RSA

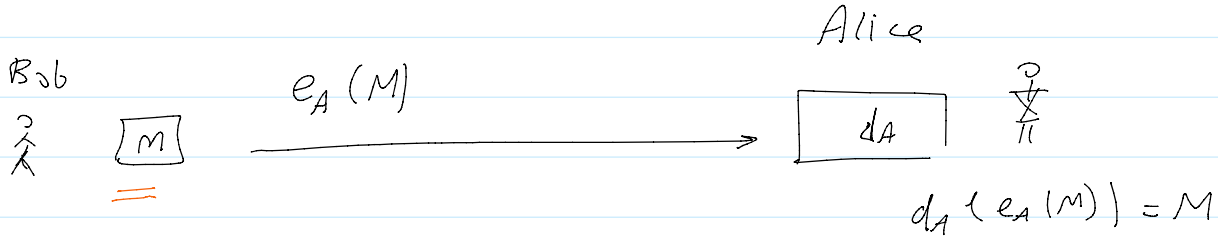
Monday, November 3, 2025 9:15 AM

See Slides P06

Missing -
100 # 5, 6, 7, 9, 13, 14, 17
200 # 10, 11, 14, 24,
500 # 2, 11, 14, 19, 20, 25, 26, 27,

1] RSA Crypto system

- Public-key crypto system (by Rivest, Shamir, Adleman), 1980's
- each user A has:
  - ① public-key: e_A for encryption
  - ② private-key: d_A for decryption.
- To Communicate



$d_A(e_A(M)) = M$

- Note: ① Convert all msgs to numbers in $\mathbb{Z}_n^*$ for some n.
  - ② $d_A(e_A(M)) = M$.
  - ③ infeasible to compute d_A from e_A.

2] RSA setups: (for user A)

① Choose 2 safe large primes: p, q (> 155 digits)
"(p-1)/2 is a prime"
keep p, q secret.

② $n = p \cdot q$ → $\mathbb{Z}_n^*$

③ $\phi(n) = \phi(p)\,\phi(q) = (p-1)(q-1)$

④ Key generation:

- Choose a public-key e such that $\gcd(e, \phi(n)) = 1$
- Compute the private-key $d = e^{-1} \pmod{\phi(n)}$

3] Encryption:

To encrypt $M \in \mathbb{Z}_n^*$

$$C \equiv f(M) \equiv M^e \pmod{n}$$

4] Decryption:

To decrypt C

$$M = f^{-1}(C) \equiv C^d \pmod{n}$$

Proof:

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

$$\equiv M^{ed} \pmod{\phi(n)}$$

$$\equiv M^1 \quad \text{by Euler Theorem}$$

5] e.g.

1 Set up an RSA scheme, with $p = 5$, $q = 11$

Soln

① $n = p \cdot q = 55$

② $\phi(n) = \phi(55) = 4 \cdot 10 = 40$

③ choose $e = 3$ $\quad \gcd(40, 3) = 1$

$$d \equiv e^{-1} \pmod{\phi(n)}$$
$$\equiv 3^{-1} \pmod{40}$$
$$\equiv (-13) \equiv 27 \pmod{40}$$

$-13 \cdot 3 \equiv -39$

[2] Encrypt $M = 8$

$$C \equiv M^e \pmod{n}$$
$$\equiv 8^3$$
$$\equiv 9 \cdot 8 \equiv 72 \equiv 17 \pmod{55}$$

[3] Decrypt $C = 17$

$$M \equiv C^d \pmod{n}$$
$$\equiv 17^{27}$$
$$\equiv 8 \pmod{55}$$

6] Modular Exponentiation (fast expo.)

$$b^m \pmod{n}$$
$$= \underbrace{b \cdot b \cdot b \cdot \ldots \cdot b}_{m-1 \text{ times}}$$

3^{19}

$19 = (10011)_2$

		y
3^1	d_0	3^1
3^2	d_1	$3^1 \cdot 3^2$
3^4		
3^8		
3^{16}	d_4	$3^1 \cdot 3^2 \cdot 3^{16}$

Mod Exp (b, m, n)

Output: $b^m \pmod n$

$m = (d_{k-1} \cdots\cdots d_1 d_0)_2$ ← i

Let $y = 1$; $a \equiv b \pmod n$

for $i = 0$ to $k-1$

{

if ($d_i == 1$)

{ $y = y * a$

}

$a = a * a$

}

Return y

e.g.

$14^{19} \pmod{11}$

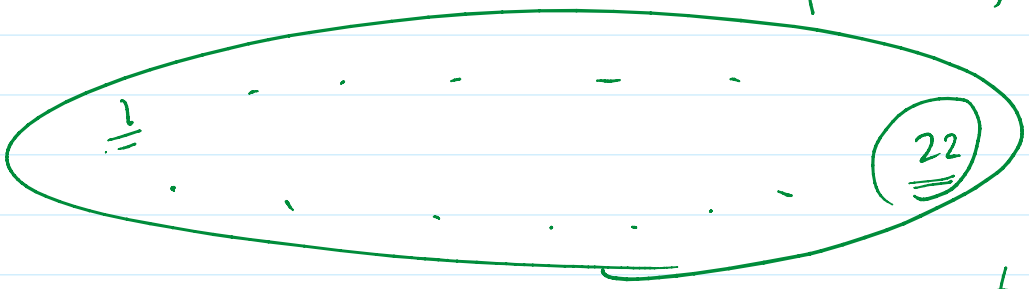
$19 = 10011_2$ ←

d_i	$y = 1$	$a \equiv 14 \equiv 3 \pmod{11}$
1	3	9
1	$27 \equiv 5$	$81 \equiv 4$
0	5	$16 \equiv 5$
0	5	$25 \equiv 3$
1	$15 \equiv 4$	9

$\therefore y = 4 \Rightarrow 14^{19} \equiv 4 \pmod{11}$

Why safe prime?

$|\mathbb{Z}_{23}^*| = 2 \cdot 11$



$\phi(2) = 1$

$M = 22$

$\phi(11) = 10$

$\phi(22) = 10$

M^e odd → 22

M^e even → 1