23-S2-Q2

(a) RSA : forward secrecy concept and why differ : DH

(b) $p = 11$ $g = 5$

Alice private key $a = 6$

Bob $b = 7$

(i) Alice public A

(ii) Bob B

(iii) Share S.

(iv) A $B \rightarrow S$

Solution : (a)

① concept

If someone records the encrypted conversation and then gets a hold of the RSA private key of the server, they can decrypt the conversation.

② why

attacker records previous encrypted content C

and get service private key d

the message M can be computed

$$M = C^d \bmod n$$

③ different RSA Diffie-Hellman

(1) Functionality:

RSA: Primarily an asymmetric encryption and signature scheme

Diffie-Hellman: A public key algorithm only for key exchange and doesn't encrypt or decrypt the message.

(2) Use Cases

RSA: digital signatures and key transport

Diffie-Hellman:

1. electronic key exchange method of the Secure Sockets Layer (SSL) protocal
2. Enable the sharing of secret key between two people who have not contacted each other before

(b) (i) $p = 11$ $g = 5$ $a = 6$ $b = 7$

$$A = g^a \bmod p$$

$$= 5^6 \bmod 11$$

$$= 5$$

(ii) $B = g^b \bmod p$

$= 5^7 \bmod 11$

$= 3$

(iii) ① $S = A^b \bmod p$

$= 5^7 \bmod 11$

$= 3$

② $S = B^a \bmod p$

$= 3^6 \bmod 11$

$= 3$

So, $S = 3$

The math behind Diffie-Hellman ensure $g^{ab} \bmod p$ is the same regardless of whether you compute $(g^a)^b$ or

$(g^b)^a$

(iv) If an attacker obtains both a and b the they can trivially compute shared key

$s = g^a \bmod p$ or $s = g^b \bmod p$

or $s = g^{ab} \bmod p$

$= 5^{6\times 7} \bmod 11$

$= (5^6)^7 \bmod 11$

$= 5^7 \bmod 11$

$= 3$