RSA

Wednesday, February 23, 2022 12:37 PM

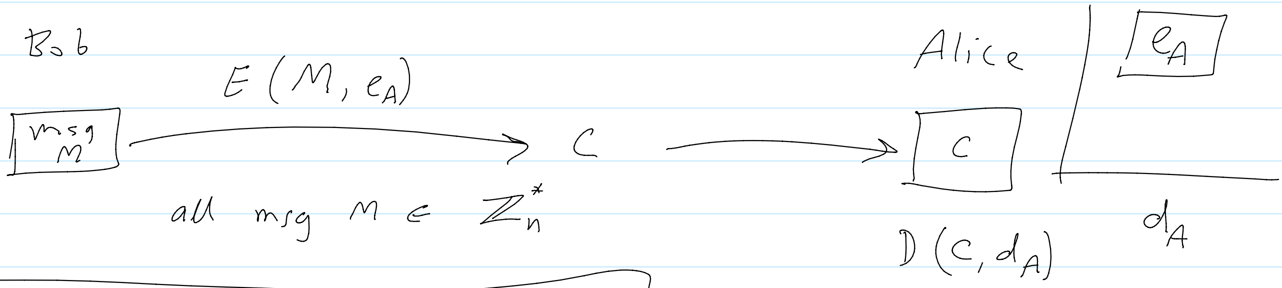
Missing

#1, 2, 8

Recall : $\phi(n)$

1] RSA Cryptosystem

- 1980's by Rivest, Shamir, Adleman
- public-key crypto system
    - two keys : - public (e): for encryption
      - private (d): for decryption
    - infeasible to compute d from e.
- RSA is based on the dificulty on integer factorization
  $n = p \cdot q$



$D(E(M, e_A), d_A) = M$

2] RSA Setups : for user A

1. Choose large primes : p, q (> 155 digits)
2. $n = p \cdot q$ (> 300 digits)
3. $\phi(n) = (p-1)(q-1)$
4. choose a public-key e relatively prime to $\phi(n)$
   publish (e, n)
5. compute the private $d = e^{-1} \pmod{\phi(n)}$
6. Encryption function : to encrypt M

   $$C = E(M, e) = M^e \pmod{n}$$

7. Decryption function : to decrypt C

   $$D(C, d) = C^d \pmod{n}$$

proof:

$$c^d = (M^e)^d \equiv M^{ed} \equiv M^1 \equiv M \pmod{n}$$

3] e.g. ① Set up an RSA scheme with $p = 5$, $q = 11$

② Create a pair of keys

③ encrypt $M = 7$

① Ammar computes $n = p \cdot q = 55$

$$\phi(n) = 4 \cdot 10 = 40$$

② pub-key $e = 2$ ✗ not co-prime 40

pri-key $d = 2^{-1} \bmod 40$ ✗

pub-key $e = 3$ ✓

pri-key $d \equiv 3^{-1} \pmod{40}$

$\equiv -13 \equiv 27 \pmod{40}$

$\gcd(40, 3) = 1$

$1 \equiv x \cdot 3 + y \cdot 40$

$13 \cdot 3 = 39 \equiv -1$

$(-13) \cdot 3 \equiv 1$

③ To encrypt 7

$$E(7, 3) \equiv 7^3 \pmod{55}$$

$$\equiv 7^2 \cdot 7$$

$$\equiv (-6) \cdot 7$$

$$\equiv -42 \equiv 13 \pmod{55}$$

To decrypt $C = 13$

$$D(13, 27) \equiv 13^{27}$$

$$\equiv 7 \pmod{55}$$

4] Read Diffie-Hellman key-exchange protocol. as an application of modular arithmetic

5] Check digit:

$$x_1 x_2 \ldots x_n, x_{n+1}$$

e.g. ① Even parity:

$x_1 x_2 \dots x_n, x_{n+1}$

e.g. ① Even parity:

$$x_{n+1} = \sum x_i \pmod 2 \qquad \text{even parity}$$

② UPCs: Universal Product Check

$$x_{n+1} = 3x_1 + x_2 + 3x_3 + \dots + x_{12} \equiv 0 \pmod{10}$$

③ ISBN: international std book number
(ISBN-10)

$$x_{10} = \sum_i i \cdot x_i \equiv 0 \pmod{11}$$; use digit X for 10

e.g.

$$\text{ISBN} = \underbrace{234\ 111\ 222}\ \underbrace{6}$$

scanned

11

$$2\ \boxed{?}\ 4\ 111\ 222\ 6$$