Scribe: Cryptography and Network Security (Lecture 22)

Kuheli Pratihar

09-Oct-2020

1 Concepts Covered

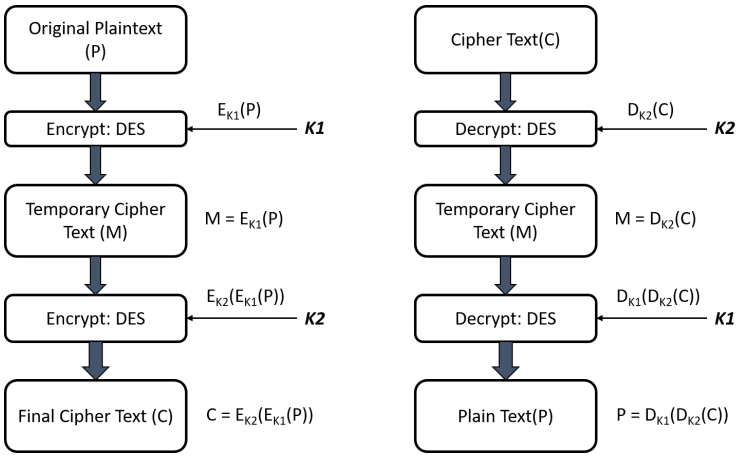
1. Analysis of The Data Encryption Standard (DES)
   (a) Multiple DES
      i. 2-DES
         A. Meet-in-the-middle attack
         B. Security of 2-DES
      ii. Triple DES
2. Generalization of Fiestel Cipher
3. Homework Questions and Solutions

2 Analysis of the The Data Encryption Standard (DES)

The Data Encryption Standard (DES) uses 56-bit key to encrypt any plain-text which can be easily cracked due to the tremendous advances in computer hardware in cryptography[2][4]. To prevent this from happening, the concept of multiple DES was introduced which is much more secured than the original DES because it has a larger key space, thereby offering more security than DES.

2.1 Multiple DES

There are two different types of multiple DES: (a) 2-DES (b) Triple DES. The two variations are covered as follows:



(a) Double DES (Encryption) (b) Double DES (Decryption)

Figure 1: Double DES

2.1.1 2-DES

2-DES (also known as *Double DES*) is an encryption technique that uses two instances of DES on the same plaintext. Both the instances use different keys (say K_1 and K_2) to encrypt the plaintext.

As shown in Figure 1a, the original plain text of size 64 bits goes into first DES instance which then gets converted into a temporary cipher text (also known as *middle text*) using the first key K_1 and then it goes to second DES instance which gives the final bit cipher text by using the second key K_2. However, the 2-DES uses a key-size of 112 bits, but provides the security level of a 2^{56} and is vulnerable to a known plaintext attack.

2.1.1.1 Meet-in-the-middle attack

The [1]**meet-in-the-middle attack**is based on the observation that, if we have

$$C = E_{K_2}(E_{K_1}(P))$$

then from Figure 1a and 1b

$$M = E_{K_1}(P) = D_{K_2}(C)$$

Given a known pair of (Plaintext, Ciphertext), say (P, C), the attack proceeds as follows:

1. The attacker encrypts P for all 2^{56} possible values of K_1. Then stores these results in a table and performs lexicographic sorting of the table by the values of M.

[1]For detailed explanation refer to Homework Section (3)

2. The attacker then decrypts C using all 2^{56} possible values of K_2.

3. After each decryption, the attacker checks the result against the table for a match. If a match occurs, then tests the two resulting keys against a new known plaintext–ciphertext pair. If the two keys produce the correct ciphertext, he accepts them as the correct keys.

2.1.1.2 Security of 2-DES

As discussed above, Double DES has a 112-bit key and enciphers blocks of 64 bits. Given that DES is not a group therefore double encryption is not equivalent to single encryption. Although security does increase by double encryption, but it does not increase much thereby making 2-DES vulnerable to the meet-in-the-middle attack.

2.1.2 Triple DES

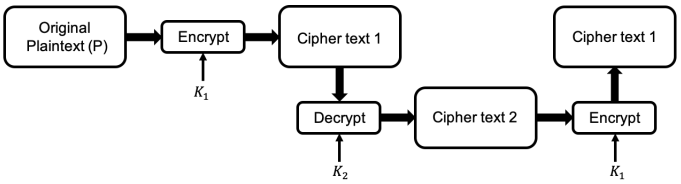


Figure 2: Triple DES with two keys [1]

Triple DES was proposed to increase the security of 2-DES (Figure 2). The first and the third stage use K_1 as a key. The middle or the second stage uses decryption with K_2 as a key. This is a modification over the simple DES to be robust to attacks. Setting $K_1 = K_2$ in this case we would get a simple DES and a backward compatible design.

3 Generalization of the Fiestel Cipher

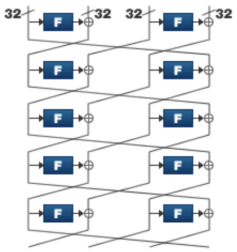


Figure 3: 4-Branch Fiestel Structure used in CLEFIA [3]

Fiestel Ciphers are used in present day blockciphers such as CLEFIA which is a 128-bit blockcipher designed by SONY corporation (Figure 3). It uses 4-branch generalized Fiestel structure which is an extension of the 2-branch Fiestel structure. Due to the 4-branch structure size of the F-function is smaller hence efficient implementation in hardware and software.

4 Homework Questions and Solutions

DES (Data Encryption Standard) although an elegantly designed cipher has become old. Its $n = 56$ bit key is being challenged by the present day computation power. As an alternative, it was thought of applying DES twice, i.e in creating a product cipher $DES' = DES \times DES$. If the key space of DES was $K = \{0,1\}^n$, the key size of the product cipher is expected to be $K_1 \times K_2 = (K_1, K_2)$, where $K_1, K_2 \in K$. The plaintext of the cipher is denoted by $P = \{0,1\}^m$ and the cipher is endomorphic (the plaintext and the ciphetext are the same set). In regard to this composed cipher answer the following questions:

1. **What is the property in the DES construction which helps to increase the key length by performing such composition? (Another way of asking the question is: why is DES not idempotent)**

   Solution:
   The property in the DES construction which helps to increase the key length by performing such composition is that DES is not a group i.e. $E_{K_2}(E_{K_1}(P))$ is not equivalent to DES encryption using a single key.

2. **Using the DES cipher an attacker obtains l pairs of plaintexts and ciphertexts: $(p_1, c_1), \cdots, (p_l, c_l)$. The key is say $(K_1.K_2)$ but unknown to the attacker (obviously, else why will he/she be an attacker).**
   Prove that for all $1 \leq i \leq l, DES_{K_1}(p_i) = DES^{-1}_{K_2}(c_i) \forall i$, where $1 \leq i \leq l$.

   Solution:
   For $1 \leq i \leq l$, we have that $c_i = DES_{K_2}(DES_{K_1}(p_i))$. Let us denote $z_i = DES_{K_1}(p_i)$. Now, c_i can be written as $c_i = DES_{K_2}(z_i)$, so $DES_{K_1}(p_i) = z_i = DES^{-1}_{K_2}(c_i)$, as required.

3. **Prove that of all the possible keys (K_1, K_2), the expected number of keys for which $DES_{K_1}(p_i) = DES^{-1}_{K_2}(c_i) \forall i$, where $1 \leq i \leq l$, is about 2^{2n-lm}.**

   Solution:
   Given that we have a key size of n bits, for $DES \times DES$, the brute force attack complexity will be of the order of 2^{2n} i.e. $2^n \cdot 2^n$.

   Now consider two tables T_1 and T_2. Each row of T_1 has l elements of the plaintext P i.e. $DES_{K_1{}^1}(p_1) \cdots DES_{K_1{}^{2^n}}(p_i)$ followed by an element

from K_1. Similarly, each row of T_2 has l elements of the ciphertext C followed by an element from K_2.

Therefore, the probability of the i^{th} entry of T_1 being exactly equal to the j^{th} entry of T_2 can be given by 2^{-ml}, where m =number of bits in the plaintext and ciphertext and l =number of pairs used.

Now, once a match is found, then $({K_1}^i, {K_2}^j)$ is the possible key out of a total of 2^{2n} keys.

Therefore,

$$E(DES_{K_1}(p_i) = DES^{-1}_{K_2}(c_i) \forall i) = 2^{2n} \times 2^{-ml} = 2^{2n-lm}$$

4. **Suppose $l \geq 2n/m$, what can you say to the attacker to help him in developing an attack against the composed cipher DES' ?**

   Solution:
   If $l \geq 2n/m$, then $2n - lm \leq 0$. Therefore (K_1, K_2) can be uniquely determined, thereby helping the attacker to develop the attack.

5. **The attacker starts building up two lists: L_1 and L_2. Each entry in the list L_1 and L_2 had l tuples of elements of P followed by an element of K. The lists are filled with all possible keys.**
   The lists are now sorted in a lexicographic manner on the l tuples. The attacker now does a linear search to find out the common l tuples in the lists.
   Explain how does the attacker maintain the list and how does this approach help him to find out the correct key? Show that the amount of memory required by the attacker is $2^{n+1}(ml + n)$ buts and the number of encryptions and/or decryptions required to identify the key is $l2^{n+1}$.
   (Hint: Use the distinguisher: for the correct key $DES_{K_1}(p_i) = DES^{-1}_{K_2}(c_i) \forall i$)

   Solution:
   The attacker maintains the list L_1 by inserting all possible values of $DES_{K_1}(p_i) \forall i$. The number of rows in the table is equal to a number of possible secret keys i.e. ${K_1}^1 \cdots {K_1}^{2^n}$.

   Similarly, the attacker maintains the list L_2 by inserting all possible values of $DES^{-1}_{K_2}(c_i) \forall i$. The number of rows in the table is equal to a number of possible secret keys i.e. ${K_2}^1 \cdots {K_2}^{2^n}$.

   This approach helps the attacker to search for a pair of secret keys (K_1, K_2) such that $DES_{K_1}(p_i) = DES^{-1}_{K_2}(c_i) \forall i$.

   The amount of memory required by the attacker equals the total size of list L_1 and L_2. However, the size of both the lists are same. Each list has a tuple size of $(ml + n)$. There are 2^n such entries, as explained above which equals to $2 \times (2^n \cdot (ml + n)) = 2^{n+1}(ml + n)$.

The number of encryptions/decryptions required to identify the key:

(a) Number of encryptions done in $L_1 = l \times 2^n$

(b) Number of decryptions done in $L_2 = l \times 2^n$

Therefore, $l \cdot 2^{n+1}$ operations are required in total to successfully identify the key.

6. **Into what class does the above kind of attack fall ?**

   Solution:
   The above attack falls under the class of *known-plaintext attack*.

5 Conclusion

In this lecture, we successfully analysed DES and also proposed multiple DES schemes like the 2-DES and the Triple DES. We took a closer look into the meet-in-the-middle attack on 2-DES. Finally, a solution has been provided to the exercise questions given in the class.

References

[1] Sayali Bagwe. *Multiple DES*. https://www.ques10.com/p/3461/short-note-on-multiple-des-1/, 2016.

[2] Behrouz A Forouzan. *Cryptography & network security, Chapter 5*. McGraw-Hill, Inc., 2007.

[3] SONY. *Structure of CLEFIA*. https://www.sony.net/Products/cryptography/clefia/about/structure.html/.

[4] Douglas Robert Stinson and Maura Paterson. *Cryptography: theory and practice*. CRC press, 2018.