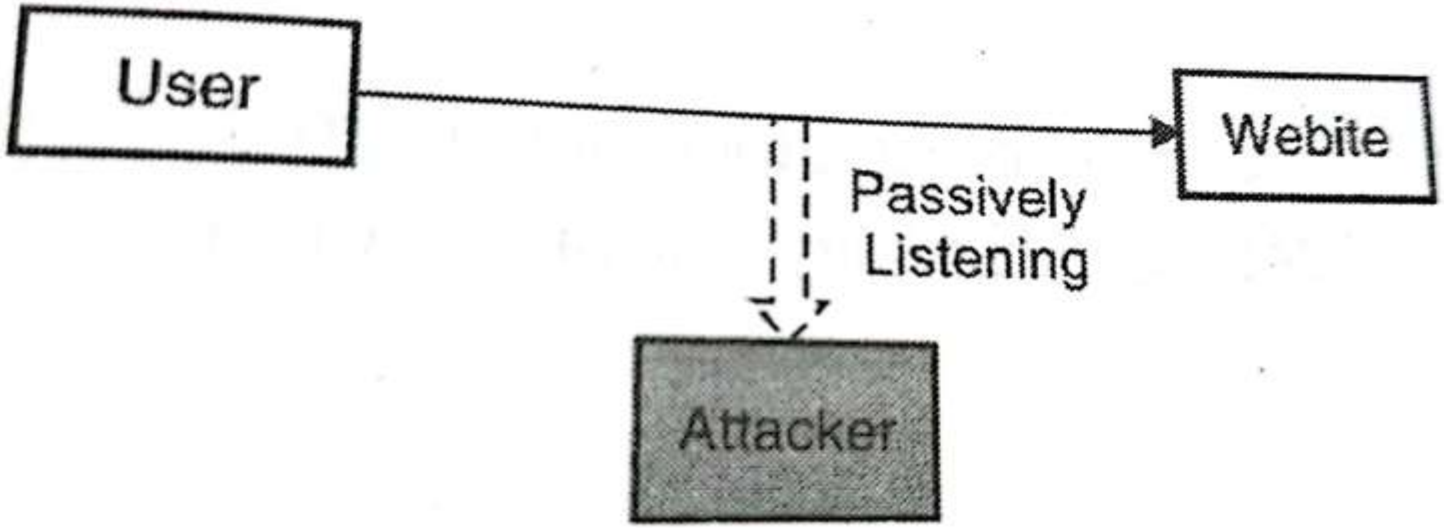
Fig. 4.4.5 : Traffic analysis

Types of security attacks

- A . Traffic analysis:
- Some of the countermeasures to traffic analysis is to randomize the communication or send fake traffic time to time to degrade the quality of information that the attacker can gather for analysis.

Types of security attacks

- B. Eavesdropping:



Types of security attacks

- B. Eavesdropping:
- Some of the countermeasures to eavesdropping is sending noise time to time or using random channels of communication.

Comparison of Active and Passive Attack

- ac

Sr. No.	Comparison Attribute	Active Attack	Passive Attack
1.	Complexity	High	Low
2.	Impact	High	Low
3.	Detection possibility	High	Low
4.	Prevention possibility	High	Low
5.	Duration of attack	Short	Long
6.	System behavior	Modified	Unaffected
7.	Original information	Modified	Unaffected
8.	Purpose	Harm the ecosystem	Learn about the ecosystem

Types of security attacks

- Give an example of substitution cipher.
- Give an example of transposition cipher.

Types of security attacks

- Substitution Cipher:
- In this operation, one character is replaced by another (like substitutes in games)
- Ex : A can be substituted by D and B can be substituted by E and so on based on a chosen substitution key.
- Characters such as y when shifted take the form of y→z, z→a, a→b
- The above example is a classical substitution cipher called Caesar cipher named after Julius Caesar.
- This type of substitution cipher is also referred to as a monoalphabetic substitution cipher because it uses only character at a time. Another type of substitution cipher is called "polyalphabetic substitution cipher"
- In this more than one alphabet is used at a time for encrypting plaintext.

Types of security attacks

- Substitution Cipher:

Table 4.5.2 : Simple substitution table

Plaintext	Ciphertext
I love cybersecurity	L oryhfbehuvhfxulwb
Apple	Dssoh
23456	56789

Types of security attacks

- Transposition Cipher:
- Transposition cipher, the position of character is jumbled up (mixed up) like a letters arranging gapmes.
- e.g the plain text apple could be transposed in to cipher text as elpap
- Note that all character in plain text are also present in the cipher text but at a different position.
- Note that it is a very simplistic example .various complex mathematical transposition algorythems are usually used in cryptography.

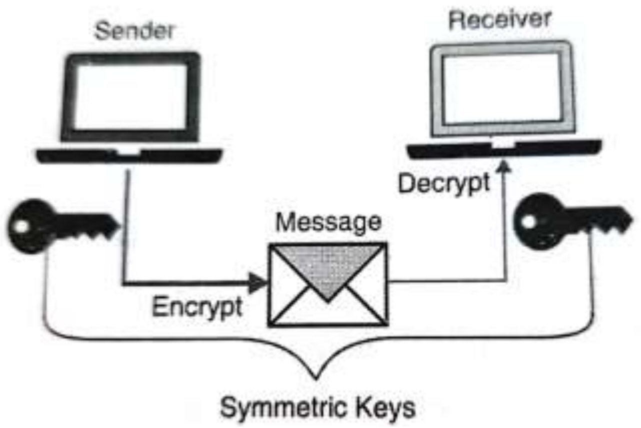
Symmetric key Encryption

- Explain DES with neat block diagram.
- Give an example of black cipher.
- Give an example of stream cipher.
- Explain working of standard DES with suitable diagram.

Symmetric key Encryption

- In symmetric key encryption the key used for encryption is same as the key used for decryption.
- Ex its like regular lock key
- If there are more entities involved and each require to secretly communicate with the another, you end up having multiple keys.
- No of keys required can be calculated as
- K=(N-1)/2---N=no of entities
- For ex. If there are 4 entities(user) then K=6
- If sender and receiver have to use same key, there should be way to securely transfer the key.

Symmetric key Encryption



1. A <> B
2. A <> C
3. A <> D
4. B <> C
5. B <> D
6. C <> D

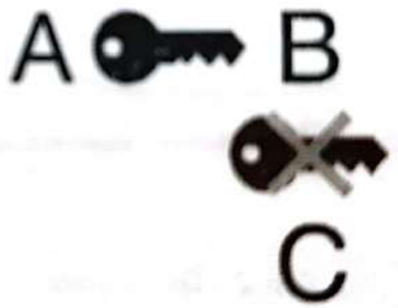


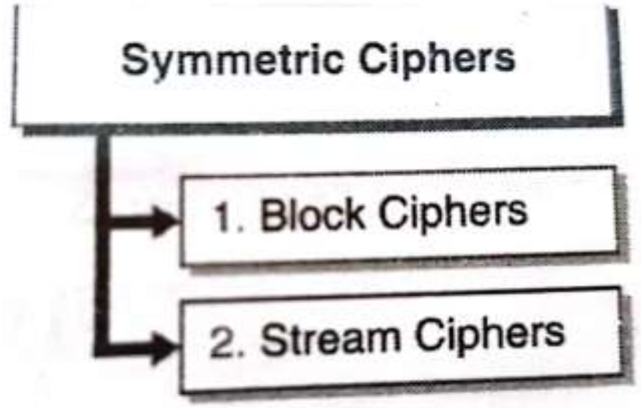
Fig. 4.6.4

Symmetric key Encryption

- Advantages of symmetric keys:
- 1. computationally faster than the asymmetric keys
- 2. hard to break if the key used is long
- Disadvantages of symmetric keys:
- 1. requires a secure mechanism to exchange keys.
- 2. each pair of sender and receiver require a unique key.
- 3. provides only confidentiality but not authenticity and non repudiation.

Types of Symmetric algorithms(ciphers)

- symmetric key based algorithms can work either on blocks of bits or one bit at a time.



- Algorithms that work on blocks are called block ciphers
- Algorithms that work on one bit at a time are called stream ciphers.

Block ciphers

- Algorithms that work on blocks are called block ciphers
- Block ciphers, the information that needs to be encrypted is broken into smaller and equal block sizes.
- If block size has lesser number of characters than required to form block then padding is done to fill the block
- Then encryption operation is applied to each block.
- The resultant ciphertext from each block is ten combined to produce the encrypted information.
- As shown in diagram
- Data encryption standard(DES) and advanced encryption standard(AES) are two of the examples of symmetric block chippers.

Block ciphers

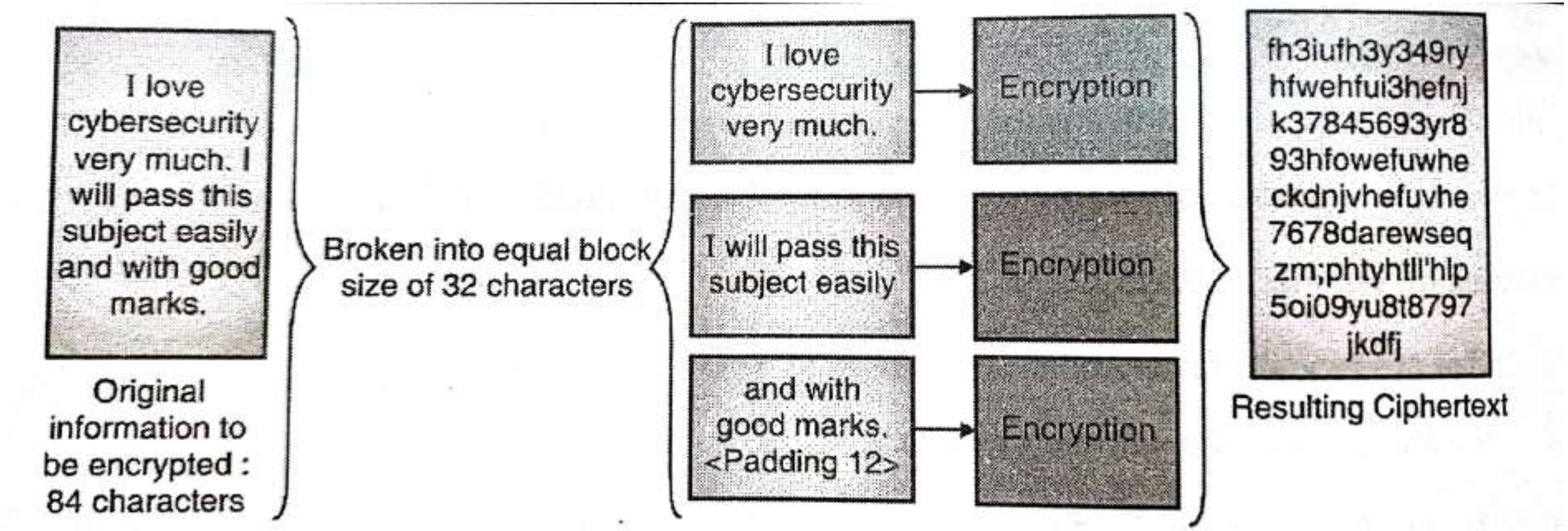


Fig. 4.7.2 : Block Ciphers

Stream ciphers

- Algorithms that work on one bit at a time are called stream ciphers.
- Each bit of plaintext is combined with the bits of security key and then XOR

ed to get

ciphertext.

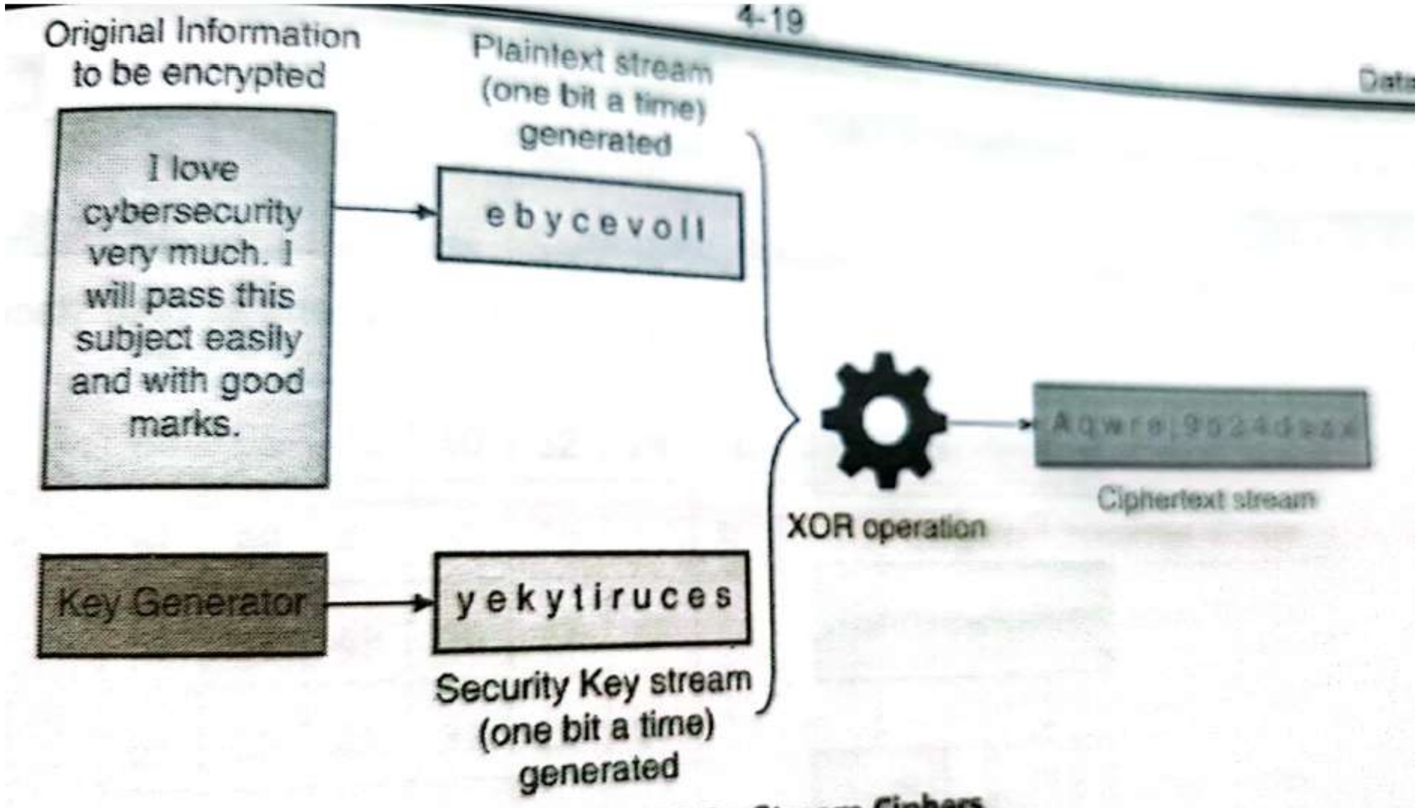


Fig. 4.7.3 : Stream Ciphers

Comparison between block and Stream ciphers

Sr. No.	Comparison Attribute	Block Cipher	Stream Cipher
1.	Security	High	Low
2.	Speed	Low	High
3.	Application	Non-real time such as documents	Real time data such as Voice
4.	Commonly used	Yes	No

Data encryption standards

- Data encryption standard (DES) is symmetric key based block cipher standard used for encryption and decryption.
- Major attributes of DES:
- It is symmetric key based algorithm
- It works as a block cipher
- It uses 64 bit blocks
- It uses key size of 64 bits in which 56 bits are the actual keys and 8 keys are used for error detection
- It uses 16 rounds of operation to convert a block of plaintext into ciphertext.
- DES is now considered insecure and obsolete due to its short key size

Block diagram of Data encryption standards

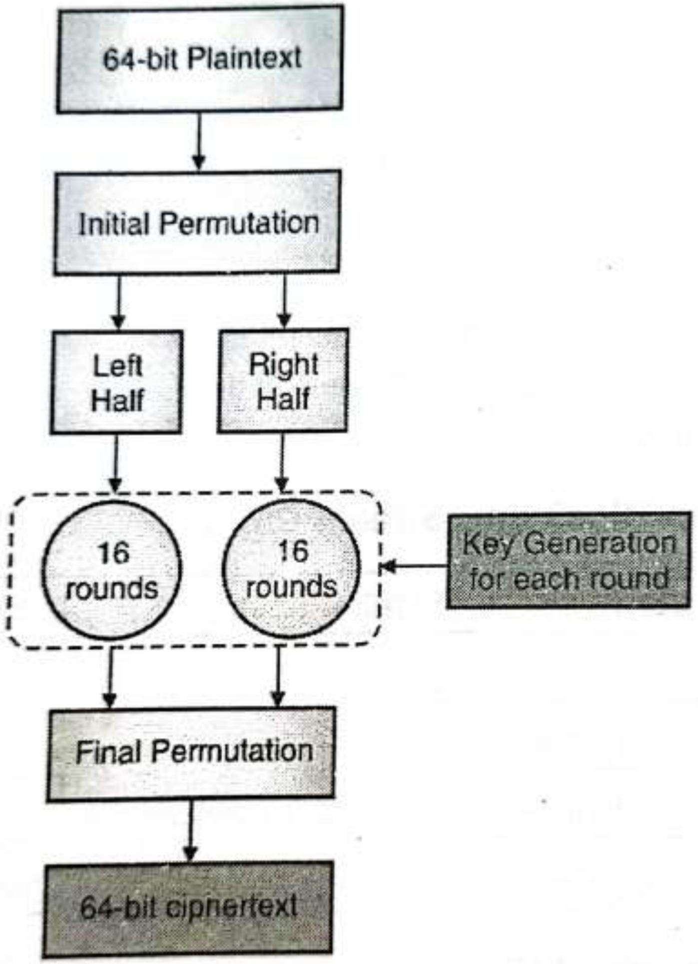


Fig. 4.8.1 : Block diagram of DES

Block diagram of Data encryption standards

- Step 1 : creation of 64 bit blocks

Table 4.8.1 : 64 bits of plaintext

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Block diagram of Data encryption standards

- Step 2 : initial permutation

4-21

Table 4.8.2 : Initial Permutation (re-arrange bits of plaintext)

58	50	42	34	26	18	10	2	← Column 2 becomes 1st row
60	52	44	36	28	20	12	4	← Column 4 becomes 2nd row
62	54	46	38	30	22	14	6	← Column 6 becomes 3rd row
64	56	48	40	32	24	16	8	← Column 8 becomes 4th row
57	49	41	33	25	17	9	1	← Column 1 becomes 5th row
59	51	43	35	27	19	11	3	← Column 3 becomes 6th row
61	52	45	37	29	21	13	5	← Column 5 becomes 7th row
63	55	47	39	31	23	15	7	← Column 7 becomes 8th row

Block diagram of Data encryption standards

- Step 3 : left half and right half split each containing 32 bits
- These individual 32 bit blocks are then continuously worked through the 16 rounds of operation.

Block diagram of Data encryption standards

- Step 4 : Subkey generation
- For the 16 rounds of operation, a unique subkey is derived for each round from the 56 bit key
- the key is derived using complex mathematical functions. Each generated subkey is 48 bit long.

Block diagram of Data encryption standards

- Step 5 : Rounds
- Left half and the right half both individually go to 16 rounds of encryption operation.
- In each of the rounds the derived subkey is used to produce temporary chiphertext which is used in next round until the final round is complete.
- Each round consists of substitutions and successive permutations.

Block diagram of Data encryption standards

- Step 6 : Final permutation
- In the last stage we need to bring the bits back to their respective positions.
- The bit positions were changed at the initial permutation stage.

Block diagram of Data encryption standards

- Step 6 : Final permutation

Table 4.8.3 : Final permutation (re-arrange bits of ciphertext)

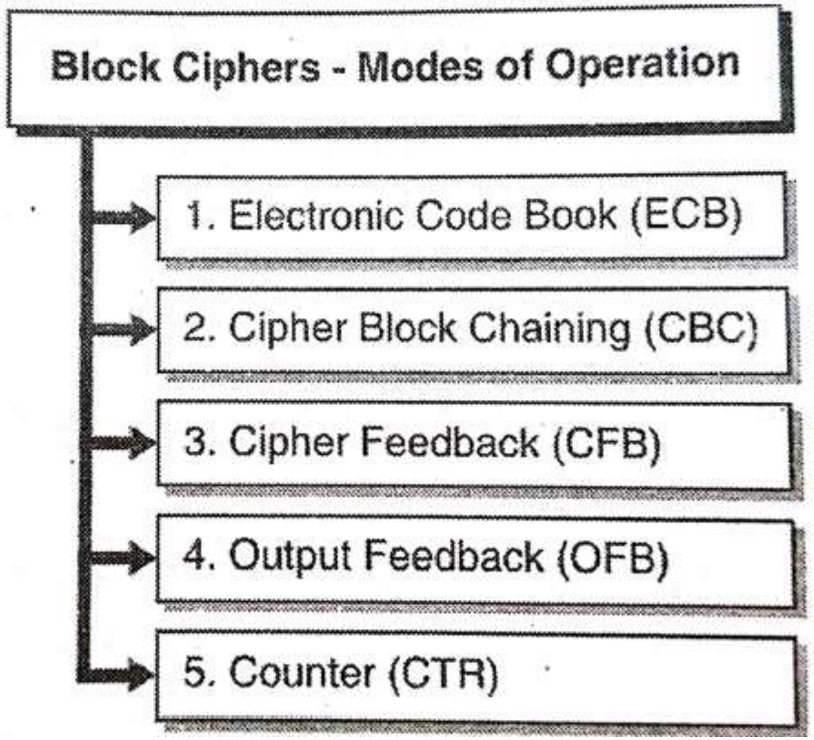
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Block diagram of Data encryption standards

- Step 7 : Final ciphertext
- Once all the steps are done you get the final ciphertext for the plaintext given the security key of your choice via DES.

Working of standard Data encryption standards

- Modes of operation for block ciphers



Working of standard Data encryption standards

- 1. electronic code book Mode

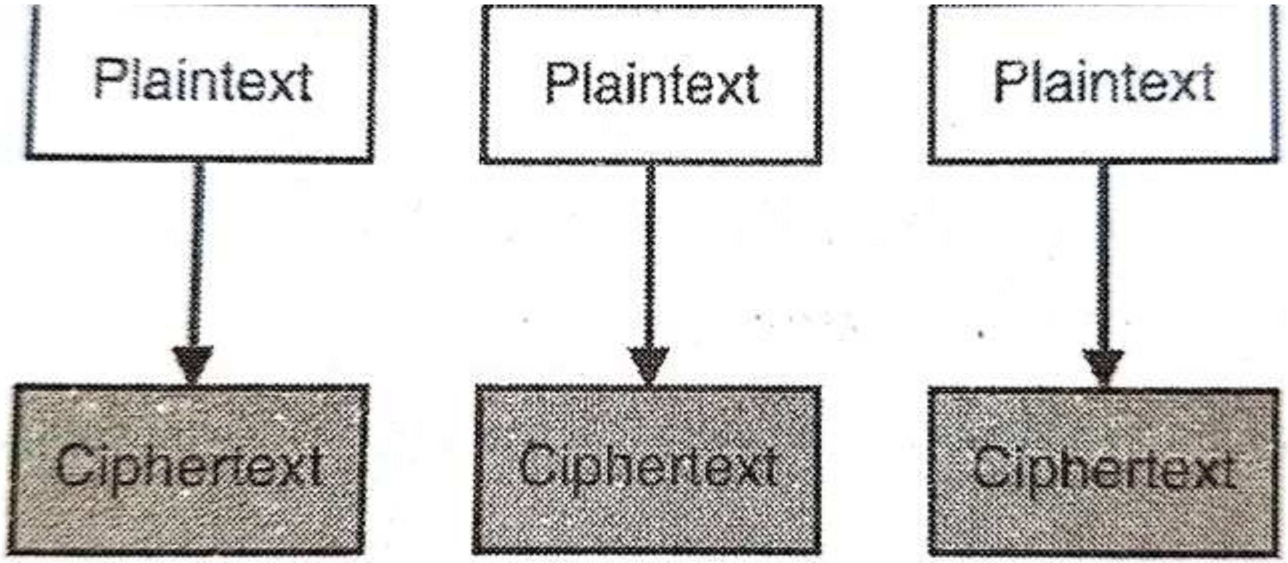
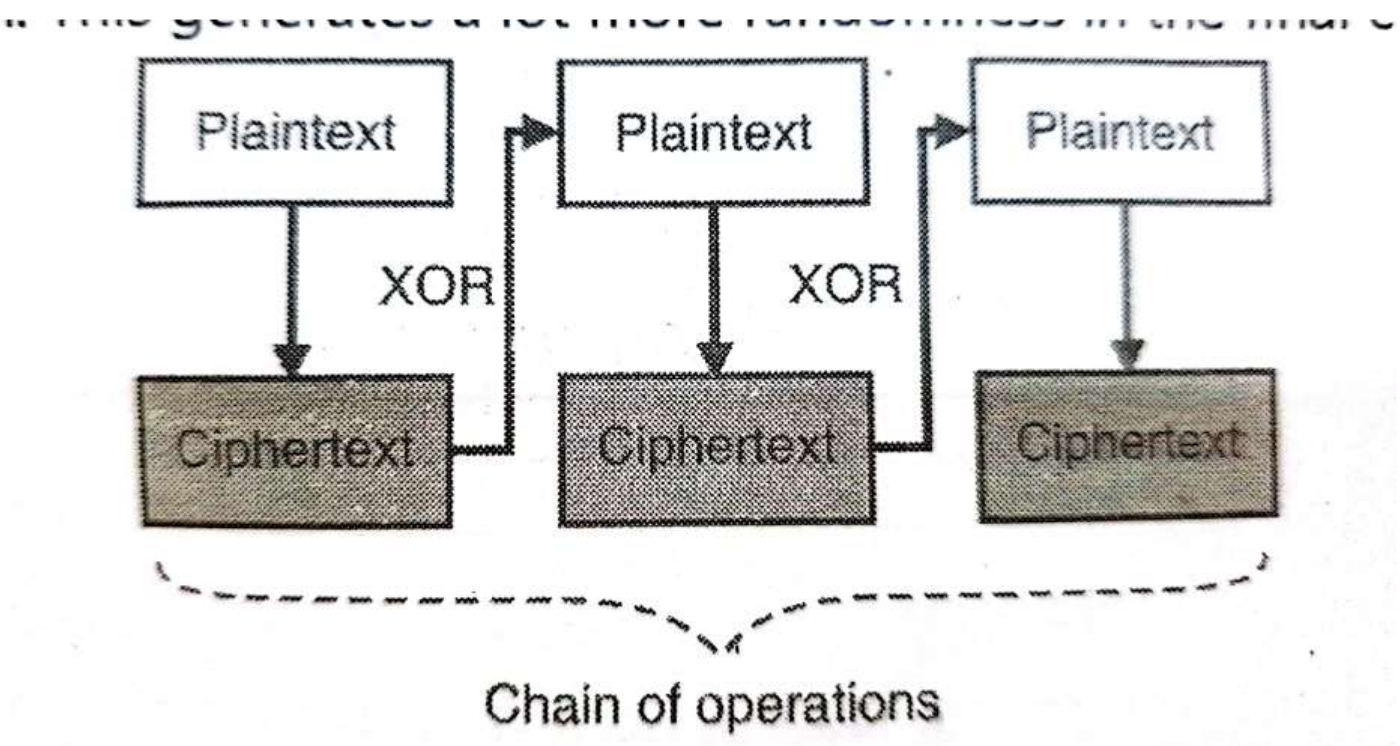


Fig. 4.8.3 : Electronic Code Book (ECB) Mode

Working of standard Data encryption standards

- 2. cipher block chaining Mode



Working of standard Data encryption standards

- 3. cipher feedback Mode

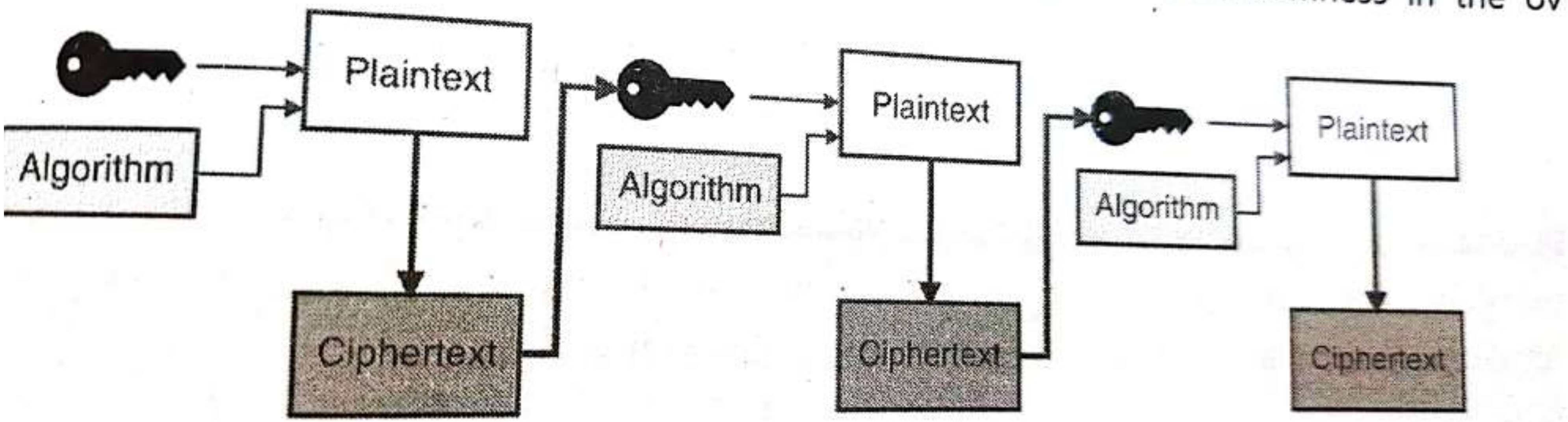


Fig. 4.8.5 : Cipher Feedback (CFB) Mode

Working of standard Data encryption standards

- 4. output feedback Mode

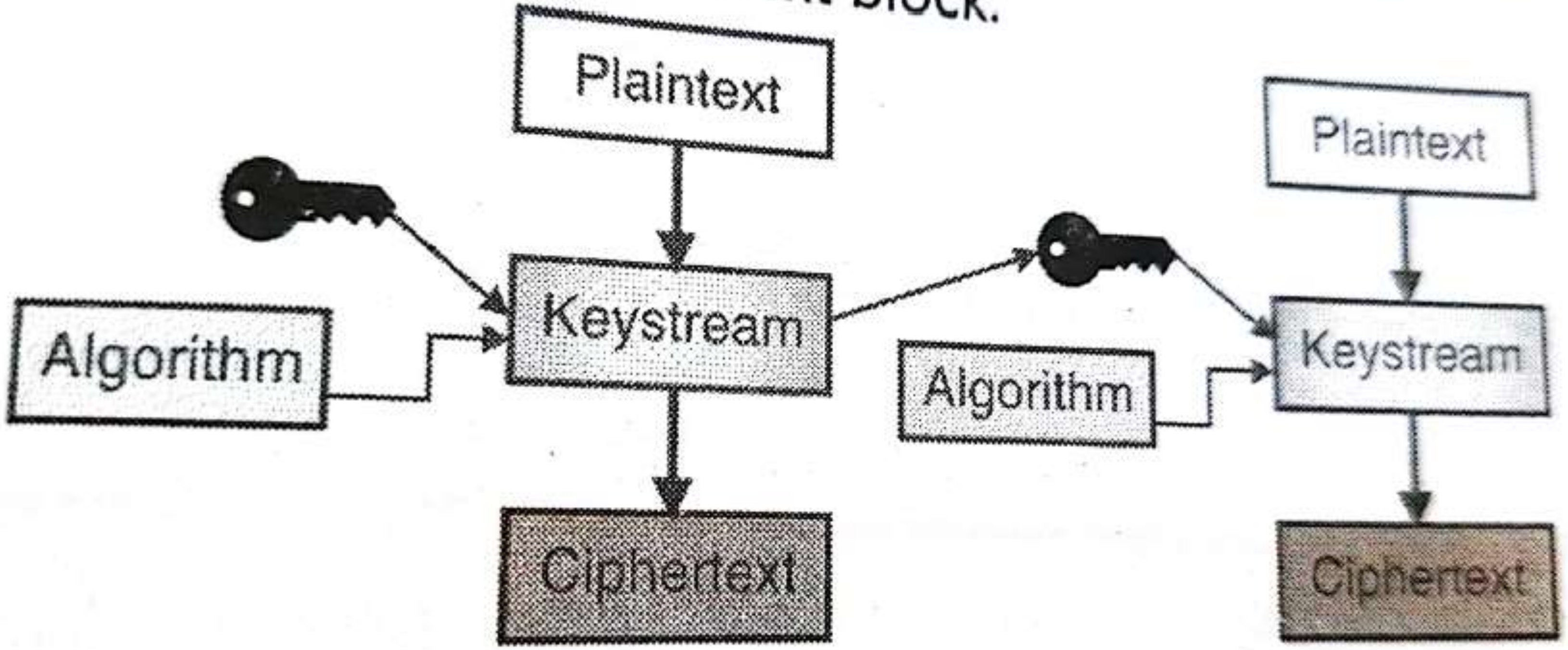


Fig. 4.8.6 : Output Feedback (OFB) Mode

Working of standard Data encryption standards

- 5. counter Mode

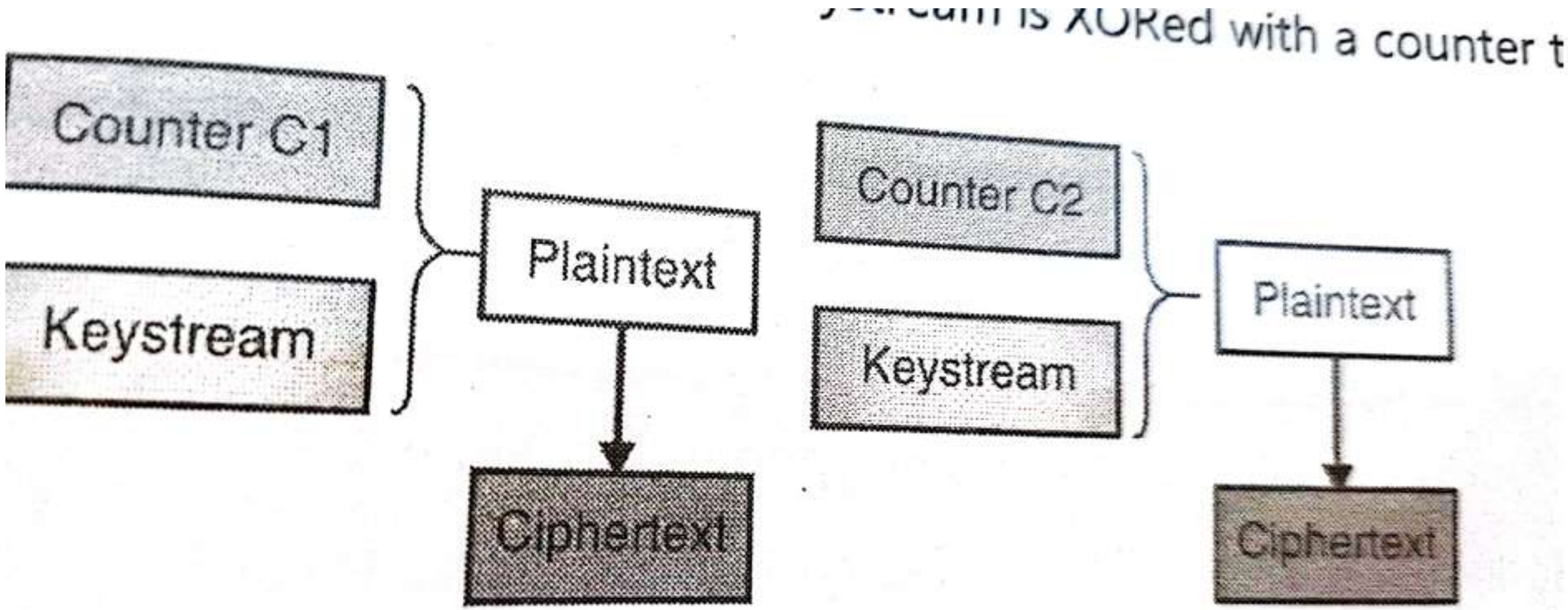


Fig. 4.8.7 : Counter (CTR) Mode

Fig. 4.8.7 : Counter (CTR) Mode

4.8.3 Comparison between Modes of Operation :

Sr. No.	Mode	ECB	CBC	CFB	OFB	CTR
1.	In-Parallel block encryption	Yes	No	No	No	Yes
2.	Suited for	Small Information	Any size of information	Small Information	Small Information	Any size of information
3.	Security and randomness	Low	High	High	High	High
4.	Speed	High	Medium	Medium	Medium	High
5.	Complexity	Low	High	High	High	Low
6.	Works like stream cipher?	No	No	Yes	Yes	Yes

Weakness in DES :

Double Data encryption standards

- Explain the double DES and the need for it. Also explain the meet in the middle attack.

Double Data encryption standards

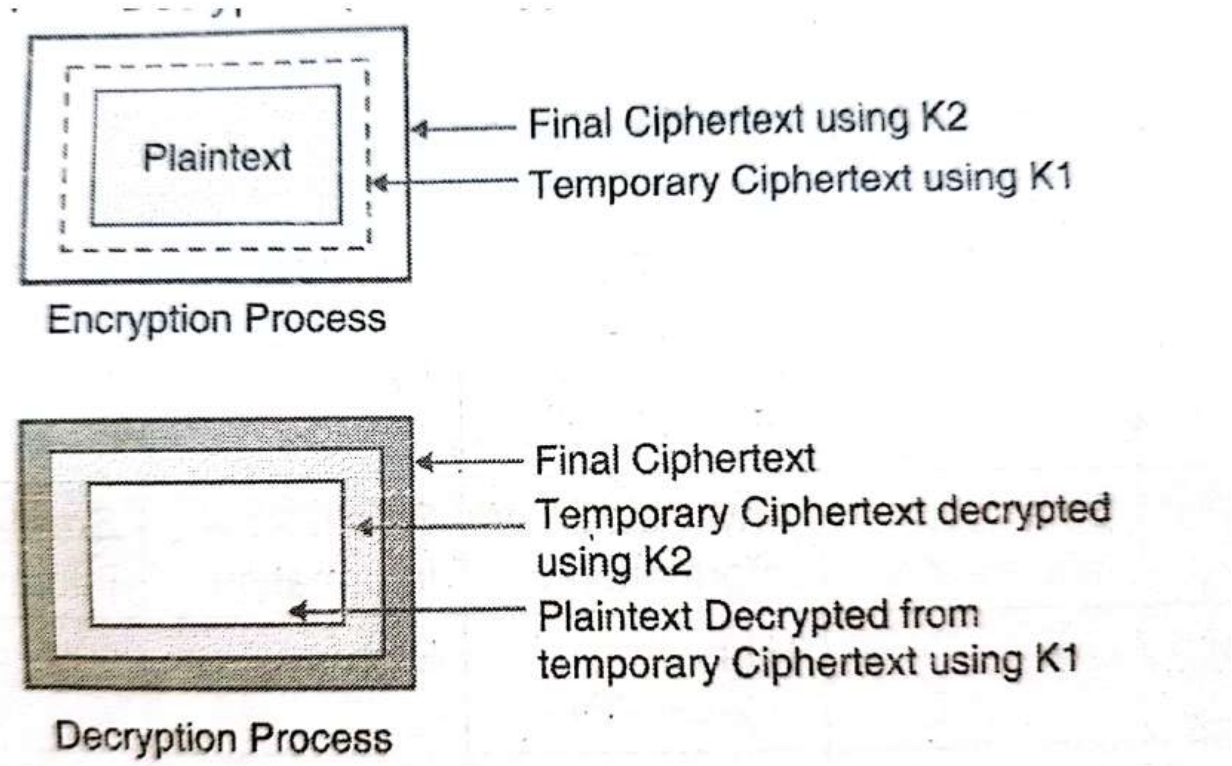


Fig. 4.8.8 : Double DES

Double Data encryption standards

- However double DES was proven to be ineffective. Meet in the middle attack was shown to reduce the complexity to just 2^{57} instead of $2^{112} as\ originally\ thought.$
- So using K1 if you could derive temporary ciphertext using encryption process and using K2 if you could also derive the same temporary ciphertext using decryption process, you have found a match and the keys you chose (K1 and K2)are now known to you.
- Hence you could effectively find both the keys and break double DES without original thought of complexity of 112 bits.
- Hence double DES was not adopted in the industry and is not used.

Double Data encryption standards

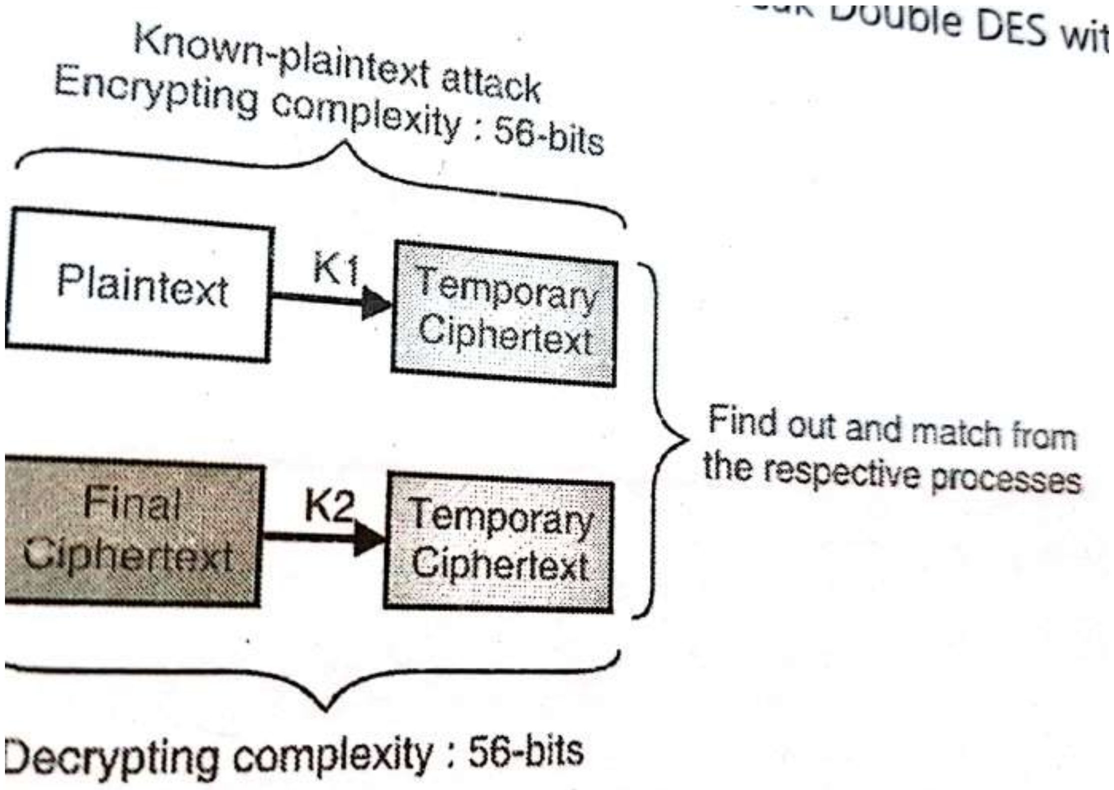


Fig. 4.8.9 : Complexity in Double DES

3DES or Triple Data encryption standards

- Explain triple DES with two keys and meet in middle attack.
- Explain working of triple DES with two and three keys.
- Write short not on AES

3DES or Triple Data encryption standards

- 3DES uses 48 rounds of operation and can work in the following modes using two or three keys as shown in table

Table 4.8.4 : 3DES or Triple DES

Sr. No.	Mode	Number of keys	Key 1	Key 2	Key 3
1.	DES-EEE3	3	Encryption	Encryption	Encryption
2.	DES-EDE3	3	Encryption	Decryption	Encryption
3.	DES-EEE2	2	Encryption	Encryption	Encryption Using Key 1
4.	DES-EDE2	2	Encryption	Decryption	Encryption Using Key 1

3DES or Triple Data encryption standards

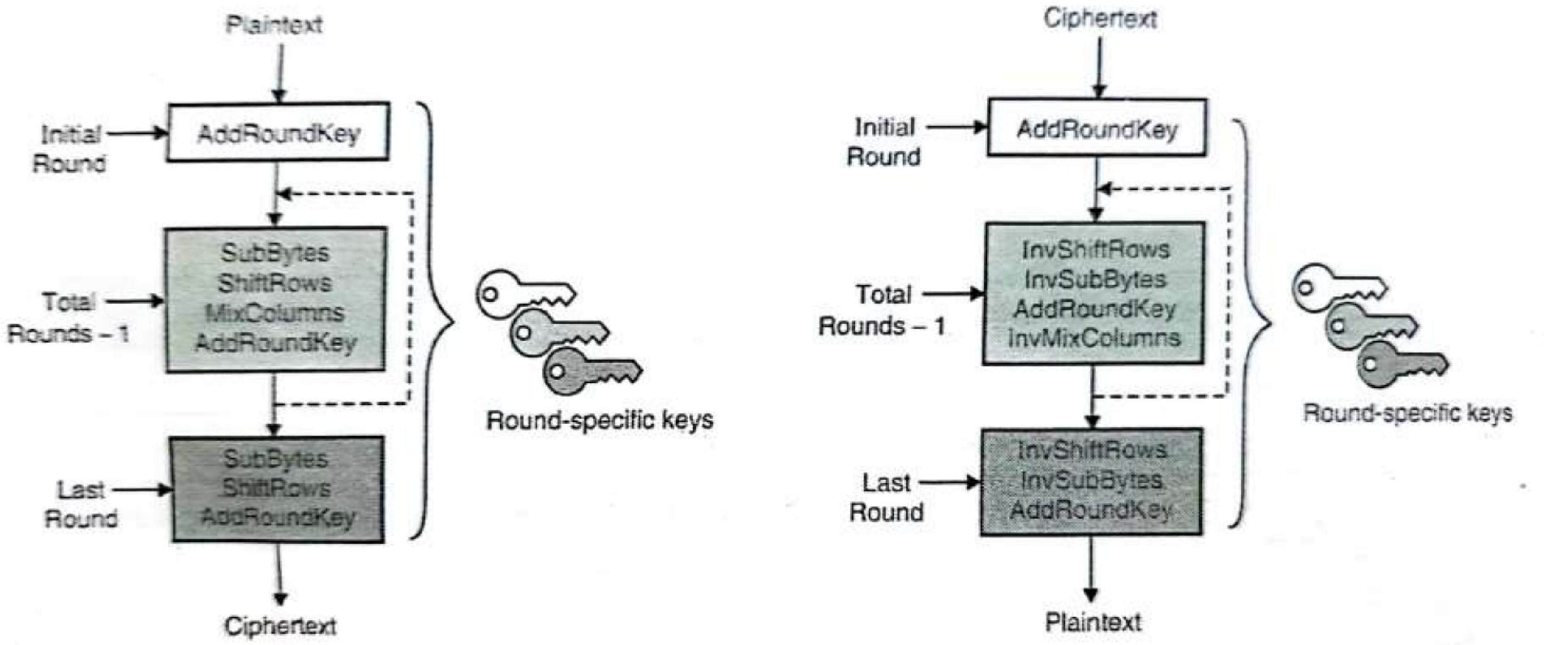
- Note that if you encrypt a plaintext using a key say K1 and run the decryption process using different key say K2 the text becomes more random.
- And hence helps to make attacks such as linear or differential cryptanalysis extremely hard.

Fig. 4.8.10 : Decryption process

Advanced encryption standards

- Advanced encryption standard (AES) is a symmetric key based block cipher standard used for encryption and decryption.
- Major attributes of AES:
- It is asymmetric key based algorithm.
- It works as a block cipher.
- It uses 128 bit blocks
- It can work with key sizes of 128,192 and 256 bits
- number of rounds of operation depends upon the key size
- 128 bit-10 rounds
- 192 bit-12 rounds
- It is considered highly secure due to its long key sizes and is used in the industry today

Detail steps for Advanced encryption standards



(a) AES Encryption Process (b) AES Decryption Process

Fig. 4.9.1 : Block diagram of AES

Detail steps for Advanced encryption standards

- 1. addroundkey:
- 2. subbytes
- 3.shiftrows
- 4. mix columns
- 5. invsubbytes
- 6. invshiftrows
- 7. inv columns

...ption process.

This is inverse of MixColumns operation. It is used in the decryption process.

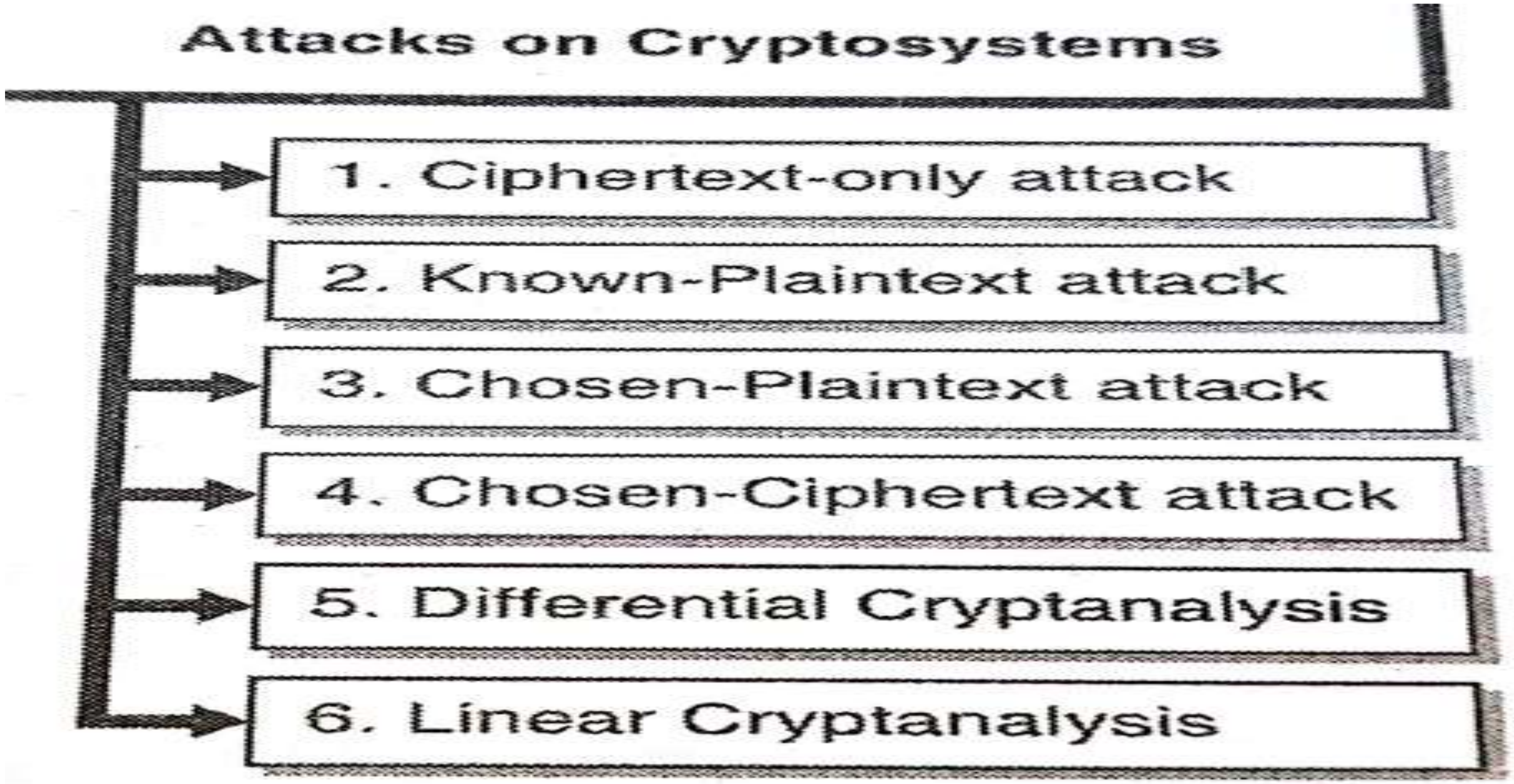
4.9.2 Comparison between DES and AES :

Sr. No.	Comparison Attribute	DES	AES
1.	Cryptographic Strength	Low	High
2.	Key Size	56-bit	128, 192 and 256 bits
3.	Block Size	64-bit	128-bit
4.	Rounds	16	10, 12, 14 - based on key size
5.	Usage	Obsolete - Not used	Currently used industry standard

4.10 Cryptographic Attack Techniques :

SIES Graduate School of Technology
RISE WITH EDUCATION

Cryptographic attack techniques



Cryptographic attack techniques

- Ciphertext only attack
- Known plaintext attack
- Chosen plaintext attack
- Chosen ciphertext attack
- Differential cryptanalysis
- Linear cryptanalysis

...y values. ... process and tries to find out the probability

4.10.1 Comparison between Differential and Linear Cryptanalysis :

Sr. No.	Comparison Attribute	Differential Cryptanalysis	Linear Cryptanalysis
1.	Plaintext selection	Carefully chosen	Any random plaintext
2.	Plaintext used	In pairs	One by one
3.	Complexity of attack	High	Low
4.	Mathematical relation between plaintexts used	Specific differences (such as XOR)	Linear approximation (such as a series of XOR operations)
5.	Goal of the attack	Identify some bits of the unknown key	Identify the linear relation between some bits of the plaintext, some bits of the cipher text and some bits of the unknown key

SIES Graduate School of Technology
RISE WITH EDUCATION

Thank You!

(vandanas@sies.edu.in)

SIES
Graduate School of Technology
RISE WITH EDUCATION