Qutaiba ALASHQAR, 202900036. 3. sınıf.

BLM 4530, Bilgi Güvenliği, final sınavı, 08.06.2023.

1.) b

2.) ~~a~~ a

3.) c

4.) ~~b~~ ~~d~~ d

5.) ~~c~~ a

6.)

1. confidentiality :- information were kept in secure.
2. Integrity: Make sure that the messages didn't modified in transit
3. Authentication:- ensures that the partines are authentic
4. Non-repudiation: ensure that the sender can not deny the message
5. Identification, Establishing and verification
6. Access Control, access to the resources
7. Availability, reliably available
8. Auditing, evidences could be Proided about the security
9. physical security, protection against phy. tampering
10. Anonymity, protection against discovery and misuse of identity.

7.) 8 bit LFSR //

CLK	FF_2	FF_1	$FF_0 = S_i$
0	0	0	1
1	1	0	0
2	0	1	0
3	1	0	1
4	1	1	0
5	1	1	1
6	0	1	1
7	0	0	1

XOR

0 0	0
0 1	1
1 0	1
1 1	0

$\Rightarrow$ 001

8.) $n = 33$, $e = 3$, RSA,

(a) $x = 5$, $sig(x) = 12$?

(b) $x = 5$, $sig(x) = 14$?

(a)

$k_{pub} = (n, e)$

$k_{pub} = (33, 3)$

$S = sig(x) = 12$ / $x = 5$

verific. // $S^e = x' \bmod n$

$x' = 12^3 \bmod 33$

$x' = 12$ ama $x = 5$ o zaman not valid.

(b)

$k_{pub} (n, e)$

$k_{pub} (33, 3)$

$S = sig(x) = 14$ / $x = 5$

verifi // $S^e = x' \bmod n$

$x' = S^e \bmod n$

$x' = 14^3 \bmod 33$

$x' = 5$

$x' = 5$ and $x = 5$

o zaman valid

4

9.) addition on $(3,1) + (5,1)$

Curve $\Rightarrow$ $y^2 = x^3 + 2x + 2 \mod 17$

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \mod p, & P \neq Q \text{ (add)} \\ \frac{3x_1^2 + a}{2y_1} \mod p, & P = Q \text{ (double)} \end{cases} \quad \begin{cases} x_3 = s^2 - x_1 - x_2 \mod p \\ y_3 = s(x_1 - x_3) - y_1 \mod p \end{cases}$$

$$s = \frac{1-1}{5-3} \mod 17 = 0 \mod 17 = 0 \qquad \boxed{s = 0}$$

* $x_3 = s^2 - x_1 - x_2 \mod p$

$x_3 = (0)^2 - (3) - (5) \mod 17$

$x_3 = -8 \mod 17$

$\boxed{x_3 = 9}$

* $y_3 = s(x_1 - x_3) - y_1 \mod 17$

$y_3 = 0(3-5) - 1 \mod 17$

$y_3 = -1 \mod 17$

$\boxed{y_3 = 16}$

New point by add. (x_3, y_3)

$(9, 16)$