Cryptography and Network Security

Suprajit Sardar

9th October 2020

1 Multiple DES

- One of the major criticism against DES is the short key-length.
- So to overcome this criticism we may try cascading several DES applications.

2 2 DES

- Uses two applications of the DES cipher.
- The total key size is 56*2 =112 bits.
- However 2 DES is vulanarable to known plain text.

3 Meet in the middle attack

- Attacker performs a known plain text attack.He collects (P,C) pairs.
- Using 1st relation he encrypts P using2$^(56)$ keys , and records all values of M.
- Using 2nd relation he decrypts C using all possible 2$^(56)$ keys and records all values of M.

4 How to reduce the complexity

- Let keys for DES1 is K1, for DES2 is K2 ,Cipher text is of 64bits(m bits) and several cipher text , plain text pairs [(P1,C1),(P2,C2).....,(Pl,Cl)].
- Here, —k1—=—k2—=2^n
- If we try brute-force we will have $2^n * 2^n = 2^(2n)$ keys combinations.
- our goal is to reduce it complexity to $2^(n + 1)$.

- DES K1(Pi) = DES$^(-1)$K2(Ci) , 1¡= i ¡= l (for all i)
- Now, creates 2 tables for Plain text side and Cipher text side

Plain text side for K1 [L1]
DESK1(P1).....DESK1(Pl) DESK2(P1).....DESK2(Pl) ith row DESK2^n(P1).....DESK2^n(Pl)

Cipher text side for K2 [L2]
DESK1(P1).....DESK1(Pl) DESK2(P1).....DESK2(Pl) jth row DESK2^n(P1).....DESK2^n(Pl)

- So, the size of the each row is m * l
- Now, the probability that ith row completely match with jth row is $2^(-ml)$
- To ensure that wrong keys don't appear we can use- Expected no. of keys(K1[i],K2[j]) is - $2^(2n)$ * $2^(-ml) = 2^(2n - ml)$
- If $l <= 2n/m$ => 2n -ml <= 0
- It indicates that there is a very high probability to uniquely find out K1 and K2.
- Now, number of encryption is done in L1 is $l*2^n$ and number of decryption is done in L2 is also $l * 2^n$
- So, in total 2 * $l * 2^n = 2^(n + 1)$ as l is no. of observation (constant)

5 Security of 2 DES

- The attacker checks for a match in the table in the value of m.He notes the key pair (K1,K2).
- If there are more than one keys, he takes another (P,C) pair.
- The attacker continues until there is only key left.

- Thus attack complexity is around 2(57)
- What does it say about the security of 2 DES ?
- From 56 to 57, it,s not a great progress.So people thought about 3 DES.

6 3 DES

- Since 2 DES was a bad design, people consider 3 applications of DES.
- The first and third stages uses K1 as key.
- The second stage uses K2 as the key.
- Also the middle stage uses decryption.
- Thus setting K1 = K2 we have simple DES.

7 Generalization of the Feistel Cipher

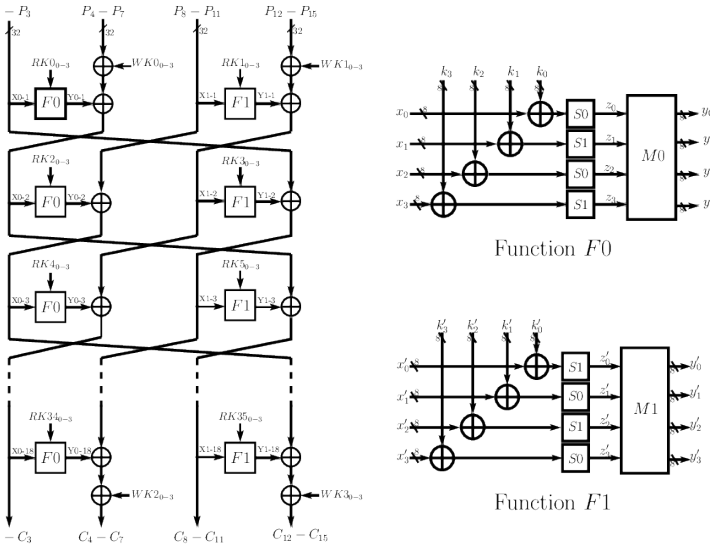

Figure 1: CLEFIA Fiestel Cipher

8 Exercise

- Q1.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?)

- Ans- 1.Weak keys : the key that is selected on the rounds are a problem . During splitting of keys to two half and swapping them might throw up the same result if they have continuous 1's and 0's. Thins ends up in using the same key through out the 16-cycles

  2.There can be same output from the S-Boxes on different inputs on permutation. These are called Semi weak keys.

  If the message is encrypted with a particular key, and is taken 1's compliment of that encryption will be same as that of the encryption of the compliment message and compliment key.

- Q2.Using the DES cipher an attacker obtains l pairs of plaintexts and ciphertexts: (p1, c1), . . . ,(pl, cl). The key is say (K1, K2) but unknown to the attacker (obviously, else why will he/she be an attacker). Prove that for all 1 <= i <= l, DESK1(pi) = DES1K2(ci) for all i, where 1< = i <= l.

  ANS-

- Q3.Prove that of all the possible keys (K1, K2), the expected number of keys for which DESK1(pi) = DES1K2(ci) for all i, where 1 <= i <= l, is about $2^(2m - ml)$.

  Ans-

- Let keys for DES1 is K1, for DES2 is K2 ,Cipher text is of 64bits(m bits) and several cipher text , plain text pairs [(P1,C1),(P2,C2).....,(Pl,Cl)].

- Here, —k1—=—k2—=2^n

- If we try brute-force we will have $2^n * 2^n = 2^(2n)$ keys combinations.

- our goal is to reduce it complexity to $2^(n + 1)$.

- DES K1(Pi) = DES$^(- 1)$K2(Ci) , 1¡= i ¡= l (for all i)

- Now, creates 2 tables for Plain text side and Cipher text side

Plain text side for K1 [L1]
DESK1(P1).....DESK1(Pl) DESK2(P1).....DESK2(Pl) ith row DESK2^n(P1).....DESK2^n(Pl)

- So, the size of the each row is m * l

- Now, the probability that ith row completely match with jth row is $2^(-ml)$

Cipher text side for K2 [L2]
DESK1(P1).....DESK1(Pl) DESK2(P1).....DESK2(Pl) jth row DESK2^n(P1).....DESK2^n(Pl)

- To ensure that wrong keys don't appear we can use- Expected no. of keys(K1[i],K2[j]) is - $2^(2n) * 2^(- ml) = 2^(2n - ml)$
- Q4.Suppose l >= 2n/m, what can you say to the attacker to help him in developing an attack against the composed cipher DES'?

  Ans-
- If $l <= 2n/m$ that implies 2n -ml <= 0
- It indicates that there is a very high probability to uniquely find out K1 and K2.
- So, the attacker will easily find the key .
- Q5. The attacker starts building up two lists: L1 and L2. Each entry in the list L1 and L2 has l tuples of elements of P followed by an element from 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) bits and number of encryptions and/or decryptionsrequired to identify the key is $l * 2^(n + 1)$. (Hint: Use the distinguisher: for the correct key DESK1(pi) = DES1K2(ci) for all i)

  Ans-
- The complexity of good sorting technique is O(nlogn).we can ignore logn as n is very very large number.
-
- Let keys for DES1 is K1, for DES2 is K2 ,Cipher text is of 64bits(m bits) and several cipher text , plain text pairs [(P1,C1),(P2,C2).....,(Pl,Cl)].
- Here, —k1—=—k2—=2^n
- If we try brute-force we will have $2^n * 2^n = 2^(2n)$ keys combinations.
- our goal is to reduce it complexity to $2^(n + 1)$.

- DES K1(Pi) = DES$^{(}$ − 1)K2(Ci) , 1¡= i ¡= l (for all i)
- Now, create 1 table for Plain text side and Cipher text side as both as of same size.

Plain text side for K1 [L1]
DESK1(P1).....DESK1(Pl) DESK2(P1).....DESK2(Pl) ith row DESK2^n(P1).....DESK2^n(Pl)

- So, the size of the each row is m * l
- So, the size of the each table is (ml + n) * 2^l .
- Now, number of encryption is done in Plain text is $l * 2^n$ and number of decryption is done in Cipher text is also $l * 2^n$.
- So, in total 2 * $l * 2^n = l * 2^{(}n + 1)$.
- Q6.Into what class does the above kind of attack fall?

  Ans-
- The above kind of attack fall into known plain text attack.