CS641
Modern Cryptology
Indian Institute of Technology, Kanpur

Mid Semester Examination

Group Name: CRYPTOSAR
Ayush Kumar Mishra (20211401), Rajat Kumar (20211403), Shubham Kumar Mishra (20211404)

Date of Submission:
March 10, 2021

Question 1

Consider a variant of DES algorithm in which the S-box S1 is changed as follows:

> For every six bit input α, the following property holds: $\text{S1}(\alpha) = \text{S1}(\alpha \oplus 001100) \oplus 1111$.

All other S-boxes and operations remain the same. Design an algorithm to break four rounds of this variant. In order to get any credit, your algorithm must make use of the changed behavior of S1.

Solution

For every six bit input α ,

$$\text{S1}(\alpha) = \text{S1}(\alpha \oplus 001100) \oplus 1111$$

so if we take $\text{S1}(\alpha \oplus 001100)$ on the left side then

$$\text{S1}(\alpha) \oplus \text{S1}(\alpha \oplus 001100) = 1111$$

Now we can conclude that when input xor is 001100 then output xor is 1111
and the probability of xored output is 1111 is 1.
Now we have to break four rounds of this variant DES using the property mentioned above.

step 1:
let us take two 64 bit input
each input have 2 halves and both have same right halves
so that xor of right halves is $R_0 = 0000\ \ 0000$
and xor of the left halves produces $l_0 = 6000\ \ 0000$
step 2:
Now pass xored input in feistal round 1
we get $L_1 = R_0$
and $R_1 = L_0 \oplus R_0$

$$R_1 = 6000\ \ 0000$$

step 3:
now in this round we have been given modified S-box which
will produce output as $F0000\ \ 0000$ with probability as 1. now we pass the output of S-box as input to P-box which give output as 0082 8200 output of the xor operation between P-box output and L_1 i.e.,

$$0082\ \ 8200 \oplus 0000\ \ 0000 = 0082\ \ 8200$$

now $R_2 = 0082\ \ 8200$ with probability 1 and $l_2 = 6000\ \ 0000$ step 4:
As we got the value for R_2&L_2
And we know the value of R_4&L_4 as DES encryption output,
so we know the value of R_3 as

$$R3 = L_4$$

$$L_3 = R_2$$

step 5:
Since we know that xor operator is invertible,now we do xor operation between R_4&L_3
Now we get the output of round 4 round P-box. So, we also get the input of P-box which will be the output of S-box with probability as 1 and from there,we get input of that S-Box.
Since we know R_3 we get the output of round 4 E-box,which we do xor with the input of round 4 S-box to get the value of k_4
So by using this approach, we get to know the value of k_4 and also was able to break this 4 round DES encryption.[Agr21]

Question 2

The SUBSET-SUM problem is defined as follows:

> Given $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ and $m \in \mathbb{Z}$, find $(b_1, \ldots, b_n) \in \{0,1\}^n$ such that $\sum_{i=1}^{n} a_i b_i = m$ if it exists.

This problem is believed to be a hard-to-solve problem in general. Consider a hypothetical scenario where Anubha and Braj have access to a fast method of solving SUBSET-SUM problem. They use the following method to exchange a secret key of AES:

> Anubha generates an $n = 128$ bit secret key k. She then chooses n positive integers $a_1, \ldots, a_n$ such that $a_i > \sum_{1 \leq j < i} a_j$. She computes $m = \sum_{i=1}^{n} a_i k_i$ and sends $(a_1, a_2, \ldots, a_n, m)$ to Braj, where k_i is ith bit of k. Upon receiving numbers $(a_1, a_2, \ldots, a_n, m)$, Braj solves the SUBSET-SUM problem to extract the key k.

Show that an attacker Ela does not need to solve SUBSET-SUM problem to retrieve the key k from $(a_1, a_2, \ldots, a_n, m)$.

Solution

In this problem we have to get Key from $(a_1, a_2, \ldots, a_n, m)$ and we don't have to use subset sum problem.
We will be making use of condition that is given in the problem,That sequence $(a_1, a_2, \ldots, a_n)$ is super increasing sequence.
In mathematics, a sequence of positive real numbers $(s_1, s_2, ...)$ is called super increasing if every element of the sequence is greater than the sum of all previous elements in the sequence [wik].

Formally, this condition can be written as

$S_i > \sum_{1 \leq j < i} S_j$

Given super increasing sequence $A = (a_1, a_2, \ldots, a_n)$ $K = (k_1, k_2, \ldots, k_n)$ and $m = (A, K)$, we can find Key(K) using Below Approach

$k_n = 1$ if and only if $m > \sum_{1 \leq j <= n-1} A_j$ and $m >= a_n$

since we have found K_n we can recursively solve this instance of problem to get our Key where $A = (a_1, a_2, \ldots, a_{n-1})$ and if $k_n = 1$ then $m = m - a_n$ else m takes it previous value only.

By iterating above step , we will get rightmost bit of K at every step and hence we will get K

Time Complexity for this problem is O(n).

[Pei13].

Question 3

Having falied to arrive at a secret key as above, Anubha and Braj try another method. Let G be the group of $n \times n$ invertible matrices over field F, $n = 128$. Let $a, b, g \in G$ such that $ab \neq ba$. The group G and the elements a, b, g are publicly known. Anubha and Braj wish to create a shared secret key as follows:

> Anubha chooses integers ℓ, m randomly with $1 < \ell, m \leq 2^n$, and sends $u = a^\ell g b^m$ to Braj. Braj chooses integers r, s randomly with $1 < r, s \leq 2^n$, and sends $v = a^r g b^s$ to Anubha. Anubha computes $k_a = a^\ell v b^m = a^{\ell+r} g b^{m+s}$. Braj computes $k_b = a^r u b^s = a^{\ell+r} g b^{m+s}$. The secret key is thus $k = k_a = k_b$.

Show that even this attempt fails as Ela can find k using u and v.

Hint: Show that Ela can

1. find elements x and y such that $xa = ax$, $yb = by$, and $u = xgy$,
2. use x, y, and v to compute k.

Solution

anubha sends:

$$u = a^l g b^m - - - (i)$$

and braj sends:

$$v = a^r g b^s - - - (ii)$$

let us take

$$x = a^l$$

then multiply both side by a^r on right side

$$a^r x = a^r a^l$$

$$a^r x = a^{r+l} - - - (iii)$$

similarly take

$$y = b^m$$

then multiply both side by b^s on left side

$$b^s y = b^s b^m$$

$$b^s y = b^{m+s} - - - (iv)$$

given that

$$a^l v b^m = a^{l+r} g b^{m+s}$$

by equation (iii) and (iv)

$$a^l u b^m = x a^r g b^s y$$

$$a^l u b^m = x(a^r g b^s) y - - - (v)$$

by equation (i)

$$a^l v b^m = xvy - - - (vi)$$

by equation (vi) we can conclude the our initial assumption is correct
so, lets take same assumption now we can say it is valid now

$$a^l = x$$

multiply by a left side

$$aa^l = ax$$

$$a^{l+1} = ax$$

$$b^m = y$$

multiply by b left side

$$bb^m = by$$

$$b^{m+1} = by$$

similarly we have to find in another order

$$a^l = x$$

multiply by a right side

$$a^l a = xa$$

$$a^{l+1} = xa$$

$$b^m = y$$

multiply by b right side

$$b^m b = yb$$

$$b^{m+1} = yb$$

as shown above we can conclude that $xa = ax$, $by = yb$ *and* $u = xgy$

now take equation(i) and equation(vi)

$$v = a^r g b^s$$

$$a^l u b^m = xvy$$

$$a^l u b^m = x(a^r g b^s)y$$

we know that $x = a^l$ and $y = b^m$

$$a^l u b^m = a^l (a^r g b^s) b^m$$

$$a^l u b^m = a^{r+l} g b^{m+s} y - - - (vii)$$

so now we prove the key by equation(vii)

$$k_a = a^{l+r} g b^{m+s}$$

$$k_a = (a^l a^r) g (b^s b^m)$$

$$k_a = a^l (a^r g b^s) b^m$$

$$k_a = x(a^r g b^s)y$$

$$k_a = xvy - - - (ix)$$

so now we prove the key by equation(viii)

$$k_b = a^{l+r} g b^{m+s}$$

$$k_b = (a^l a^r) g (b^s b^m)$$

$$k_b = a^l (a^r g b^s) b^m$$

$$k_b = x(a^r g b^s)y$$

$$k_b = xvy - - - (x)$$

from equation (ix) and (x) we can say that

$$k = k_a = k_b$$

References

[Agr21] Dr. Manindra Agrawal. Modern Cryptology, Lecture 6 pdf. https://hello.iitk.ac.in/sites/default/files/cs641a2021/Lecture_6.pdf, 2021.

[Pei13] Chris Peikert. Cryptanalysis of Knapsack Cryptography, Lattices in Cryptography at Georgia Tech. https://web.eecs.umich.edu/~cpeikert/lic13/lec05.pdf, 2013.

[wik] wikipedia. Superincreasing sequence. https://en.m.wikipedia.org/wiki/Superincreasing_sequence.