Mid Sem

● Graded

Group

ABHAYA PRATAP SINGH
ANANYAE KUMAR BHARTARI
NAVEEN KUMAR MATHUR
View or edit group

Total Points

48 / 50 pts

Question 1

DES — Resolved **15** / 15 pts

+ 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

Regrade Request — **Submitted on: Mar 17**

Sir, we wrote that probability would change to 1 with explanation and thoughtful analysis to be the same as in the lectures, so we wrote in reference the lecture numbers and slide numbers.

But our marks for not writing probability change in S1 had been deducted, and about analysis, sir, told not to repeat anything similar that was taught in class (mark the reference for so).

Ok

Reviewed on: Mar 17

Question 2

SUBSET-SUM

Resolved **13** / 15 pts

✔ **+ 7.5 pts** Algorithm

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

+ 0 pts Incorrect

– 2 pts prove that your algorithm works correctly. Not that there exists only one key.

Regrade Request **Submitted on:** Mar 17

Sir, in the problem, the task was to retrieve the key using the specification in question only. If it were written explicitly in question also to prove correctness, we would have written so.
As the task was to find the key deducting (-2), marks would be harsh considering the mean is just 43.07.

the 2nd rubric asks for a proof of correctness.

Reviewed on: Mar 17

Question 3

Invertible Matrices

20 / 20 pts

✔ **+ 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

Question assigned to the following page: 1

CS641
Modern Cryptology
Indian Institute of Technology, Kanpur

Mid Semester Examination

Group Number:
Naveen Kumar Mathur (190535), Abhaya Pratap Singh (190019), Ananayae Kumar Bhartari (190129)

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

Let the two inputs be **a** and **b**
Given that,

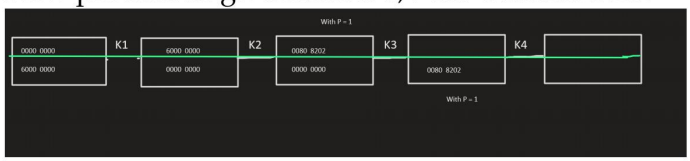
$$s1(\alpha) = s1(\alpha \oplus 001100\ ) \oplus 1111$$

If **XOR** of two inputs **a** and **b** is 001100
then, S1 is updated like this and all procedure same as lecture

$$\text{a} \oplus b = 001100$$
$$\text{b} = \text{a} \oplus 001100$$
$$\text{s1(a)} = \text{s1(b)} \oplus 1111$$
$$\text{s1(a)} \oplus s1(b) = 1111$$

Question assigned to the following page: 1

For every input pair with **XOR 001100**, the output **XOR** is **1111** with probability 1. Now proceed as given in lec. 6, 7 for 4-round DES.



Question assigned to the following page: 2

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

Claim : Only 1 key with such specifications exist

Proof: Let there exist **two distinct keys** or sequence b_is and b'_is.
such that, $\sum_{i=1}^{n} a_i \, b_i$ = **m** $= \sum_{i=1}^{n} a_i \, b'_i$ differing by atleast one bit.

Then, traversing both sequences and finding first differing bit from last.
Now suppose, $b_k = 1$ and $b'_k = 0$ (k is the position where they differ first from last) .

$\implies$ a_k must have been included in the subset of sum m corresponding to the sequence b_i but not in subset corresponding to b'_i

But we are given in the problem, $a_k > \sum_{i=1}^{k-1} a_i$
$\implies$ $\sum_{i=1}^{k-1} a_i.b_i + a_k > \sum_{i=1}^{k-1} a * b_i$

So, here lies contradiction. So there exist a unique key.

Question assigned to the following page: 2

Algorithm to find the Key

- First set a counter and start traversing the sequence **a**.
- Traverse till an element more than **m** is found.
- Now set **sum = m**.
- If counter stops at some a_k , such that $a_k == sum$.
- Then key will be $b_i = 0 \; \forall \; 1 \leq \mathbf{i} \leq \mathbf{n}$ && $\mathbf{i} \neq \mathbf{k}$ and b_k=1.
- If $a_k \neq$ m, then substract a_k from sum
  i.e,

$$\mathbf{sum} = \text{m} - a_k$$

- Now repeat the above steps to find the unique key untill sum become **0** then return b.

```
# code for algorithm discussed in problem 2
def key_finder(a,m):
    b=[0]*128
    sum=m
    while(sum>0):
        id=0
        for i in range(len(a)):
            if(a[i]<=sum):
                id+=1
            else:
                break
        if(a[id-1]==sum):
            b[id-1]=1
            sum=0
        else :
            b[id-1]=1;
            sum-=a[id-1]

        if(sum==0):
            break
    return b
```

Question assigned to the following page: 3

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

Lemma : 1
$a, x \in G$, $xa = ax \iff ax^{-1} = x^{-1}a$
as $a, x \in G$ both x and a are invertible.
hence,
$xa = ax \iff a = x^{-1}ax \iff ax^{-1} = x^{-1}a$

We have to solve this system of equation
$xa = ax$ —-(i)
$by = yb$ —-(ii)
$u = ugy$ —-(iii)
We know that each of these equation admit infinitly many solution independently and a unique solution will be common to all that unique solution is what we want to find
[unique sol. $x = a^l$, $y = b^m$]

$a^l.a = a^{l+1} = a.a^l$ —(i)

Question assigned to the following page: 3

$b^m.b = b^{m+1} = b.b^m$ —(ii)
$u = a^l.g.b^m$ ——(iii)

Hence, this is the only unique solution to all three equations.

we can cast the two variable equation into 1 variable by
$u = xgy$
$x^{-1}.u = gy \iff x^{-1} = gyu^{-1}$
It is possible as $x, g, y \in G$, hence ,Inverse exists.
Using Lemma 1;
$x^{-1}.a = a.x^{-1}$
$g.y.u^{-1}.a = a.g.y.u^{-1}$ —-(i)
$by = yb$ —(ii) Therefore, this is a system of equation in y only,
hence, we write (i) and (ii) as
$g.y.u^{-1}.a - a.g.y.u^{-1} = 0$
$by - yb = 0$
Now, y equals to

$$\begin{bmatrix} y_{11} & y_{12} & \cdots \\ y_{21} & \cdots & \cdots \\ \cdots & \cdots & y_{128,128} \end{bmatrix}$$

Hence we can make $2X128X128$ equation from (i) and (ii), but,
the number of variables are $128X128$, so no. of equation are more than no. of variables,
Hence, Two cases are possible
either a unique solution exist or no solution exist,
But as we have shown before a solution exist.
Therefore, we will find a unique solution.
This solution can be found by GAUSS ELIMINATION method.

Hence we have found the unique y.
Now, $x^{-1} = g.y.u^{-1}$
$\implies$ x^{-1} is determinable, hence x is also determinable.
We have found x ,y namely a^l , b^m.

Question assigned to the following page: 3

$$\mathbf{k} = \text{xvy}$$
$$\text{as } \mathbf{k} = a^{(l+r)}\text{g}b^{(m+s)}$$
$$\mathbf{k} = \text{x}a^{r}\text{g}b^{s}\text{y} = \text{xvy}$$
Ela can determine the values easily.

More over we can sometime skip this lengthy process if both **a, b** admit **two** different eigen values s.t.

$$\frac{\ln \lambda_a}{\ln \lambda'_a} \neq \frac{\ln \lambda_b}{\ln \lambda'_b}$$

where λ_a, λ'_a are eigen values of a
and λ_b, λ'_b are eigen values of b.

We can say that ,
y_1 be eigen-vector of a^T corresponding to λ_a

y_2 be eigen-vector of a^T corresponding to λ'_a

a and a^T have same eigenvalues

And
x_1 be the eigen-vector of b corresponding to λ_b

x_2 be the eigen-vector of b corresponding to λ'_b

Now

$$\mathbf{u} = a^{l}\text{g}b^{m}$$
$$[a^T.y_1 = \lambda_a.y_1] \text{ , After Taking transpose : } [{y_1}^T.a = {y_1}^t.\lambda_a]$$
$$\text{Then , } y_1^T\text{u}x_1 = y_1^T a^{l}\text{g}b^{m}x_1$$
$$y_1^T\text{u}x_1 = \lambda_a^l y_1^T\text{g}x_1\lambda_b^m$$

$$\lambda_a^l\lambda_b^m = \frac{y_1^T.u.x_1}{y_1^T.g.x_1}$$

Taking ln both sides

Question assigned to the following page: 3

$$\text{l.ln}\lambda_a + \text{m.ln}\lambda_b = \frac{(y_1^T.u.x_1)}{(y_1^T.g.x_1)}$$

Similarly

$$\text{l.ln}\lambda'_a + \text{m.ln}\lambda'_b = \frac{y_2^T.u.x_2}{y_2^T.g.x_2}$$

We obtain two simultaneous equations that can be solved easily.

So, we can find **l, m**

$$\mathbf{k} = a^l \text{v} b^m$$

as shown earlier.

Question assigned to the following page: 3

References

For Question 1:
Lecture no.6 slide no. 10 onwards to lec. 7 and upto slide 8.