

---

## [CS309] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy

Scribed by: Kunj Thakkar (202251142)

Autumn 2024-2025

Lecture (Week 4)

---

# 1 Attack Models

Cryptographic attack models describe different scenarios in which the attacker might try to break cryptographic algorithms and encryption systems in order to look at information which is not intended to be secret. There are 4 different type of attacks possible below are listed in detail:

## 1.1 Cipher Text only attack

### Description

This is very basic attack model. Attacker only have access to cipher text which is encrypted with some encryption algorithm

### Attacker's Knowledge

- The encrypted text (*Cipher Text*)
- The encryption algorithm used (but not the key)

### Attackers goal

- recovery of plain text
- recovery of key

### Success Criteria

- **Complete Break:** if attacker is successful in recovering the key
- **Partial Break:** if attacker can deduce some non-random information or partial plain text

### Difficulty

This is the most difficult attack model as attacker have the least amount of knowledge in this.

## 1.2 Known Plain Text Attack

### Description

In this attack model, attacker has access to cipher text as well as some part of plain text

### Attacker's Knowledge

- Some plain text-cipher text pairs
- The encryption algorithm used

### Attackers goal

- Decrypt new cipher texts which are not part of known plain texts
- Recovery of the key

### Success Criteria

if the attacker can decrypt new cipher texts or can gain the key

## 1.3 Chosen Plain Text Attack

### Description

This model assumes that the attacker can choose arbitrary plain text and can obtain their corresponding cipher texts.

### Attacker's Knowledge

- can select any plain text
- can obtain corresponding cipher texts for chosen plain texts

### Attackers goal

- Decrypt the cipher texts
- Recovery of the key

## 1.4 Known Cipher Text Attack

### Description

In this model, the attacker can choose arbitrary cipher texts and obtain their corresponding decrypted plain text.

### Attacker's Knowledge

- can select any cipher texts
- can obtain corresponding plain text for chosen cipher text

### Attackers goal

- Decrypt other cipher texts
- Recovery of the key

## 1.5 Comparative Analysis

For comparative analysis we will address this attack models with their abbreviations

- Cipher Text Only Attack: COA
  - Known Plain Text Attack: KPA
  - Chosen Plain Text Attack: CPA
  - Chosen Cipher Text Attack: CCA
1. Increasing Order of attacker's advantage:  $COA < KPA < CPA \approx CCA$
  2. Robustness of Encryption: If an algorithm is secure against stronger attacks(e.g., CPA), its generally secure against weaker ones(e.g., COA)

## 2 CryptAnalysis of DES

### 2.1 Key Space

The Data Encryption Standard(DES) employs a 56-bit secret key for encryption and decryption. This key length results in total key space of  $2^{56}$  possible keys

### 2.2 Brute Force Attack

A straight forward brute force attack on DES will require checking of all  $d^{56}$  keys to find the correct one

## 2.3 Completion Property

DES exhibits a property known as the complementation property: For message M, key K, and resulting cipher text C:

$$DES(M, K) = C$$

$$DES(\overline{M}, \overline{K}) = \overline{C}$$

Where  $\overline{M}$ ,  $\overline{K}$ ,  $\overline{C}$  represents bitwise complements of M, K, and C respectively

## 2.4 Chosen Plaintext Attack Utilizing completion property

### Attack Scenario

1. Attacker selects two plain texts:  $M_1$  and  $M_2$
2. Attacker receives corresponding cipher Texts:  $C_1$  and  $C_2$

### Attack procedure

For each possible key  $K_i$  in key space:

- compute  $DES(M, K_i) = C^*$
- if  $C^* = C_1$  then  $K_i$  is the actual secret key
- if  $C^* = C_2$  then  $K_i$  is the complement of the actual secret key
- If neither,  $K_i$  is not the correct key or its complement

### Effeciency:

- Each test eliminates two keys  $K_i$  and its complement
- Reduces the effective search space to  $2^{55}$  keys

### Advanced Attacks

Various cryptanalytic techniques, such as Differential Attacks and Linearization Attacks, have further reduced DES's security. It has been observed that DES can be broken with approximately  $2^{43}$  complexity

### Potential Solution

To enhance security, one proposed is to increase the length of the secret key. This can be achieved by performing the encryption multiple times using different keys

### 3 Double Encryption DES

The message is encrypted using the DES algorithm twice.

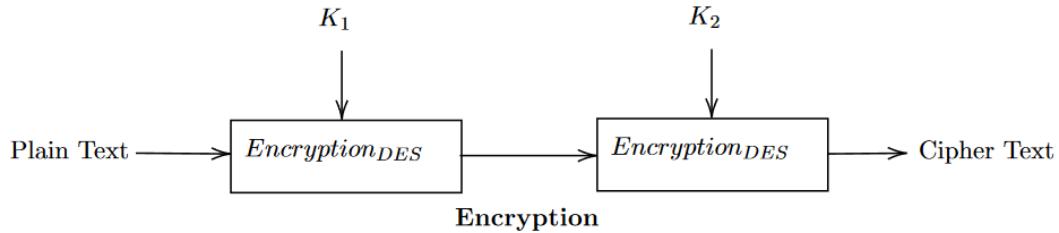
#### 3.1 Key space

The length of secret key is 112 bits concatenation of two 56 bit keys.

$$K = K_1 || K_2$$

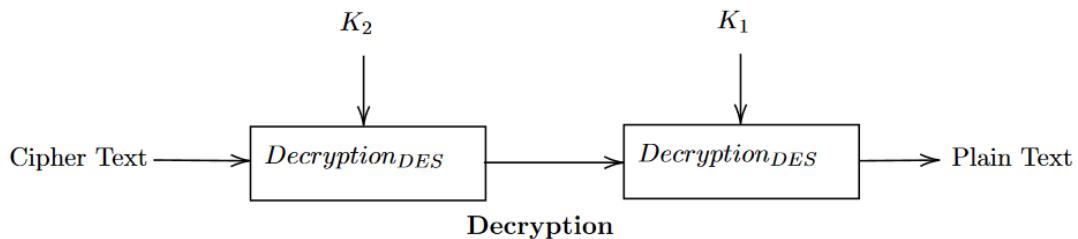
#### 3.2 Encryption process

1. Encrypt the plain text with key  $K_1$
2. Encrypt the result using the key  $K_2$



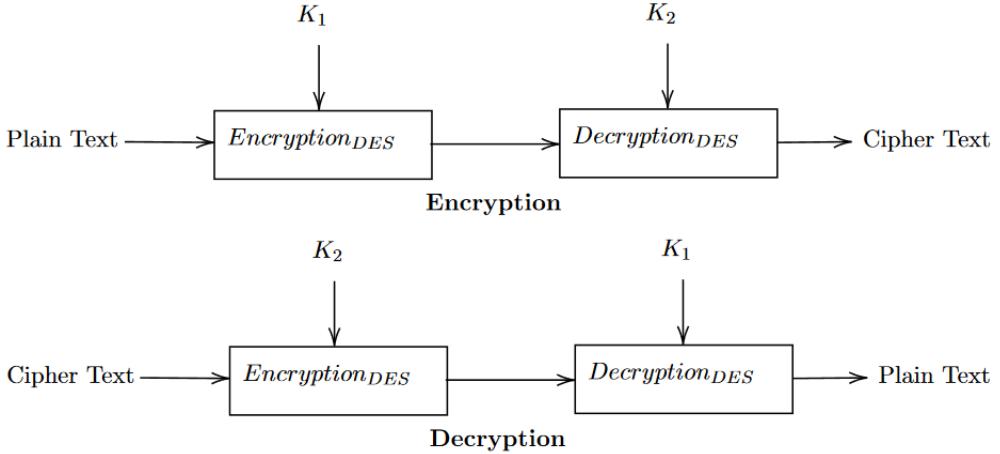
#### 3.3 Decryption process

1. Decrypt the cipher text with key  $K_2$
2. Decrypt the result text with key  $K_1$



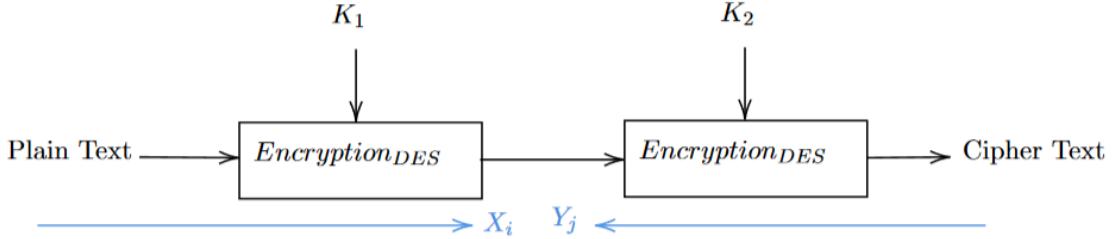
**note:** Order of use of key matters in this so be careful while encrypting and decrypting the text using this.

*Similarly we can use one Encryption then Decryption algorithm for encryption and vice versa for decryption*



### 3.4 Potential breakage of Double DES

As we know that the length of the key in double DES is 112 bits. Consider the following encryption technique. The key is concatenation of two 56 bit long keys i.e.  $K = K_1||K_2$ , and lets consider the



attack to be KPA(Known Plain Text Attack) i.e. Attacker knows the plain text  $M$  corresponding to cipher Text  $C$ .

$$C = Enc(Enc(M, K_1), K_2)$$

$$keys = \{sk_1, sk_2, \dots, sk_{2^{56}}\}$$

since the attacker has both, the cipher text as well as corresponding plain text. The attacker can perform the following:

$$Enc(M, sk_i) = X_i$$

$$Dec(C, sk_j) = Y_j$$

The blue arrows in the above diagram represent the above steps. The attacker has performed encryption of the plain text in the forward direction using key  $sk_i$ , while decryption of cipher text using key  $sk_i \neq sk_j$ . Now,

$$if X_i = Y_j \implies K_1 = sk_i \text{ and } K_2 = sk_j$$

two tables can be created, one that maps  $sk_i$  with corresponding  $X_i$ , and other that maps  $sk_j$  with corresponding  $Y_j$ . Now, we can do a lookup in these table, and where we find that  $X_i = Y_j$ , we get the secret key as:

$$K = sk_i || sk_j$$

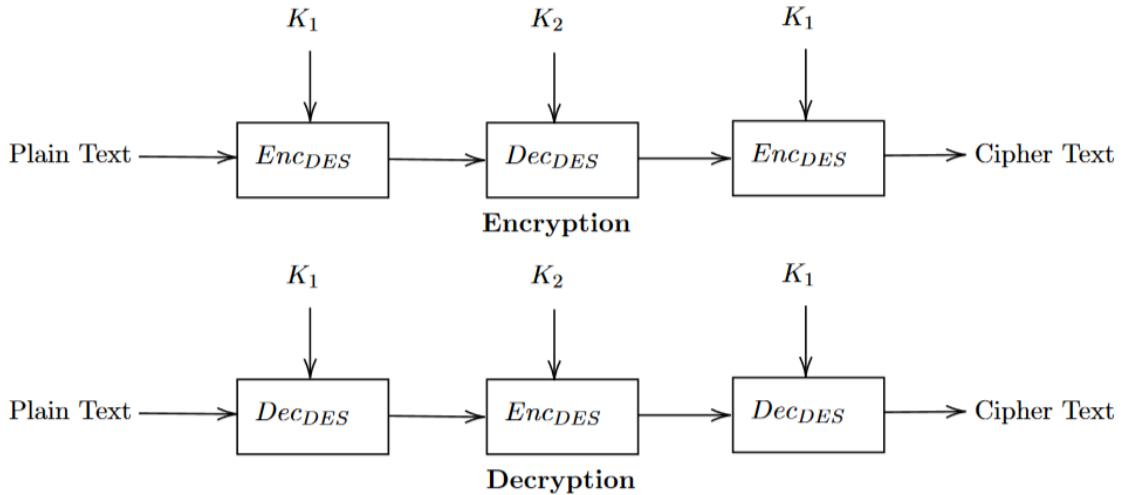
Hence, Double DES will not provide any extra security over DES as the complexity will be more or less same (neglecting several smaller complexities). This is true, in general, for all the encryption algorithms.

## 4 Triple Encryption of DES

### 4.1 Key space

similar to double DES here also two keys of 56 bits are used with concatenating first one with the second one making the final key to be 112 bits long key

$$K = K_1 || K_2$$



## 4.2 Encryption process

1. Encrypt with K1
2. Decrypt with K2
3. Encrypt with K1 again

## 4.3 Decryption process

1. Decrypt with K1
2. Encrypt with K2
3. Decrypt with K1 again

# 5 Advanced Encryption Technique(AES)

The DES encryption standard was compromised shortly after its public release. In response, the National Institute of Standards and Technology (NIST) launched a competition to find a more secure replacement. Cryptographers from around the globe submitted their designs, and the Rijndael algorithm, created by Joan Daemen and Vincent Rijmen from Belgium, emerged as the winner. It was subsequently adopted as the Advanced Encryption Standard (AES) and has remained unbroken to this day.

Before studying the AES we need to study maths behind it so here is the maths needed

## 5.1 Maths required for AES

### Groups

A binary operation  $*$  on a set  $S$  maps pairs of elements from  $S$  to another element in  $S$ . A group is a set  $G$  with a binary operation  $*$  that satisfies the following properties:

- **Associativity:**  $(a * b) * c = a * (b * c)$  for all  $a, b, c \in G$
- **Identity Element:** There exists an element  $e \in G$  such that  $a * e = a = e * a$  for all  $a \in G$
- **Inverse Element:** For every  $a \in G$ , there exists  $a^{-1} \in G$  such that  $a * a^{-1} = e$

### Abelian Groups

If a group  $G$  satisfies the commutative property, i.e.,  $a * b = b * a$  for all  $a, b \in G$ , it is called an Abelian group.

### Finite Groups

A group  $(G, *)$  is called finite if it contains a finite number of elements. For example, consider the set  $Z_n = \{0, 1, 2, \dots, n - 1\}$  with the operation  $+_n$ , defined as  $x +_n y = (x + y) \bmod n$ . This set forms a finite Abelian group.

## Lagrange's Theorem

Lagrange's Theorem states that if  $G$  is a finite group and  $H$  is a subgroup of  $G$ , then  $|H|$  divides  $|G|$ . In other words, the order of any subgroup of a finite group divides the order of the group.

- Let  $a \in G$ .
- The order of  $a$  is denoted as  $O(a)$ .
- Let  $S = \{e, a, a^2, \dots, a^{O(a)-1}\}$ , where  $e$  is the identity element.
- The set  $S$  is a subgroup of  $(G, *)$ , and  $\langle a \rangle$  denotes the cyclic group generated by  $a$ .

$$O(a) \mid |G|$$

## Order of Powers of an Element

If the order of  $a \in G$  is  $t$ , then the order of  $a^k$  will be  $\frac{t}{\gcd(t,k)}$ .

- $\langle a \rangle = \{e, a, a^2, \dots, a^{O(a)-1}\} = \langle a \rangle$
- $\langle a^k \rangle = \{e, a^k, a^{2k}, \dots, a^{(t/\gcd(t,k))-1}\}$
- Let  $b = a^k$ , then  $b$  generates a cyclic subgroup of  $G$ .

$$O(a^k) = \frac{O(a)}{\gcd(O(a), k)}$$

## Generation of Subgroups

If  $O(a^k) \mid O(a)$ , then  $a^k$  is also a generator of  $\langle a \rangle$ .

$$\begin{aligned} \langle a \rangle &= \{e, a, a^2, \dots, a^{O(a)-1}\} \\ \langle a^k \rangle &= \{e, a^k, a^{2k}, \dots, a^{(t/\gcd(O(a), k))-1}\} \end{aligned}$$

Thus, we conclude that:

$$O(a) \geq O(a^k)$$

## Ring

A ring  $(R, +_R, \times_R)$  consists of a set  $R$  with two binary operations arbitrarily denoted by  $+_R$  (addition) and  $\times_R$  (multiplication) on  $R$ , satisfying the following properties:

### Properties

1.  $(R, +_R)$  is an abelian group with identity element  $0_R$ .
2. The operation  $\times_R$  is associative, i.e., for all  $a, b, c \in R$ :

$$a \times_R (b \times_R c) = (a \times_R b) \times_R c$$

3. There exists a multiplicative identity, denoted by  $1_R \neq 0_R$ , such that for all  $a \in R$ :

$$1_R \times_R a = a \times_R 1_R = a$$

4. The operation  $\times_R$  is distributive over  $+_R$ , i.e., for all  $a, b, c \in R$ :

$$(b +_R c) \times_R a = (b \times_R a) +_R (c \times_R a)$$

and

$$a \times_R (b +_R c) = (a \times_R b) +_R (a \times_R c)$$

Thus, the set of all integers under multiplication and addition forms a ring.  $(R, +_R, \times_R)$

- $a \times_R b = b \times_R a, \forall a, b \in R$  then it is a commutative Ring
- $(Z, +, \cdot) \rightarrow$  commutative Ring
- $a \cdot b = b \cdot a$

An elt 'a' of a ring R is called unit or an invertible elt if there's an elt  $b \in R$  s.t.  $a \times_R b = 1_R$

The set of units in a Ring R forms a group under multiplicative operation. This is known as group of units of R.

## 5.2 Field

A field is a nonempty set F together with two binary operations  $+$  and  $\times$  for which the following properties are satisfied:

1.  $(F, +)$  is an abelian group.
2. If  $0_F$  denotes additive identity elt of  $(F, +)$  then  $(F \setminus \{0_F\}, \times)$  is a commutative/abelian group.
3.  $\forall a, b, c \in F$  we have  $a \times (b + c) = (a \times b) + (a \times c)$

E.g., set of rational nos. is a field.

### 5.2.1 Examples of Fields

- $(Z, +, \cdot) \rightarrow \text{Field } \times$
- $(Q, +, \cdot) \rightarrow \text{Field } \checkmark$
- 0: additive identity
- 1: multiplicative identity
- $(Q \setminus \{0\}, \cdot) \rightarrow \text{commutative group}$

### 5.2.2 Finite Fields

$F_p = \{0, 1, 2, \dots, p-1\}$ , where  $p$  is a prime number.

- $(F_p, +_p, \times_p)$  is a Field  $\checkmark$
- $+_p : (x+y)(\text{mod } p) \rightarrow \text{comm. grp.}$
- $\times_p : (x \cdot y)(\text{mod } p) \rightarrow \text{comm. grp.}$

### 5.2.3 Field Extension

Suppose  $k_1$  is a field with addition  $+$  and multiplication  $\times$ . Suppose  $k_2 \subset k_1$  is closed under both these operations s.t.  $k_2$  itself is a field for the restrictions of  $+$  and  $\times$  to the set  $k_2$ . Then  $k_2$  is called a subfield of  $k_1$  and  $k_1$  is called a field extension of  $k_2$ .

### 5.2.4 Polynomial Ring over a Field

Let  $F$  be a field  $(F, +, \times)$

$$F[x] = \{a_0 + a_1x + a_2x^2 + \dots \mid a_i \in F\}$$

polynomial ring

$$F[x] = \{a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1} \mid a_i \in F\}$$

Operations on polynomials:

- $(F, +, \times)$
- $(F[x], +, \times)$

Addition of polynomials:

$$\begin{aligned} & a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1} \\ & + b_0 + b_1x + b_2x^2 + \dots + b_{n-1}x^{n-1} \\ & = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_{n-1} + b_{n-1})x^{n-1} \end{aligned}$$

where  $a_i + b_i$  is the additive operation in the field  $F$

Multiplication of polynomials:

$$\begin{aligned} & (a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}) \\ & \times (b_0 + b_1x + \cdots + b_{n-1}x^{n-1}) \\ & = (a_0 \times b_0) + (a_0 \times b_1 + a_1 \times b_0)x + \cdots \\ & \quad + (a_{n-1} \times b_{n-1})x^{2n-2} \end{aligned}$$

where  $a_i \times b_j$  is the multiplicative operation in the field  $F$

Note:  $(F, \times)$ ,  $(F, +)$