[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Chitranshi Srivastava (202051055)

Winter 2022-2023
Lecture 7 (Week #4)

In the previous week, we discussed about Data Encryption Standard(DES) - its encryption, decryption and its complementarity property.

1 Attack Models

1.1 Cipher Text only Attack

Here, the attacker only knows the cipher text generated by an algorithm. The algorithm is known to everyone. The goal is to recover the corresponding plain text or find the secret key. If any of this is recovered, then the cipher is said to be broken. But if some part of plain text is recovered due to randomness, then the cipher is not said to be broken.

1.2 Known Plain text Attack

Here, the attacker knows some part of the plain text corresponding to the cipher text. Let's suppose that the attacker knows plain text $p_1, p_2, ...p_n$ corresponding to the cipher text $c_1, c_2, ..., c_n$. The goal here is to generate new plain text-cipher text pair, for example, new plain text p from new cipher text c, such that $c \notin \{c_1, c_2, ..., c_n\}$ or to recover the secret key.

The attacker has the advantage of knowing some plain text corresponding to cipher text. The Known Plain Text Attack is therefore stronger than Cipher Text Only Attack. If an encryption algorithm is secure to Known Plain Text Attack, then it will surely be secure for Cipher Text only Attack, but the reverse is not true.

1.3 Chosen Plain text Attack

Here, the attacker chooses the plain text according to his/her choice and he/she will be provided with the corresponding cipher text using the encryption algorithm. From this, the attacker tries to find the plain text for some different cipher text or tries to recover the secret key.

This attack model is much stronger than the Known Plain Text Attack as the attacker has the freedom to select the plain text arbitrarily. Hence, any encryption algorithm that is secure under this model, is also secure under the other two attack models.

1.4 Chosen Cipher text Attack

In this attack model, the attacker chooses some cipher text and is allowed to get the corresponding plain text. The goal of the attack is to get some new cipher text-plain text pair or recovering the secret key.

These attacks are much stronger in the Public-Key cryptography domains, as the key used to decrypt will be receiver's secret key. Hence, the attacker, if successful, will get the receiver's secret key.

2 Cryptanalysis of DES

DES provides 56 bit security. The parity bits are generated using these 56 bits, so they are not taken into consideration here.This means that a Brute Force Attack or Exhaustive Search on DES will look for 2^{56} keys to get the secret key.
This search space can be reduced to 2^{55} keys using the complementation property of DES. The complementation property states:

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

Let's now consider the Chosen Plain Text Attack Model. The attacker chooses two plain texts M and $\overline{M}$ and asks for cipher text corresponding to these plain texts. Lets say:

$$DES(M, K) = C_1$$
$$DES(\overline{M}, K) = C_2$$

Attacker is getting C_1 and C_2 and his/her goal is to get the secret key K. We know about the complementation property of DES. So we perform the operation:

$$DES(\overline{\overline{M}}, \overline{K}) = \overline{C_2}$$
$$\implies DES(M, \overline{K}) = \overline{C_2}$$

Now, the attacker has the following information:

$$DES(M, K) = C_1$$
$$DES(M, \overline{K}) = \overline{C_2}$$

where, C_1, C_2 and hence $\overline{C_2}$ are known to attacker.
The set of all possible keys using 56 bits, is as follows:

$$keys = \{K_1, K_2, ..., K_{2^{56}}\}$$

Attacker chooses a key, say $K_i \in keys$. Now, the attacker performs the following:

$$DES(M, K_i) = \tilde{C}$$

Now, from the information that we have, we can have the following interpretations:

$$\text{if } \tilde{C} = C_1 \implies K_i = K (\text{the actual secret key})$$
$$\text{if } \tilde{C} = \overline{C_2} \implies K_i = \overline{K} (\text{complement of actual key})$$
$$\text{if } \tilde{C} \neq C_1 \implies K_i \neq K$$
$$\text{if } \tilde{C} \neq \overline{C_2} \implies K_i \neq \overline{K} \implies \overline{K_i} \neq K$$

Hence, for each key K_i, either the actual key K will be found, or we will be able to eliminate two keys, K_i and $\overline{K_i}$.
Hence, our search space has become half and we need to search for 2^{55} keys to get the actual key.

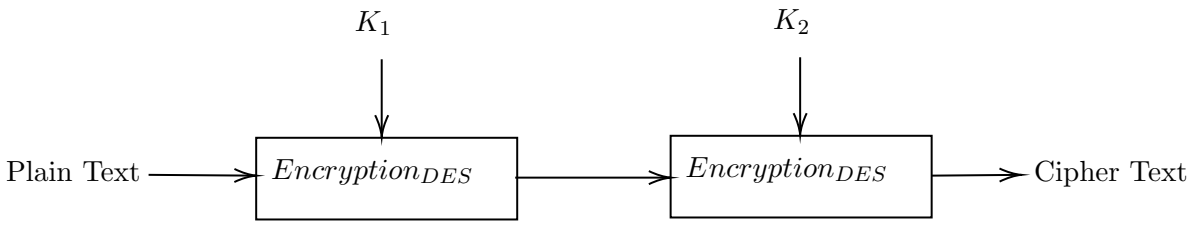
DES is vulnerable to different attacks such as Differential Attacks and Linearization Attacks. It has been observed that DES can be broken in approximately 2^{43} complexity.
One possible solution is to increase the length of the secret key;increase the length of the secret key to n times and perform the encryption n times.

3 Double Encryption of DES

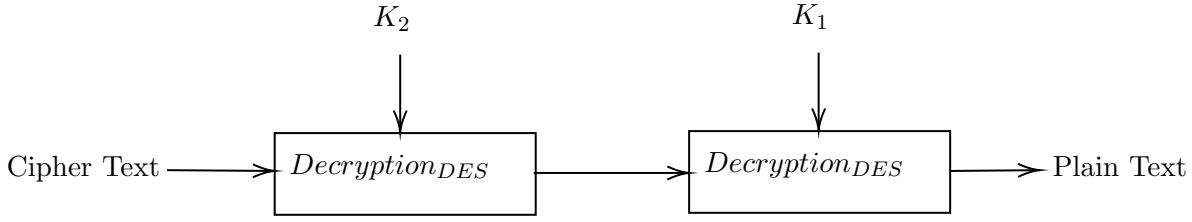
The message is encrypted twice using the DES algorithm. The encryption and decryption function remains same. The length of the secret key is 112 bits and is as follows:

$$K = K_1||K_2$$

One way to do double encryption is :



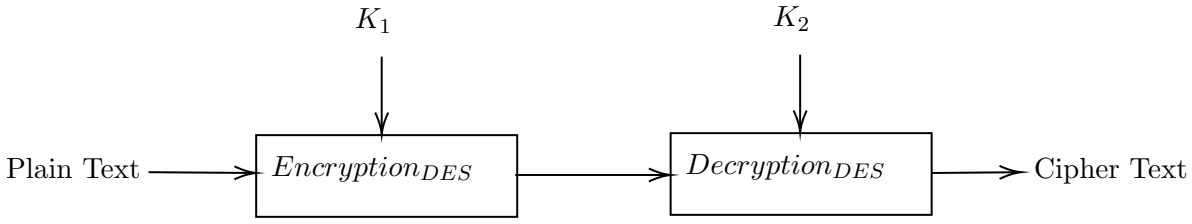
Encryption



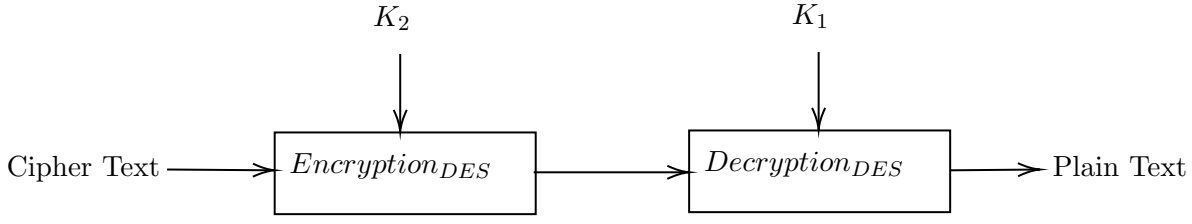
Decryption

Encryption:
We first encrypt using key K_1 and then with key K_2.
Decryption:
We first encrypt using key K_2 and then with key K_1.

We can use different permutations of Encryption and Decryption functions of the basic DES implementation like above. Another example is:



Encryption

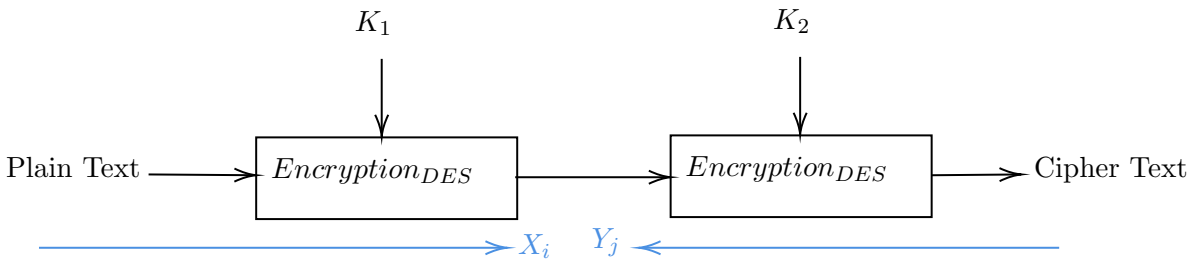


Decryption

Similarly, we can make two other types of double DES:

- Decryption-Encryption
- Decryption-Decryption

The length of key for Double Encryption DES is 112-bits and hence it is expected to provide better security. However, this is not the case. Let us prove it by considering the following situation:



The key K will be concatenation of two 56-bit keys, i.e. $K = K_1||K_2$. Let us consider the Known Plain Text Attack, i.e. the attacker knows the plaintext M corresponding to cipher text C. Therefore,

$$C = Enc(Enc(M, K_1), K_2)$$
$$keys = \{sk_1, sk_2, ..., sk_{2^{56}}\}$$

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 $sk_j \neq sk_i$. Now,

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

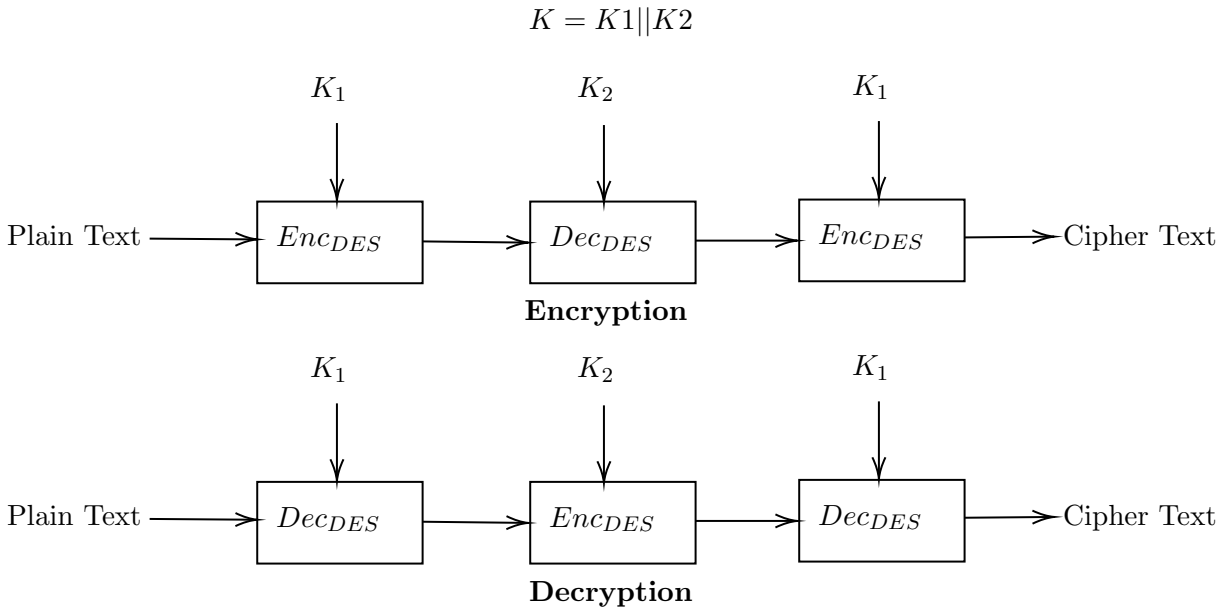
Two tables can be created, one that maps sk_i with corresponding X_i, and other that maps sk_j with corresponding Y_j. Now, we can do a lookup in these table, and where we find that $X_i = Y_j$, we get the secret key as:

$$K = sk_i||sk_j$$

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

The standard mechanism to provide double security using DES is to use triple layer of encryption. The length of key in this remains 112-bit and it is a concatenation of two 56-bit keys. Let K be the key, then,



different combinations such as EEE, EED, EDE etc. can be used. Consequently, the decryption will also have a different combination, where the E and D will be swapped, hence, DDD, DDE, DED etc.

Note:

- the key used in the middle function should be different than the key used in first and last function
- the key in first and last function must be same

5 Advanced Encryption Standard

DES design was initially kept secret but when it was made public, it was immediately broken. Thereafter, A lot of cryptographers around the world submitted their designs along with the implementation. One of the submission in the competition was *Rijndael*. In the proposal, it was mentioned that the winner will be renamed as Advanced Encryption Standard. AES is unbreakable till date.

Before learning about the AES algorithm deeply, it is required to learn about certain mathematical structures.

5.1 Mathematics Recall

A binary operation $*$ on a set S is a mapping from $S \times S$ to S. It means $*$ is a rule which assigns to each ordered pair of elements from S to an element of S.

$$* : S \times S \to S$$
$$\text{if } *(a,b) = c \text{ and } a, b \in S \implies c \in S$$
$$*(b,a) = d \implies d \in S$$

The ordering in the pair is important, hence, it is not necessary that $c = d$.

5.1.1 Group

A Group $(G, *)$ consists of a set G and a binary operation $*$ on G satisfying the following axioms:

1. $*$ is associative on G, that is, $a * (b * c) = (a * b) * c \ \forall \ a, b, c \in G$
2. There is an element $e \in G$ called the Identity Element, such that $a * e = a = e * a \ \forall \ a \in G$.
3. For each $a \in G$, there exists an element $a^{-1} \in G$, called the inverse of a, such that $a * a^{-1} = e = a^{-1} * a \ \forall \ a \in G$.

5.1.2 Abelian Group

A group G is called an Abelian (or commutative) Group if $a * b = b * a \ \forall \ a, b \in G$.

5.2 Examples

5.2.1 Example 1:

Let,
$*$: matrix multiplication over square matrices of order n and
M: set of $n \times n$ matrices over $\mathbb{R}$.
Is $(M, *)$ a group?
Solution: We know that matrix multiplication is associative and hence $*$ is associative on M. Also, there always exist Identity Matrix I_n, such that $A * I_n = A = I_n * A$. However,

$$\forall \ (A \in M) \nexists (A^{-1} \in M) \text{ such that } A * A^{-1} = I_n = A^{-1} * A$$

The inverse of matrix doesn't exist if its determinant is equal to zero. Hence, $(M, *)$ is not a group.

5.2.2 Example 2:

Consider M in the previous problem to be the set of all invertible square matrices and $*$ be the same. Clearly, $(M, *)$ will now be a group as non-invertible matrices do not belong to M. Is $(M, *)$ an Abelian Group?
Solution: For a group to be an Abelian Group, it must be commutative over the set of elements. However, in general, matrix multiplication is not commutative, that is $A * B \neq B * A$. Hence, $(M, *)$ is not an Abelian Group.

5.2.3 Example 3:

$\mathbb{Z}$: set of all integers and $+$ is addition operation. Is it a group?
Solution: We know that addition is associative, i.e,

$$a + (b + c) = (a + b) + c$$

Also, $0 \in \mathbb{Z}$ is identity element such that:

$$a + 0 = a = 0 + a \ \forall \ a \in \mathbb{Z}$$

And, for each $a \in \mathbb{Z} \ \exists (-a)$ such that $a + (-a) = 0 = (-a) + a$. Hence, $(\mathbb{Z}, +)$ is a group.

Note: $(\mathbb{Z}, -)$ is not a group as subtraction is not associative.

5.2.4 Example 4:

Consider the multiplication operation $\times$ on the set of integers $\mathbb{Z}$. Is it a group?
Solution: The multiplication operation is:

$$\text{associative: } a \times (b \times c) = (a \times b) \times c$$
$$\text{existence of identity element: } a \times 1 = a = 1 \times a$$

However, inverse of a, that is, $a \times a^{-1} = 1 = a^{-1} \times a$ does not exist for multiplication operation on $\mathbb{Z}$. This is because, for multiplication operation $a^{-1} = \frac{1}{a} \notin \mathbb{Z}$.
Hence, $(\mathbb{Z}, \times)$ is not a group.

5.2.5 Example 5:

set of all rational numbers and $\times$ is multiplication operation. Is $(\mathbb{Q}, \times)$ a group?
Solution: No, it is not a group. It satisfies all the other properties of a group but for $0 \in \mathbb{Q}$ inverse does not exist. Hence, $(\mathbb{Q}, \times)$ is not a group. However, if we consider the set $\mathbb{Q} - \{0\}$, then $(\mathbb{Q} - \{0\}, \times)$ is a group.

Finite Group :
If the number of elements in a set is finite, and $(G, *)$ is a group, then $(G, *)$ is a finite group.

5.2.6 Example 6:

Consider the set $\mathbb{Z}_n$ which contains integers from 0 to $n-1$ (both inclusive) and the operation $+_n$ which means $x +_n y = (x + y) mod$ n. Is $(\mathbb{Z}_n, +_n)$ a group?
Solution: Let's check for each property one by one:

- Associativity

$$\begin{aligned} (x +_n y) +_n z &= (((x + y) mod n) + z) mod\ n \\ \implies (x +_n y) +_n z &= (x + y + z) mod\ n \\ \implies (x +_n y) +_n z &= (x + (y + z) mod\ n) mod\ n \\ \implies (x +_n y) +_n z &= x +_n (y +_n z) \end{aligned}$$

  Hence, $(\mathbb{Z}_n, +_n)$ is associative.

- Existence of Identity Element in $\mathbb{Z}_n$. Clearly, 0 is the identity element as :

$$x +_n 0 = x = 0 +_n x.$$

- Existence of inverse. Clearly, for $x \in \mathbb{Z}_n$, $n - x$ will be the inverse of x.

$$x +_n (n - x) = (x + n - x) mod\ n = n\ mod\ n = 0$$

Hence, $(\mathbb{Z}_n, +_n)$ is a group. Moreover, it is an Abelian group.

5.2.7 Example 7:

Consider the set $(\mathbb{Z}_n - \{0\})$ and the operation $*_n$, i.e, $x *_n y = (x * y) mod\ n$. Is $((\mathbb{Z}_n - \{0\}), *_n)$ a group?
Solution: It is easy to verify that the given operation is associative on the given set, and also it has an identity element equal to 1. Now, let us see for inverse. We know that for $x \in (\mathbb{Z}_n - \{0\})$, inverse x^{-1} will be defined as:

$$x *_n x^{-1} = 1 \implies x * x^{-1} \equiv 1\ mod\ n$$

The x^{-1} here is known as multiplicative inverse of x under modulo n. We know that it exists only iff $gcd(x, n) = 1$. Hence, there may exist some x, for which $gcd(x, n) \neq 1$ and hence, x^{-1} does not exist. Hence, $((\mathbb{Z}_n - \{0\}), *_n)$ is not a group.

Consider the set which has only those integers from 0 to n-1, which are co-prime to n. This set is usually denoted by $\mathbb{Z}_n^*$. The cardinality of this set can be calculated using the Euler's Totient Function $\phi(n)$.

$$\mathbb{Z}_n^*: \{x \in \mathbb{Z}_n \text{ and } gcd(x, n) = 1\}$$

Hence, $(\mathbb{Z}_n^*, *_n)$ is a group.