24-S1-Q1

Q: RSA

(a) small prime num affect security?

(i) RSA: 5 11 pub: 3 private?

(ii) m=4, C=?

(iii) decrypt?

(b) (i) spear? whaling? target?

(ii) technological measure?

Solution (a)

① RSA relies on the computational difficulty of factoring large numbers.

② If small prime numbers are used (eg. 5 and 11), an attacker can factor the RSA modulus n extremely quickly

③ One n is factored, the attacker knows the secret $\varphi(n)$ and can easily compute the private key d. This completely breaks RSA security

④ In a real deployment, primes used should typically be 512, 1024, or more bits long so that factoring n is infeasible within given time with current technology

(i) Calculate Bob's private key d

$p = 5$, $q = 11$

$n = p \times q = 5 \times 11 = 55$

$\phi(n) = (p-1) \times (q-1) = 4 \times 10 = 40$

4 factor : 2

10 factor : 2 , 5

Select e from 1 2 3 5 7 11 13 ...

× × ✓ × ✓ ✓ ✓

$e = 3$

$e \cdot d \bmod \phi(n) = 1$

let k denote positive integer

$$d = \frac{k \cdot \phi(n) + 1}{e}$$

$$= \frac{40k+1}{3}$$

let $k=1$, $d = \frac{41}{3}$ ×

let $k = 2$, $d = \frac{81}{3} = 27$ ✓

So, the Bob's private key is 27

(ii) Alice ciphertext c

$$c = m^e \bmod n$$

$$= 4^3 \bmod 55$$

$$= 9$$

(iii) Bob decrypt :

$$c^d \bmod n$$

$$= 9^{27} \bmod 55$$

$$= (9^3)^9 \bmod 55$$

$$= 729^9 \bmod 55$$

$$= 14^9 \bmod 55$$

$$= [(14)^3]^3 \bmod 55$$

$= (2744)^3 \bmod 55$

$= (49)^3 \bmod 55$

$= 4$

So, Bob recover the original message $m = 4$

(b) (i) Spear Phishing

① Although spear phishing uses email, it takes a more targeted approach.

② Cyber criminals targets a specific individual or a group of people.

whaling phishing attack

① A whaling phishing attack is an advanced form of phishing that is precisely engineered to target the most critical individuals in companies.

② Such as senior executives, high-ranking managers and employees with high-level access.

(ii) measures

① Scrutinize the emails you receive.
Most phishing emails have significant errors like spelling mistakes and format changes from that of legitimate sources.

② Make use of an anti-phishing tool bar

③ Update your passwords regularly and use MFT

④ Conduct regular employee training

⑤ Stay up-to-date with security patches and updates.