CSE653 - Topics in Cryptanalysis
End Semester Examination - Winter 2025

Name - 27^{th} April 2025
Roll No - Total Marks - 30

Answer all questions

1. Answer the following questions: $[(0.5 \times 4) + 3 = 5]$

   (a) What are four *fault attack* models used in fault attack on ciphers.

   Any of the following four: known fault model, random fault model, bit flip, stuck-at-fault, byte/nibble faults, timing based faults.

   Writing the properties of block ciphers such as security, avalanche, etc will not carry any marks.

   (b) Consider that an attacker is able to inject faults at the 9th round of AES 128, just before the MixColumn operation, as described in the figure below.
   Let $x_f = x \oplus \varepsilon$. Then compute the value of $s_i \oplus s_i^f, \quad 0 \leq i \leq 3$, in terms of ε, a, b, c, and the required key bytes.

   The mixcolumn matrix is

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

   Now the value of (s_0, s_1, s_2, s_3) and $(s_0^f, s_1^f, s_2^f, s_3^f)$ is computed as

$$(s_0, s_1, s_2, s_3) = 2x + 3a + b + c, x + 2a + 3b + c, x + a + 2b + 3c, 2x + a + b + 3c$$
$$(s_0^f, s_1^f, s_2^f, s_3^f) = 2x_f + 3a + b + c, x_f + 2a + 3b + c, x_f + a + 2b + 3c, 2x_f + a + b + 3c$$

   Therefore

$$s_0 \oplus s_0^f = 2(x \oplus x_f) = 2\varepsilon, \quad s_1 \oplus s_1^f = (x \oplus x_f) = \varepsilon,$$
$$s_2 \oplus s_2^f = (x \oplus x_f) = \varepsilon, \quad s_3 \oplus s_3^f = 3(x \oplus x_f) = 3\varepsilon$$

   Note: If you didn't write the value of the MixColumn **1 marks will be deducted**, even if the method of calculation is right. No discussion will be entertained in this regard. **Any undue discussion will lead to deduction of 1 more marks**.

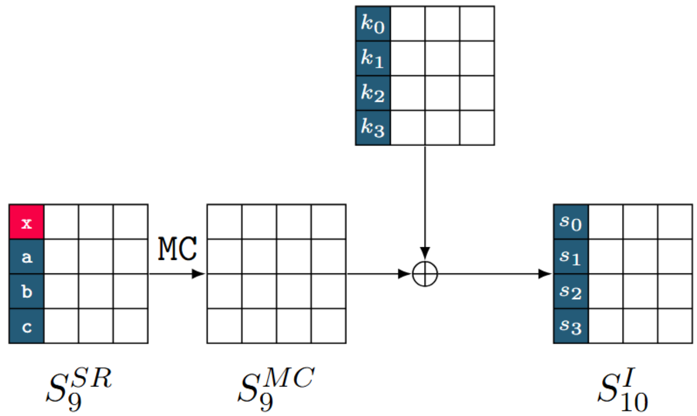
2. Answer the following questions: $[2+2+2+(0.5 \times 4) = 8]$

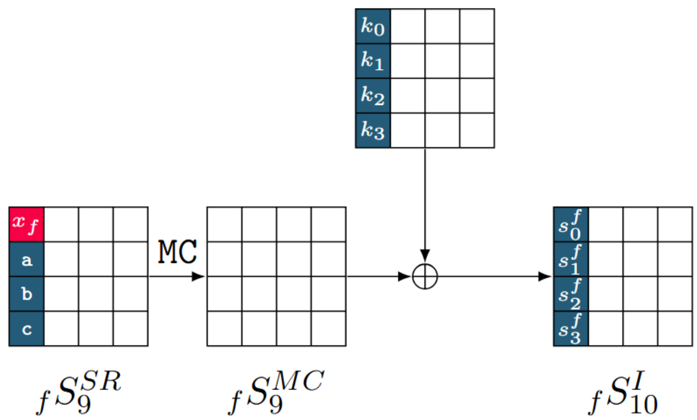
   (a) Show that the number of people needed to have a 50% chance of two colliding birthdays is 23.

   Let $P(n)$ be the probability that no two out of n people share a birthday.

   For $n = 1$:
   Only one person $\Rightarrow$ probability $= 1$.

   For $n = 2$:
   First person: any birthday (365 options).
   Second person: 364 choices (to avoid matching the first).





$$P(2) = \frac{365}{365} \cdot \frac{364}{365}$$

In general, for $n \leq 365$:

$$P(n) = \frac{365}{365} \cdot \frac{364}{365} \cdot \frac{363}{365} \cdots \frac{365-n+1}{365} = \prod_{k=0}^{n-1} \left(\frac{365-k}{365} \right)$$

which shows that the number of people needed to have a 50% chance of two colliding birthdays is 23

Now, calculate this value for $n = 23$:

$$P(23) \approx 0.4927$$

So the probability that at least two people share a birthday is:

$$1 - P(23) \approx 1 - 0.4927 = 0.5073$$

(b) Consider that you have a n-bit hash function. Describe a birthday attack in order to find collisions for this hash function. (State the steps clearly).

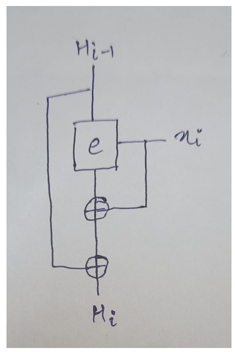
i. Compute $2^{n/2}$ hashes of $2^{n/2}$ arbitrarily chosen messages and store all the message/hash pairs in a list.

ii. Sort the list with respect to the hash value to move any identical hash values next to each other.

iii. Search the sorted list to find two consecutive entries with the same hash value.

(c) Draw a block diagram for the following hash function bilt from a block cipher $e()$:

$$e(x_i, H_{i-1}) \oplus x_i \oplus H_{i-1}$$



(d) List 4 properties of hash functions.

Any of the four: arbitrary sized input, fixed sized output, efficiently computable, preimage resistant, second preimage resistant, collision resistant

3. Answer the following questions: [(1.5+0.5)+(2+0.5+0.5)+(1+1)= 7]

(a) Show that if $n = pq$, where p and q are distinct prime numbers, and we know the values of n and $\phi(n)$, then it is easy to find p and q. Using this factorize 143. (Use the quadratic formulae)

Suppose $n = pq$ is the product of two distinct primes. If we know n and $\phi(n)$, then we can quickly find p and q.

Note that:

$$n - \phi(n) + 1 = pq - (p-1)(q-1) + 1 = p + q$$

Therefore, we know both pq and $p+q$. The roots of the polynomial

$$X^2 - (n - \phi(n) + 1)X + n = X^2 - (p+q)X + pq = (X-p)(X-q)$$

are p and q, but they can also be calculated using the quadratic formula:

$$p, q = \frac{(n - \phi(n) + 1) \pm \sqrt{(n - \phi(n) + 1)^2 - 4n}}{2}$$

This yields the values of p and q.

We have, $n = 143$ and we know that $\phi(n) = 120$.

Consider the quadratic equation:

$$X^2 - (n - \phi(n) + 1)X + n = X^2 - 24X + 143$$

The roots are given by:

$$X = \frac{24 \pm \sqrt{24^2 - 4 \cdot 143}}{2} = \frac{24 \pm \sqrt{576 - 572}}{2} = \frac{24 \pm \sqrt{4}}{2} = \frac{24 \pm 2}{2}$$

$$\Rightarrow X = 13 \quad \text{or} \quad X = 11$$

So, $p = 13$ and $q = 11$.

(b) Consider that a 56-bit key is written as a number $m \approx 10^{17}$. This is encrypted using RSA as $c = m^e(\mod n)$.
Describe an attack (**NOT bruteforce**), given c, to recover the value of m.
What is the complexity of this attack?
When will this attack fail?

The attack is as follows. The attacker makes two lists:

i. $cx^{-e} \pmod n$ for all x with $1 < x < 10^9$.
ii. $y^e \pmod n$ for all y with $1 < y < 10^9$.

She looks for a match between an element on the first list and an element on the second list. If she finds one, then she has:

$$cx^{-e} \equiv y^e \pmod n$$

This yields:

$$c \equiv x^e y^e \pmod n \Rightarrow c \equiv (xy)^e \pmod n$$

So:

$$m \equiv xy \pmod n$$

Complexity: - $O(2^9)$

Failure: The attack fails if x or $y > 10^9$

(c) State the **Fermat's Primality Test**. Using this show that 72 is not a prime.

Fermat Primality Test.

Let $n > 1$ be an integer. Choose a random integer a with $1 < a < n - 1$.

- If $a^{n-1} \not\equiv 1 \pmod n$, then n is **composite**.
- If $a^{n-1} \equiv 1 \pmod n$, then n is **probably prime**.

Given $n = 72$. Choose a random integer a such that $1 < a < n - 1$.
Let us pick $a = 5$ (a common small base for the test).
Now compute:

$$a^{n-1} \bmod n = 5^{71} \bmod 72$$

Using modular exponentiation, we find:

$$5^{71} \bmod 72 \neq 1$$

For example:

$$\begin{aligned}
&5^2 = 25, \\
&5^4 = 625, \quad 625 \bmod 72 = 49, \\
&5^{16} = 49 * 49 = 25 \bmod 72 \\
&5^{64} = 5^4 * 5^{16} = 49 * 25 \bmod 72 = 1 \\
&5^{71} = 5^{64} * 5^4 * 5^2 * 5 = 1 * 49 * 25 * 5 = 5 \bmod 72
\end{aligned}$$

Therefore,

$$5^{71} \not\equiv 1 \pmod{72} \Rightarrow 72 \text{ is composite.}$$

Note: You can use any $1 < a < n-1$

4. Answer the following questions: [(1+2)+1+(2+1) (2.5+0.5)= 10]

(a) State and prove the **Piling Up** lemma

Piling-up Lemma. Let $e_{i_1,i_2,\ldots,i_k}$ denote the bias of the random variable

$$X_{i_1} \oplus X_{i_2} \oplus \cdots \oplus X_{i_k}.$$

Then,

$$e_{i_1,i_2,\ldots,i_k} = 2^{k-1} \prod_{j=1}^{k} e_{i_j}.$$

Proof. The proof is by induction on k. Clearly, the result is true when $k = 1$. We next prove the result for $k = 2$, where we want to determine the bias of $X_{i_1} \oplus X_{i_2}$.
We have that

$$\Pr[X_{i_1} \oplus X_{i_2} = 0] = \left(\frac{1}{2} + e_{i_1}\right)\left(\frac{1}{2} + e_{i_2}\right) + \left(\frac{1}{2} - e_{i_1}\right)\left(\frac{1}{2} - e_{i_2}\right) = \frac{1}{2} + 2e_{i_1}e_{i_2}.$$

Hence, the bias of $X_{i_1} \oplus X_{i_2}$ is $2e_{i_1}e_{i_2}$, as claimed.
Now, as an induction hypothesis, assume that the result is true for $k = \ell$, for some positive integer $\ell \geq 2$. We will prove that the formula is true for $k = \ell + 1$.
We want to determine the bias of $X_{i_1} \oplus X_{i_2} \oplus \cdots \oplus X_{i_{\ell+1}}$. We split this random variable into two parts, as follows:

$$X_{i_1} \oplus \cdots \oplus X_{i_{\ell+1}} = (X_{i_1} \oplus \cdots \oplus X_{i_\ell}) \oplus X_{i_{\ell+1}}.$$

The bias of $X_{i_1} \oplus \cdots \oplus X_{i_\ell}$ is $2^{\ell-1}\prod_{j=1}^{\ell} e_{i_j}$ (by induction), and the bias of $X_{i_{\ell+1}}$ is $e_{i_{\ell+1}}$. Then, by induction (more specifically, using the formula for $k = 2$), the bias of $X_{i_1} \oplus \cdots \oplus X_{i_{\ell+1}}$ is

$$2 \times \left(2^{\ell-1} \prod_{j=1}^{\ell} e_{i_j}\right) \times e_{i_{\ell+1}} = 2^{\ell} \prod_{j=1}^{\ell+1} e_{i_j},$$

as desired.
By induction, the proof is complete.

(b) Define $N_L(a, b)$ for a 4-bit S-box with input (x_1, x_2, x_3, x_4) and output (y_1, y_2, y_3, y_4).

For a random variable with (hexadecimal) input sum a and output sum b, where $a = (a_1, a_2, a_3, a_4)$ and $b = (b_1, b_2, b_3, b_4)$ (in binary), let $N_L(a, b)$ denote the number of binary eight-tuples $(x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4)$ such that

$$(y_1, y_2, y_3, y_4) = \pi_S(x_1, x_2, x_3, x_4)$$

and

$$\bigoplus_{i=1}^{4} a_i x_i \oplus \bigoplus_{i=1}^{4} b_i y_i = 0.$$

(c) Consider the following S-box:

If $a = 9 = [1001]$ and $b = 2 = [0010]$ then what is $N_L(a, b)$ for the above S-box?
Also compute the value of $\epsilon(a, b)$.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$y = S(x)$	F	E	B	C	6	D	7	8	0	3	9	A	4	2	1	5

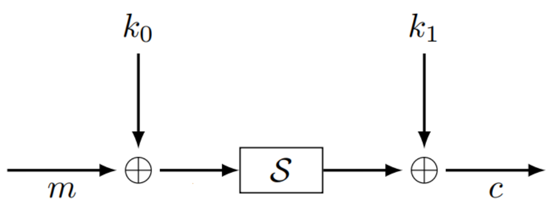
For $a = 9 = [1001]$ and $b = 2 = [0010]$, we have

$\alpha \cdot x$	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0
$\beta \cdot S(x)$	1	1	1	0	1	0	1	0	0	1	0	1	0	1	0	0

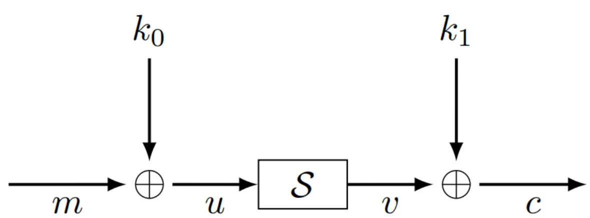
It is clear that $N_L(a, b) = 2$. Therefore the value of $\epsilon(a, b)$ is $-3/8$

(d) Consider a toy cipher: $c = S(m \oplus k_0) \oplus k_1$, where $m, c, k_0, k_1 \in \{0, 1\}^4$, as illustrated below.

For the S-box given above and the values of $a = 9$ and $b = 2$, calculate the value of the relation $k_0 \oplus k_1$ in terms of a, b, m, and c. What is the probability of this relation?



Consider the following figure



From the figure, we have:

$$u = m \oplus k_0 \quad \text{with probability } 1.$$

$$\alpha \cdot u \oplus \beta \cdot v = 0 \quad \text{with probability } \frac{1}{8}.$$

$$v = c \oplus k_1 \quad \text{with probability } 1.$$

This can also be written as:

$$\alpha \cdot u \oplus \beta \cdot v = 0 \quad \text{with probability } \frac{1}{8}.$$

Substituting for u and v, we get:

$$\alpha \cdot (m \oplus k_0) \oplus \beta \cdot (c \oplus k_1) = 0 \quad \text{with probability } \frac{1}{8}.$$

Finally, simplifying, we obtain:

$$\alpha \cdot k_0 \oplus \beta \cdot k_1 = \alpha \cdot m \oplus \beta \cdot c \quad \text{with probability } \frac{1}{8}.$$