CS641A Mid Sem

HIRAK MONDAL, YASH SARASWAT, MAYANK BANSAL

TOTAL POINTS

50 / 50

QUESTION 1

1 DES **15 / 15**

+ **15 pts** Correct using alternate solution

✓ + **2 pts** **Mention and explain about the difference of XOR being 1111**

✓ + **4 pts** **Mention and explain about changed probability/behaviour of S box**

✓ + **4 pts** **Formulation of plaintext attack and input to rounds of DES till second round**

✓ + **5 pts** **Brief analysis of algorithm for key extraction (can relate with lecture)**

- **4 pts** Changes in analysis not specified due to change in S1. If you have not mentioned that prbability 14/64 would change to 1 (for example in slide 2 and 3 of Lecture 7)

+ **0 pts** Wrong Answer / Missing Solution

QUESTION 2

2 SUBSET-SUM **15 / 15**

✓ + **7.5 pts** **Algorithm**

✓ + **7.5 pts** **Formal Proof of Correctness**

+ **0 pts** Incorrect

QUESTION 3

3 Invertible Matrices **20 / 20**

✓ + **7 pts** **Find the key using $$x,y \in G$$ satisfying the properties.**

✓ + **10 pts** **Reducing the system of equations to linear form.**

✓ + **3 pts** **Reason for the existence of a non-trivial solution of linear system.**

+ **0 pts** Incorrect or NA

CS641

Modern Cryptology
Indian Institute of Technology, Kanpur

Group Number: Stuxnet
Mayank Bansal (20111032), Hirak Mondal (20111022), Yash (20111073)

Mid Semester Examination

Date of Submission:
March 10, 2021

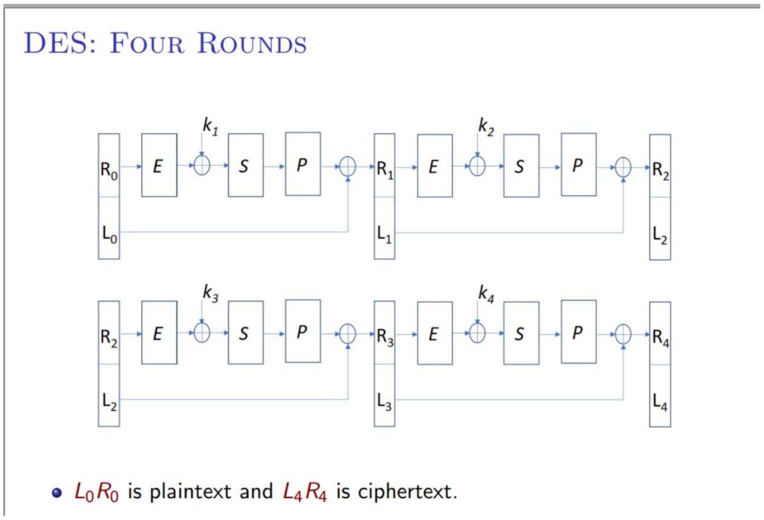
Question 1

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



DES: Four Rounds

- L_0R_0 is plaintext and L_4R_4 is ciphertext.

Figure 1: DES: Four rounds structure. src: [Agg]

We know that the problem to solve the four round DES is that we don't know either the exact value or the XORed value (of the input plaintext blocks) of the output of the S-box in the second round. This can be overcome as followed -

Let α_1 and α_2 corresponding to the two plaintext blocks, be two inputs to the S-box S1 of second round DES, such that

$$\alpha_1 \oplus \alpha_2 = 001100 \tag{1.1}$$

$$\alpha_2 = \alpha_1 \oplus 001100 \tag{1.2}$$

Using the property mentioned in the question, we get -

$$S1(\alpha_1) = S1(\alpha_2) \oplus 1111 \tag{1.3}$$

$$S1(\alpha_1) \oplus S1(\alpha_2) = 1111 \tag{1.4}$$

This means that if any two plaintexts are selected such that the inputs to S-box S1 of second round DES satisfy equation (1.1) then we will definitely get equation (1.4) as a result, thus ensuring an output of 1111 with probability 1 (with rest of the S-boxes in the second round DES producing 0000 as result when XOR is taken). .

Now that we know the XOR output of S-boxes of second round DES, we can calculate either the exact value or the XOR value of the lines in our third and fourth rounds of DES enabling us to break this version of DES as we studied in [Agg].

ALGORITHM

I: Select two plaintext blocks such that their corresponding inputs to the S-box S1 of round two satisfies equation (1.1).

II: Calculate the values of lines as explained in [Agg] till we reach the S-box of the second round.

III: Calculate the output of the second round S-boxes through equation (1.4) using the input values selected in step **I**.

IV: Continue to calculate the values of the lines of round three and round four as explained in [Agg].

The above algorithm will allow us to break the given version of four round DES.

1 DES 15 / 15

+ **15 pts** Correct using alternate solution

✓ + **2 pts** **Mention and explain about the difference of XOR being 1111**

✓ + **4 pts** **Mention and explain about changed probability/behaviour of S box**

✓ + **4 pts** **Formulation of plaintext attack and input to rounds of DES till second round**

✓ + **5 pts** **Brief analysis of algorithm for key extraction (can relate with lecture)**

- **4 pts** Changes in analysis not specified due to change in S1. If you have not mentioned that prbability 14/64 would change to 1 (for example in slide 2 and 3 of Lecture 7)

+ **0 pts** Wrong Answer / Missing Solution

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 $a_i > \sum_{1 \le j < i} a_j$. 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

As Anubha is sending $(a_1, a_2, \ldots, a_n, m)$ to Braj, the attacker Ela can easily intercept this information. This means that Ela has access to $(a_1, a_2, \ldots, a_n, m)$.

The key k is given as a n (n=128) bit string. Another value m is given as

$$m = \sum_{i}^{n} a_i k_i \tag{2.1}$$

The constraint: $a_i > \sum_{1 \le j < i} a_j$ means that every succeeding value in the sequence $(a_1, a_2, \ldots, a_n)$ will be greater than the sum of it's preceding values.

Ela does not need to solve the SUBSET-SUM problem to retrieve the key. She can do so simply by following the below mentioned algorithm -

ALGORITHM

```
I: for i from n to 1 do
II:     if $m \geq a_i$ then
III:        $k_i = 1$
```

```
        m = m - $a_i$
    else
        $k_i = 0$
```

The logic behind the above algorithm is that, if $m \geq a_i$, then, according to equation (2.1), a_i will contribute to the value of m and thus the corresponding bit in the key k needs to be 1. This is because the sum of the preceding values of a_i is less than a_i and if a_i is ignored then we cannot get the correct value of m.

Similarly, if $m < a_i$, then a_i needs to be ignored an the corresponding bit in the key will be 0.

Thus, through the above algorithm, each bit of the key k can be assigned either 0 or 1 and thus by running the algorithm once Ela can find the key.

The time complexity of the above algorithm is simply O(n) unlike the SUBSET-SUM problem which has time complexity of $O(2^n)$.

2 SUBSET-SUM 15 / 15

✓ + 7.5 pts Algorithm

✓ + 7.5 pts Formal Proof of Correctness

+ 0 pts Incorrect

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

We have referred to [Shp08] in order to come up with the solution of this question.

It is still possible for the attacker Ela to find the key k without getting access to the values ℓ,m,r,s.

Let us assume that sent value u (which Ela can easily get by intercepting the communication channel) can be decomposed in the following way -

$$u = xgy \tag{3.1}$$

where x and y are two unknown nxn invertible matrix belonging to the group G and also satisfy the below mentioned equations -

$$xa = ax \tag{3.2}$$

$$yb = by \tag{3.3}$$

If Ela is able to obtain at-least one solution to the equations (3.1), (3.2) and (3.3), then it is possible for her to get the key k. Let us see how is that possible.

Both the equations (3.2) and (3.3) upon matrix product and after equating L.H.S. and R.H.S. gives us a system of n^2 linear equations each in terms of the unknown elements of the matrices x and y.

The problem is with the equation (3.1). The equation consists of product of two unknown matrices on the R.H.S. (namely x and y) which disables us to translate the equation (3.1) into a system of linear equations. Thus it is required to transform the equation first into a suitable form.

To do that, we first premultiply both sides of equation (3.1) by x^{-1} to get -

$$x^{-1}u = gy \tag{3.4}$$

This is a valid operation as x is an invertible matrix.

Now, post-multiplying u^{-1} in equation (3.4) to get -

$$x^{-1} = gyu^{-1} \tag{3.5}$$

Now, since x is invertible, by properties of matrices we know that equation (3.2) is possible if and only if

$$x^{-1}a = ax^{-1} \tag{3.6}$$

also holds.

Finally, using equations (3.5) and (3.6), we get -

$$gyu^{-1}a = agyu^{-1} \tag{3.7}$$

So, equation (3.7) along with equation (3.2) gives us a system of linear equations with $2n^2$ equations and n^2 unknows corresponding to the unknown matrix y. This gives us a over-determined system of linear equations which implies that there exists at-least one non-trivial (non-zero) solution for y. By solving for y we can find x^{-1} and in turn x.

After doing the above, in addition to u and v, we also know x and y. Ela can use Braj's transmission v to get the key as follows -

$$xvy = xa^r gb^s \tag{3.8}$$

$$xa^r gb^s = a^r xgyb^s \tag{3.9}$$

(Used equation (3.2) here)

$$a^r xgyb^s = a^r ub^s = k_b = k_a = k \tag{3.10}$$

So in this way, even this attempts fail as Ela can get the key by using only u and v.

References

[Agg] Manindra Aggarwal. Cryptanalysis of DES.

[Shp08] Vladimir Shpilrain. Cryptanalysis of Stickel's Key Exchange Scheme. In Edward A. Hirsch, Alexander A. Razborov, Alexei Semenov, and Anatol Slissenko, editors, *Computer Science – Theory and Applications*, pages 283–288, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

3 Invertible Matrices 20 / 20

- ✓ + **7 pts** **Find the key using $$x,y \in G$$ satisfying the properties.**
- ✓ + **10 pts** **Reducing the system of equations to linear form.**
- ✓ + **3 pts** **Reason for the existence of a non-trivial solution of linear system.**
- + **0 pts** Incorrect or NA