CS641

Modern Cryptology
Indian Institute of Technology, Kanpur

Group Number: CodeNymro
Sumit lal (20111278), Sharvari Ajay Oka (20111055), SonamTshering (20111064)

Mid Semester Examination

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: $\mathrm{S1}(\alpha) = \mathrm{S1}(\alpha \oplus 001100) \oplus 1111$.

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

In order to break r round DES algorithm, we need r-2 round characteristic [Agr21b]. Hence in order to break 4 round DES we use the probability of 2 round characteristic:

$$(6000\overline{0}, \overline{00}, 1, \overline{00}, 6000\overline{0}, \frac{14}{64}, 6000\overline{0}, 00828000) \quad \mathit{equals} \quad \frac{14}{64}. \tag{1.1}$$

This characteristic says that if we use two inputs such that their input XOR to second round S1 is 001100, we get E000(in hexadecimal) as the output with probability $\frac{14}{64}$. Following is the algorithm which is used to break the given variant of algorithm:

We choose two input plain-texts such that their input XOR to second round S1 is 001100, with output of rest s-boxes (S2-S8) as zero and the XOR of output of S1 is 1110 [Agr21a].

If we understand the variant of S1 given in the question, it basically interchanges the two inputs given to the S1 box e.g if we consider the case where we do not use the variant and the inputs to S1 box is A and B and their XOR (A $\oplus$ B), after applying the variant, basically the inputs get interchanged and hence their XOR remains same. Even after applying XOR with 1111 to get the output of S1 box, it does not make any difference as it only flips the bits of both the input and in turn keeps the XOR result same.

Therefore we can conclude that even if we apply the variant over the S1 box, we can obtain the 2- round characteristic as shown in equation 1.1.
Hence we can say that with the given variant of DES, we can successfully break 4 round DES.

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

Anubha sends $(a_1, a_2, \ldots, a_n, m)$ to Braj where $a_i > \sum_{1 \leq j < i} a_j$ and $m = \sum_{i=1}^{n} a_i k_i$ where $k_i \in \{0, 1\}$.
As the channel is considered to be attack prone, Ela also knows the super-increasing sequence $a_1, a_2, \ldots, a_n$ and m (sum of subset of $a_i k_i$). Hence this problem boils down to a greedy algorithm which helps to solve the subset sum problem in polynomial time, if the sequence is super-increasing [RO12]. The algorithm works as follows [Sub19]:

Let k be the output array which is the secret key.
Iterate variable i from n to 1. (Here n=128)
If $a_i \leq m$, include it in the output by setting the corresponding i^{th} bit in the output array. and update the value of m=m-a_i and decrement value of i.
Else, decrement the value of i.

After completion of the iteration, if m=0, we get an output consisting of 0's and 1's where 0 or 1 at i^{th} position represent that the corresponding bit k_i of the secret key. Otherwise we consider that an appropriate key does not exist.

In this way without applying subset sum problem, Ela can find secret key k in polynomial time.

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

Ela does not have access to any private exponents such as l, m, r, s but as u, v are accessible to Ela [Shp08, BCM11]. She can find $n \times n$ invertible matrices x and y as follows:
From the given hints, lets consider the equations:

$$xa = ax \tag{3.1}$$

$$yb = by \tag{3.2}$$

$$u = xgy \tag{3.3}$$

where x and y are invertible matrices of size $n \times n$ and a, b, g and u are known to everyone who can access the channel.
From the given equation we can say that equation 3.1 and 3.2 are linear system of equation however equation 3.3 is non-linear system of equation as it has product of two unknown matrices.
In order to convert the equation into system of linear equation, we can follow the steps:
We have considered that $xa = ax$, which can be proven to be equivalent to $x^{-1}a = ax^{-1}$

as follows:
Multiply equation 3.1 both side by x^{-1} we get,

$$\begin{aligned} x^{-1}xa &= x^{-1}ax \\ Ia &= x^{-1}ax \end{aligned} \tag{3.4}$$

where I is an identity matrix of size n × n

Multiply with x^{-1} to eliminate x on rhs.

$$\begin{aligned} ax^{-1} &= x^{-1}axx^{-1} \\ ax^{-1} &= x^{-1}aI \\ ax^{-1} &= x^{-1}a \end{aligned} \tag{3.5}$$

hence $xa = ax$ is equivalent to ax^{-1}=x^{-1}a. Let $x_1 = x^{-1}$.
Multiply equation 3.3 both side by x^{-1}

$$\begin{aligned} x^{-1}u &= x^{-1}xgy \\ x^{-1}u &= gy \end{aligned}$$

The equation 3.1, 3.2 and 3.3 will get converted to as follows:

$$x_1a = ax_1 \tag{3.6}$$

$$yb = by \tag{3.7}$$

$$x_1u = gy \tag{3.8}$$

multiply equation 3.8 with u^{-1} on both side,

$$\begin{aligned} x_1uu^{-1} &= gyu^{-1} \\ x_1 &= gyu^{-1} \end{aligned} \tag{3.9}$$

Substituting the value of x_1 in equation 3.6,

$$gyu^{-1}a = agyu^{-1} \tag{3.10}$$

From equation 3.10 and 3.7 we can see that there are $2n^2$ linear equations with n^2 variables and only one unknown variable y. Now with such system of equations y can be easily found as it is the invertible matrix.

Substituting this values of y in equation 3.8, to find x_1. Now $x_1 = x^{-1}$, hence we get x.

Ela knows v which is sent from Braj to Anubha, hence she can find;

$$xvy = xa^r gb^s y \tag{3.11}$$

since $xa = ax$ and $yb = by$

Therefore

$$xvy = xa^r gb^s y = a^r xgyb^s = a^r ub^s = k \tag{3.12}$$

Using this methodology Ela can find the secret key k.

References

[Agr21a] Manindra Agrawal. Lecture 6 (Slide14). CS641 Modern Cryptology, Feb 2021.

[Agr21b] Manindra Agrawal. Lecture 7 (Slide12). CS641 Modern Cryptology, Feb 2021.

[BCM11] Simon R Blackburn, Carlos Cid, and Ciaran Mullan. Group theory in cryptography. *Proceedings of Group St Andrews 2009 in Bath*, pages 133–149, 2011.

[RO12] Roohallah Rastaghi and Hamid R Dalili Oskouei. Cryptanalysis of a public-key cryptosystem using lattice basis reduction algorithm. *arXiv preprint arXiv:1210.7417*, 2012.

[Shp08] Vladimir Shpilrain. Cryptanalysis of Stickel's key exchange scheme. In *International Computer Science Symposium in Russia*, pages 283–288. Springer, 2008.

[Sub19] Find the Subsequence with given Sum in a Superincreasing Sequence. https://www.geeksforgeeks.org/find-the-subsequence-with-given-sum-in-a-superincreasing-sequence/, 03 Dec 2019.