Cryptography and Network Security

AKASH KUMAR GANGWAR(20CS60R31)

15-oct-2020

1 Introduction

In this scribe we will learn about cryptanalysis of modern day cipher that is block cipher and will also know about product cipher. In DES and AES there is many round encryption needed, to find that number of round we have to do a cryptanalysis on block cipher.Linear cryptanalysis is a known plaintext attack in which the attacker studies probabilistic linear relations (called linear approximations) between parity bits of the plaintext, the ciphertext, and the secret key.

2 Product Cipher

Product ciphers are modern day cipher.By combining two or more simple transposition ciphers or substitution ciphers, a more secure encryption may result i.e. Product cipher. As these cipher is obtained from simple cipher , these are also known as **iterated cipher**.

For designing a new block cipher , there is two mandatory things that is needed -

1. Round description : This describes that how many internal rounds are used for encyption and every rounds may contain sub-operation like subbytes, shift rows or mix column etc.
2. Key schedule : It is a algorithm which gives you a intermediate round keys starting from the original input keys.

3 Cipher Transformation

Round function takes two input round key and current state. assume that round function is "g" and round key for round r is "K^r"and current state W^{r-1} so next state W^r will be :(figure 1)

We iterate this process multiple times to obtain block cipher and we will get cipher W^{Nr} where Nr is the number of rounds of cipher.

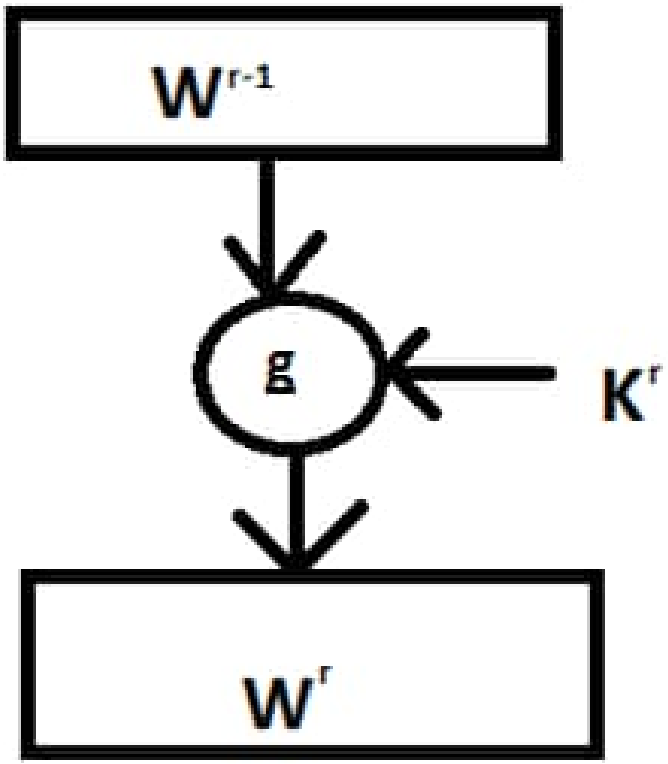

Figure 1:

4 SPN cipher

SPN, or substitution–permutation network (SPN), is a series of linked mathematical operations used in block cipher algorithms.

In such cipher suppose there are m blocks each of length l, then total block length will be lm.On each block we perform S-box substitution.

S : {0,1} ^{l} $-->$ $\{0,1\}^{l}$

After S-box we apply P-box permutation except last round on whole block length i.e. lm.

P : {0,1} ^{lm} $-->$ $\{0,1\}^{lm}$

4.1 Algorithm

{point no 1 to 7 is for last rounds and 8 to 10 for last round}

Algorithm 1: ALGORITHM

Input : x: $\{0,1\}^{lm}, K_0 : \{0,1\}^{lm}$

Output: Output, y : $\{0,1\}^{lm}$

Key Schedule : generates $(K_0, K_1, K_2....K_N r)$

$W^0 = x$

for $r = 1$ *to* $Nr - 1$ **do**

  $u^r = w^{r-1} \wedge K^{r-1}$

  for $i = 1$ *to* m **do**

    $V_i^r = S(u_i^r)$

  $W^r = V_{P(1)}^r, V_{P(2)}^r.....V_{P(lm)}^r,$

$u^{Nr} = V^{Nr} \wedge K^{Nr}$

for $i = 1$ *to* m **do**

  $V_i^{Nr} = S(u_i^{Nr})$

$y = v^{Nr} \wedge K^{Nr}$

4.2 Example : GPig Cipher

This is a Block cipher in which l=m=Nr=4 that means it contains 4 block each of size 4 bits and number of rounds of encryption is also 4. S-box works on each of 4 bits.

In figure 2 GPig Cipher is shown there are 4 round and in initial 3 rounds S-box substitution and p-box permuation is used respectively but in last round only P-box permuation is used. S-box is used on 4-bits of each block and P-box is used on all blocks simultaneously.

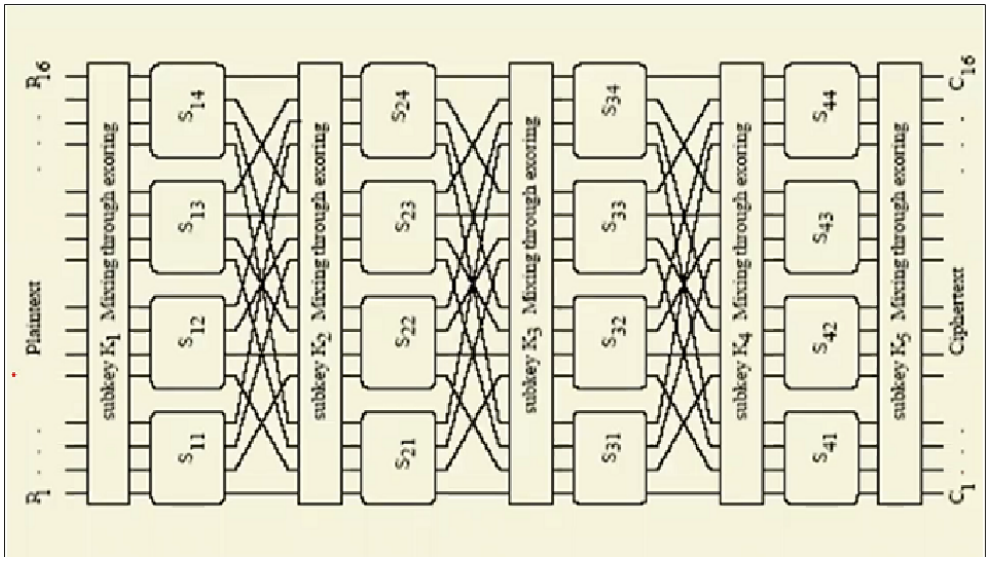

Figure 2: The Cipher Diagram

4.3 Key Scheduling

In GPig we use a simple key schedule in which key K for round r i.e. K^r is made by taking successive 16 bits from Key starting at position Kr+1.

For ex. Key is 1100 0011 1010 0101 1100 0011 1010 1111 then K^0 will take initial 16 bits and K^1 will take key from 5^th bits to 20^th bit and so on.

5 Linear Cryptanalysis (Lc)

Linear Cryptanalysis is a attack that target to obtain linear approximation between plain text and each states of cipher text in block cipher prior to last round. LC is a known plain text attack model because in this attack , the attacker has a large number of plain text and cipher text pairs which he used to guess last round keys and verify it by decrypting the cipher text to obtain the previous state before last round.

For the purposes of linear cryptanalysis, a linear equation expresses the equality of two expressions which consist of binary variables combined with the exclusive-or (XOR) operation. For example, the following equation, from a hypothetical cipher, states the XOR sum of the first and third plaintext bits (as in a block cipher's block) and the first ciphertext bit is equal to the second bit of the key:

P1 $\oplus P3 \oplus C1 = K2$

The probability of approximation should be bounded away from 1/2 as this is known as "good" approximation. The attack will not work if all cipher will be random whose approximation have a probability 1/2.

5.1 Pilling Up Lemma

In cryptanalysis, the piling-up lemma is a principle used in linear cryptanalysis to construct linear approximation to the action of block ciphers. The piling-up lemma allows the cryptanalyst to determine the probability that the equality:
$X_1 \oplus X_2 \oplus X_3 \oplus ..... \oplus X_n = 0$
holds. where the X 's are binary variables (that is, bits: either 0 or 1).

Let P(A) denote "the probability that A is true". If it equals one, A is certain to happen, and if it equals zero, A cannot happen.

we consider the piling-up lemma for two independent binary variables, where $P(X_1 = 0) = p_1$ and $P(X_2 = 0) = p_2$.
Then, $P(X_1 = 1) = 1 - p_1$ and $P(X_2 = 1) = 1 - p_2$

As X_1 and X_2 are independent then $P(X_1 \wedge X_2 = 0) = p_1p_2 + (1 - p_1)(1 - p_2)$

Now convert these probability in terms of Bias. Bias shows how much these probability deviate from 1/2.
Let $\epsilon_1 = p_1 - 1/2$ and $\epsilon_2 = p_2 - 1/2$, thus
$P(X_1 \wedge X_2 = 0) = 1/2 + 2\epsilon_1\epsilon_2$
This was for two variable but we can convert it in generalized lemma for n variables too. Let $X_1, X_2, X_3, ...X_n$ are n independent random binary variable with Bias $\epsilon_1, \epsilon_2, \epsilon_3....\epsilon_n$ then,
$P(X_1 \wedge X_2 \wedge X_3..... \wedge X_n = 0) = 1/2 + 2^{n-1}(\epsilon_1\epsilon_2\epsilon_3.....\epsilon_n)$

Note: Pilling Up Lemma only works when random variables are independent.

6 Conclusion

In Linear Cryptanalysis, we calculate Bias that is how much probability of any expression deviate from 1/2 . If bias tends to zero then that will not be a good approach from the point of view of attacker if Bias is tends to 1 then it will be a good linear approximation for attacker.