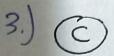
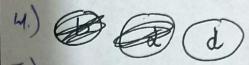
Qutaiba ALASHQAR, 20290036. 3. simf.

BLM 4530, Bilgi Gavenliĝi, hinal sinowi, 08.06.2023.











6.)

1. confidentiality: - information were kept in secure.

2. Integrity: Marke sure that the messeuges didn't motified

3. Authoritication: ensures that the partines are authoritic

4. Non-repudicition. onsume that the sender can not deny the many

5. Marchicasion, Establishing and venhication

6. Access County access to the resources

7. Availability, reliably available

8. Auditing, evidences could be Proided about the security

9. physical security, protection against phy. tramporing

lo. Anonymity, protection engainst discovery and misuse of identity.



7.) 8 bit LESR //

	CLK	FF2	FF,	FFo= Si
	0	0	0	
	1	11	0	20
	2	0	1	0
1	2	13	0	1
	4	1/3	1 1	0
	5	1 1	1 /3	1
1	6	0 1	A	,
1	7	000	131	
-				

XISR 0000

=> 001

8.) n=33, e=3, RSA, (x = 5, sig(x) = 12 ? (b) x=5, sig(x)=14? a Kpub=(n,e) Kpwh=(33,3) S = Sig(x) = 12 / x = 5 verlie. 1/5e=21 mod m x' = 12 mad 33 $\left[\chi'=12\right]$ and $\chi=5$ 0 sometiment pot valid. (b) + prod (m, e) Kpmh (33,3) 5 = sig (x) = 14/ X=5 berlill se x' mod " x'= 5° mal M x'= 14 mod 33 (x' = 5) x'=5 and x=5 O Zamun Valla

9.) addition (3,1) + (5,1)
Curve =>
$$y^2 = x^3 + 2x + 2 \mod 17$$

$$S = \begin{cases} \frac{y_2 - y_1}{2x_2 - x_1} & \text{mod } P, & P \neq Q \text{ (add)} \\ \frac{3x_1^2 + q}{2y_1} & \text{mod } P, & P = Q \text{ (doubled)} \end{cases} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \text{ mod } P \\ \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{P} \begin{cases} \chi_3 = S^2 - \chi_1 - \chi_2 \end{cases} \xrightarrow{$$

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

$$\chi_3 = (0)^2 - (3) - (5)$$
 mad 17

$$(x)$$
 $y_3 = 5(x, -x_3) - 4, mod 17$

New point by add.
$$(\chi_3, y_3)$$

$$(9,16)$$

