Public-key Cryptography

Saturday, September 30, 2023 12:17 PM

Recall : linear congruences

$$ax \equiv b \pmod n$$

$$\Rightarrow x \equiv b \cdot a^{-1} \pmod n$$

what if no a^{-1}?

$$\gcd(a, n) = d \neq 1$$

$d \nmid b$ → No solutions

$d \mid b$ → d solutions

① simplify (div by d)

$$gx \equiv h \pmod m$$

$$\Rightarrow x_0 \equiv h \cdot g^{-1} \pmod m$$

$$x_1 = x_0$$

$$x_k = x_0 + km$$

$$x_d = x_0 + dm$$

$g = \frac{a}{d}$, $h = \frac{b}{d}$, $m = n/d$

e.g.

$$12x \equiv 15 \pmod{21}$$

$$\Rightarrow 4x \equiv 5 \pmod 7$$

$$x \equiv 5 \cdot 4^{-1} \equiv 5 \cdot 2 \equiv 3$$

$$x_1 = 3$$

$$x_2 = 3 + 7 = 10$$

$$x_3 = 3 + 2 \cdot 7 = 17$$

§9. Public-key Cryptograph:

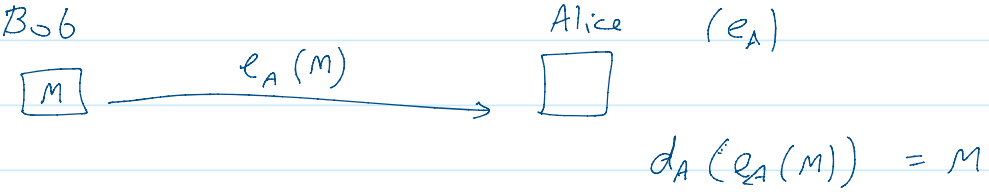
13 a public-key crypto scheme : 2 keys

① Each user $\underline{A}$ has a public-key e_A for encryption and a private-key d_A for decryption

② People use e_A to encrypt messages to A

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

③ User A uses d_A to decrypt. $d_A(e_A(M)) = M$



④ It is computationally infeasible to compute d_A from e_A

2] RSA Crypto-system

- by Rivest-Shamir-Adleman 1980's
- it is based on the difficulty of integer factorization

3] RSA setups: for user A

1. choose large primes p, q (>300 digits)
2. $n = p \cdot q$, $\mathbb{Z}_n^*$
3. $\phi(n) = (p-1)(q-1)$
4. A chooses public-key (e, n) s.t. $\gcd(\phi(n), e) = 1$
5. Compute A's private-key (d), $d = e^{-1} \pmod{\phi(n)}$

4] RSA: Encryption

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

4] RSA : Encryption

$$E(M) = M^e \pmod n \equiv C$$

Decryption

$$D(C) = C^d \pmod n$$

Note:

$$C^d \equiv (M^e)^d \equiv M^{e \cdot d} \pmod n$$
$$\equiv M^1 \equiv M \pmod n$$

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

$n = p \cdot q = 55$

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

choose $e = 3$

$d = 3^{-1} \pmod{40}$

$\equiv 27$

$3 \times 13 \equiv 39 \equiv -1$

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

$-13 \equiv 27$

Encrypt $M = 7$

$E(7) = M^e \bmod n$

$\equiv 7^3 \pmod{55}$

$C \equiv 13$

Decrypt $C = 13$

$D(13) = 13^{27} \pmod{55}$

$\equiv 7$

6] Discrete-log Problem

in $\mathbb{Z}_p^*$, $\quad b^x \equiv a \pmod p$

$\Rightarrow x = \log_b a \pmod p$

b^{24}

$[[(b \cdot b)^2]^2]^2 \cdot b^8$

b^8

e.g. $\mathbb{Z}_{13}^*$

$\langle 2 \rangle = \{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$

$2^x \equiv 5 \pmod{13}$

Find x?

7] Note: It is computationally infeasible to compute the DLog.

8] Diffie-Hellman key-exchange scheme

Alice	Eve	Bob
1. Alice and Bob agree prime p, and $g \in \mathbb{Z}_p^*$ of large order.	p, g	p, g	p, g
2. Alice chooses private x Bob chooses private y	x	$a = g^x$ $b = g^y$	y
3. Alice sends $a \equiv g^x$ Bob sends $b \equiv g^y$	$a \equiv g^x$		$b \equiv g^y$
4. A computes $b^x = g^{yx} \equiv$ key B computes $a^y = g^{xy} \equiv$ key	b		a

$b^x = (g^y)^x = g^{xy} = (g^x)^y = a^y$

9] Diffie-Hellman assumption:

"It is infeasible to compute g^{xy} knowing only g^x and g^y"

10] e.g. $72 \equiv (-2) \pmod{11}$

$p = 13, \quad g = 2$

A	B
$p = 13, \ g = 2$	
$x = 7$	$y = 5$
$a = g^x \equiv 11$	$b = 2^5 \equiv 6$
$a = 11$ →	
	← $b = 6$
$b^x = 6^7 = 7$	$a^y \equiv 11^5 \pmod{13}$
	$\equiv (-2)^5$
	$\equiv -32 \equiv -6 \equiv 7 \pmod{13}$

11] ElGamal scheme

- public-key crypto-system based DLog Problem