Li Xiangman 20119884

Section 1.

1. C	11. B	21. D
2. D	12. B	22. A
3. D	13. B	23. D
4. B	14. A	24. B
5. C	15. B	25. B
6. C	16. C.	26. A.
7. A	17. C	27. B
8. A	18. B	28. A
9. A	19. C	29. A
10. C	20. D	30. C

Section 2.

Q1.

1> because of Incentive.

① Block Reward

② Transaction Fee.

2> Find nonce to create block.

The method is

Hash | Hash (previous_hash || TS || tx root || nonce) < Threshold

each time the value is larger than threshold, update the nounce and compute, until find the value smaller than threshold

3> The Bitcoin payment use Bitcoin address to be the destination and source, it is a hash of ECDSA public key, and it is one-time public key. It will not linked to user's identity, because it is from a private ECDSA private key which is a random number.

4> Double spending is same bitcoins are spends two times

5>
① Finish transaction after finishing keeping account
② hash function prevents double spending of currency.

Q2.

1>. Handshake Procotal let client and server
a. negotiate MAC algorism and encryption
b. build the cipher key
c. establish session
d. connected each other
e. authenticate each other.

2>.

a. • Client Hello.
it is include TLS vision, Random number and Cipher suite.
The function is connect with Server and list the encription algorism that they can use, and the random # is used in binding session key

• Server Hello
it will include TLS vision, Random number and selected Cipher
↓
bilud session key

b. Serve AKE
① Certificate (optional) : Server sends the client a certificate
② Certificate request (optional) : if Server request client certificate, it will send this message

③. Server key exchange (op) : if certificate not include enough public key information, it will send this.

④. Serve hello done

C. Client AKE

① Certificate: (op) Client will sent if received request

② client key exchange: create master secret to use for symmetric encryption

③ certificate verify: (op) Client use public key to sign the certificate

d. Finish:

① Change Cipher Spec Protocol:
client tell server to change encrypt mode

② Finish: client tell server can start the secure data connection.

③ Change Cipher Spec Proctol:
server tell client ~~can~~ to change encrypt mode

④ Finish:
Server tell client can start the secure data connection

Q3.

$h(x) = xA$

$$\begin{cases} x_1+x_2+x_3+x_4 = 0 \\ x_2+x_3+x_4+x_5 = 1 \\ x_3+x_4+x_5+x_6 = 0 \\ x_4+x_5+x_6+x_7 = 1 \end{cases}$$

$\therefore x_5 - x_1 = 1$

$x_7 - x_3 = 1$

$x_2 - x_6 = 1$

$x_4 = x_1+x_2+x_3$

$\therefore$

x_1	x_2	x_3	x_4	x_5	x_6	x_7
0	0	0	0	1	1	1
0	0	1	1	1	1	0
0	1	0	1	1	0	1
0	1	1	0	1	0	0
1	0	0	1	0	1	1
1	0	1	0	0	1	0
1	1	0	0	0	0	1
1	1	1	1	0	0	0

Q4.

a7.

$x_p \leftarrow y^{d_p} \bmod p = y^{d \bmod (p-1)} \bmod p$

$= y^d \bmod p$

$x_q \leftarrow y^{d_q} \bmod q = y^{d \bmod (q-1)} \bmod q$

$= y^d \bmod q$

$x = M_p q y^d + M_q p y^d \bmod n$

$= q^{-1} \cdot q \cdot y^d + p^{-1} \cdot p \cdot y^d \bmod n$

↳ base on CRT

$\begin{cases} x \equiv y^d \bmod p \\ x \equiv y^d \bmod q \end{cases}$

↳ base on CRT

$\therefore x = y^d \bmod n.$

b7. $d_p = d \bmod (p-1) = 123 \bmod 14 = 11$

$d_q = d \bmod (q-1) = 123 \bmod 22 = 13$

$M_p = q^{-1} \bmod p = 23^{-1} \bmod 15 = 2$

$M_q = p^{-1} \bmod q = 15^{-1} \bmod 23 = 20$

c. $x_p = y^{d_p} \bmod p = 17^{11} \bmod 15 = 8$

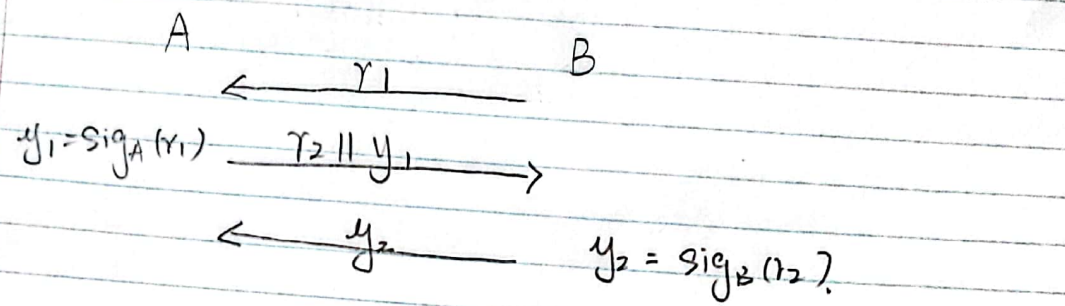
$x_q = y^{d_p} \bmod q = 17^{13} \bmod 23 = 10$

$x = M_p q y^d + M_q p y^d \bmod n$

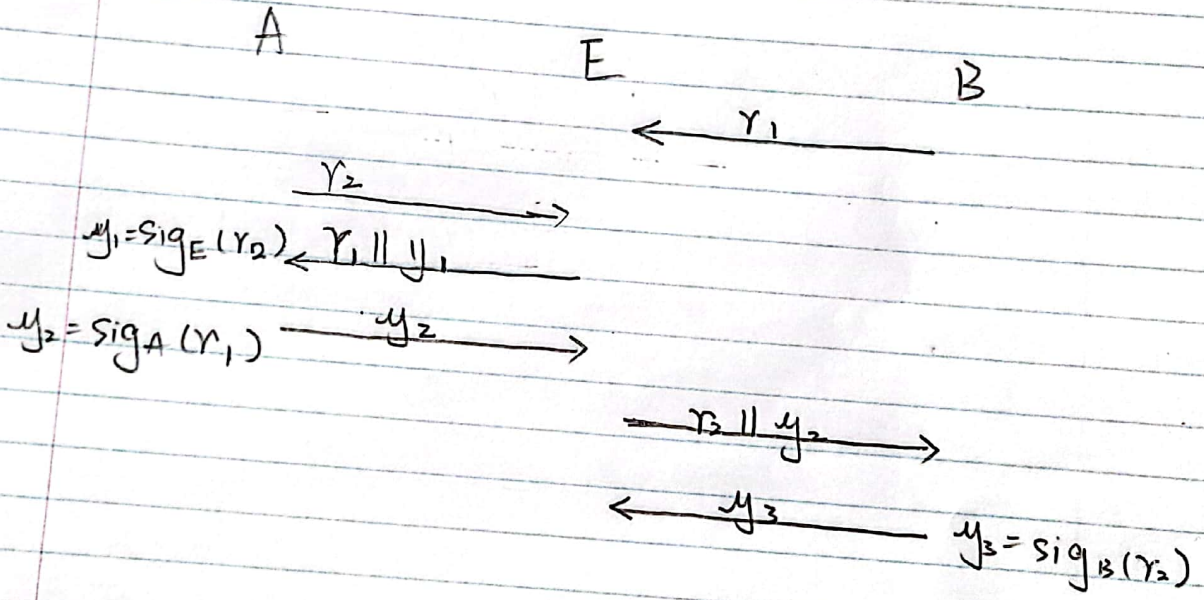
$= 2 \times 23 \times 8 + 20 \times 15 \times 10 \bmod 15 \times 23$

$= 263$

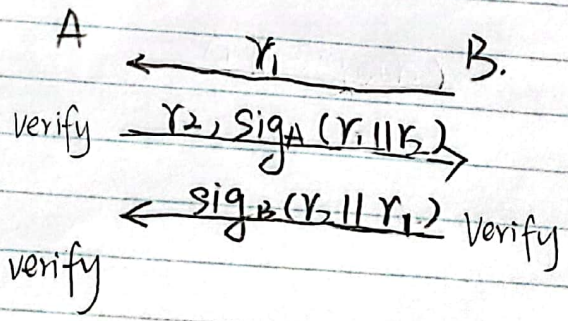
Q5.



- insecure, paralle atlack



improvment:



Abbey

Q6.

a> 2. β public

$\alpha^a \bmod p$

$\beta^{\delta} \equiv \alpha^{x-k\gamma} \bmod p$

$\equiv \alpha^x \cdot (\alpha^k)^{-\gamma} \bmod p$

$\beta^{\delta} \equiv \alpha^x \cdot \gamma^{-\gamma} \bmod p$

$\alpha^x \equiv \beta^{\delta} \cdot \gamma^{\gamma} \bmod p$

$\therefore u = \gamma^{\gamma}$

$v = \beta^{\delta}$

$w = \alpha^x$

if $w \equiv uv \bmod p$

the signature is valid.

else it will be reject

b> $A = \beta_1 = \alpha^{a_1} \bmod p$ (γ, δ_1) x_1

$B = \beta_2 = \alpha^{a_2} \bmod p$ (γ, δ_2) x_2

$|a_1 - a_2| <= c$

$\delta_1 = (x_1 - k\gamma) a_1^{-1} \bmod (p-1)$

$\delta_2 = (x_2 - k\gamma) a_2^{-1} \bmod (p-1)$

$\therefore \beta_1 \cdot \beta_2^{-1} = \alpha^{a_1} \cdot \alpha^{-a_2} = \alpha^{a_1 - a_2} \bmod p$

$= \alpha^c \bmod p$

because c is small in absolute valu so it can compute c from $\alpha^c \bmod p$

∴ now adversary get $c = a_1 - a_2$

Then $\delta_1 \cdot (c - a_2) = x_1 - k\gamma \mod (p-1)$

$\delta_2 \cdot a_2 = x_2 - k\gamma \mod (p-1)$

we know (γ, δ_1), (γ, δ_2), x_1, x_2, p, c

So we have two equation and two unknown number k, a_2,

we can compute k, a_2

then use $c - a_2$ get a_1.