24 - S1 - Q2

(a) D. H. $p = 7$ $g = 5$

Alice private key $a = 7$

Bob $b = 4$

(i) pub. key ?

(ii) shared key ?

(b) digital signature ?

Bitcoin & Ethereum

Solution (a)(i)

① $y_A = g^a \bmod p$

$= 5^7 \bmod 7$

$= 5$

So Alice's public key is 5

② $y_B = g^b \bmod p$

$= 5^4 \bmod 7$

$= 2$

So Bob's public key is 2

(ii) shared key

Alice : $y_B^a \bmod p$

$= 2^7 \bmod 7$

$= 2$

Bob : $y_A^b \bmod p$

$= 5^4 \bmod 7$

$= 2$

So, the shared secret key is 2

(b) ① Definition:

A digital signature is a message digest used to cryptographically sign a message

② Signing process:

(1) the signer generate a hash of message

(2) the signer use a private key to encrypt this hash, producing the signature

(3) the original message and the signature are then transmitted

③ Verification:

(1) the verifier recomputes the hash of the received message

(2) the verifier uses the public key of the signer to decrypt the signature back into a hash value

(3) If the two hashes match, the verifier knows the document was not altered (integrity) and it was indeed signed by the claimed signer (authenticity).

④ Role of Hash Functions

(1) Hash functions produce a short fingerprint from longer message

(2) efficiency: only the small digest is signed, it just a bit string of small fixed length

(3) security

Once the algorithm is processed, there is no feasible way to use the ciphertext to retrieve the plaintext.

There is no feasible way to generate two different plain texts that compute to the same hash value

⑤ Digital Signature in Blockchain and Cryptocurrencies

(1) Blockchain uses cryptographic techniques, such as hashing and digital signatures to ensure transaction authenticity

(2) Blockchain: the record of an event, cryptographically secured with a digital signature

(3) Bitcoin, Ethereum heavily used digital signature such as ECDSA

(4) Each transation is signed by the sender's private key, so that the network can verify

that the rightful owner of the funds has authorized the transaction

(5) validators check these signatures before including transaction in blocks

(6) This mechanism enforces trustless validation no central authority is needed — only the math of digital signatures and consensus rules.