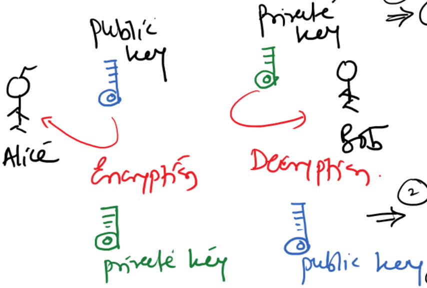
Public/Asymmetric Key Cryptosystem



① → Confidentiality

② → Digital signature

③ → authentication

→ ④ Key management (key distribution)

Algorithms: ① RSA
② Knapsack
③ ECC

Disadvantage: Slow (Speed ↓)

Public/Asymmetric Key Cryptosystem (cont.)

Requirements:

1. $D_{Kr}(E_{Ku}(P)) = P$
   Even though keys are different, the above conversion is possible just because both keys are originated by the same source/end.
   $\rightarrow$ Ku and Kr are inverse to each other (multiplicative inverse or additive inverse).
2. It is exceedingly difficult to deduce D from E (i.e., plaintext from ciphertext, private key from public key).
   $\rightarrow$ By knowing public key one can not find out the private key (modular arithmetic is considered).
3. Encryption cannot be broken by a chosen plaintext attack.

Public/Asymmetric Key Cryptosystem (cont.)

Public Key Cryptosystem:

1. Knapsack
2. RSA
3. Diffie-Hellman
4. Elliptic Curve Cryptography (ECC)

Public/Asymmetric Key Cryptosystem (cont.)

RSA Algorithm

$\Longrightarrow$ Invented by Rivest, Shamir, and Adleman @MIT, USA.

Key Generation

- p and q $\Longrightarrow$ large prime numbers.
- n = p $\times$ q
- z = (p - 1) $\times$ (q - 1)
- Choose e relatively prime to z (i.e., GCD(e,z) = 1)
- Fine d (multiplicative inverse of e modulo z)
  Here, (e $\times$ d) mod z = 1
- **Public Key**: {n, e}
- Encryption (E): C = P^e mod n
- **Private Key**: {n, d}
- Decryption (D): P = C^d mod n

Public/Asymmetric Key Cryptosystem (cont.)

Example

- p =3, and q = 11
- $n = p \times q = 33$
- $z = (p - 1) \times (q - 1) = 20$
- $GCD(e, z) = 1 \implies GCD(e, 20) = 1$
  $\implies e = 3, 7, 9, 11, 13, 17, 19$
  Let $e = 3$
- $(e \times d) \bmod z = 1 \implies (3 \times d) \bmod 20 = 1$
  $\implies d = 7$
- **Public Key**: $\{n, e\} = \{33, 3\}$
- **Private Key**: $\{n, d\} = \{33, 7\}$

Public/Asymmetric Key Cryptosystem (cont.)

- Let plaintext P = 19
- **Encryption (E)**: C = P^e mod n = 19^3 mod 33 = 6859 mod 33 = 28 (Ciphertext)
- **Decryption (D)**: P = C^d mod n = 28^7 mod 33 = 13492928512 mod 33 = 19 (Plaintext)

Questions

1. What will be the value of e for (e $\times$ 7) mod 360 = 1 ?
2. Encrypt the plaintext (P) "abcdefghij" using RSA algorithm for the following paramaters:
   - p = 5,
   - q =11, and
   - d = 27

Public/Asymmetric Key Cryptosystem (cont.)

Extended Euclidean Algorithm

known

$(e \times d) \bmod z = 1$

unknown

unknown

$(e \times d) \bmod z = 1$

known

$\overbrace{x_1 \quad x_2 \quad x_3}^{L}$			$\overbrace{y_1 \quad y_2 \quad y_3}^{R}$			$Q = \lfloor x_3 / y_3 \rfloor$ floor function
x_1	x_2	x_3	y_1	y_2	y_3	
1	0	z	0	1	e or d	
*	*	*	*	*	* → 1	Here $* = L - QR$

if $(y_3 == 1)$

Ans $= y_2$ iff $(y_2 > 0)$

if $(y_2 < 0)$

Ans $= y_2 + z$

Public/Asymmetric Key Cryptosystem (cont.)

Example 1: $(3 \times d) \bmod 20 = 1$

$$(\overset{e}{3} \times d) \bmod \overset{z}{20} = 1 \qquad d = ?$$

	x_1	x_2	x_3		y_1	y_2	y_3		$Q = \lfloor x_3/y_3 \rfloor$	
a	1	0	20	b	0	1	3	c	$Q = \lfloor 20/3 \rfloor = 6$	
	0	1	3 (e)	d	1	−6	2		$Q = \lfloor 3/2 \rfloor = 1$	f
				g	−1	7	1			

$y_3 \neq 1$

$y_3 == 1$

Steps: a, b, c, d, e, f, and g

$\therefore \boxed{d = 7}$ as $y_2 > 0$

Public/Asymmetric Key Cryptosystem (cont.)

Example 2: $(5 \times d) \bmod 96 = 1$

$(\underbrace{5}_{e} \times d) \bmod \underbrace{96}_{z} = 1 \qquad d = ?$

x_1	x_2	x_3	y_1	y_2	y_3	$Q = \lfloor x_3 / y_3 \rfloor$
1	0	96	0	1	5	$Q = \lfloor 96/5 \rfloor = 19$
			1	-19	1	$\rightarrow y_3 == 1$

$\therefore d = y_2 + z \rightarrow$ as $y_2 < 0$

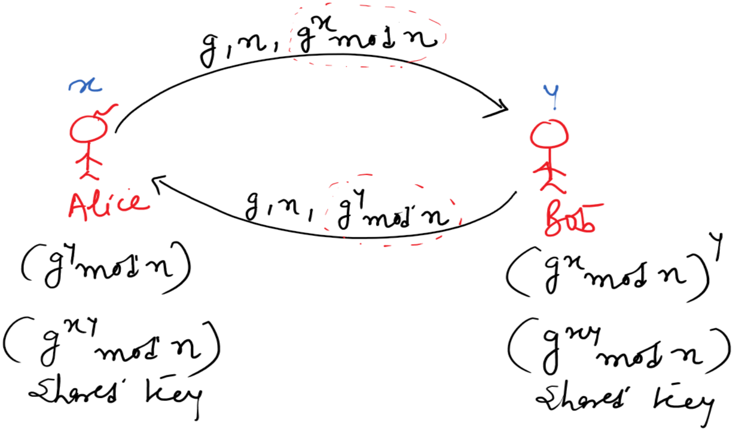
$= -19 + 96$

$d = 77$

Public/Asymmetric Key Cryptosystem (cont.)

Diffie-Hellman Key Exchange Algorithm

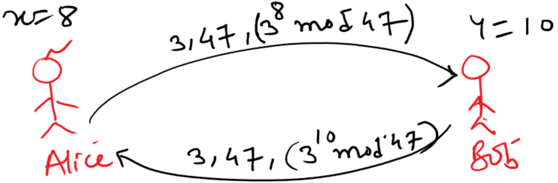
Purpose: Key Distribution



Public/Asymmetric Key Cryptosystem (cont.)

Example:

$n=47,\ g=3$



$(3^{10} \bmod 47)$

$59049 \bmod 47 = 17$

$17^8 \bmod 47$

$6975757441 \bmod 47 = 4$

Shared key

$(3^8 \bmod 47)$

$6561 \bmod 47 = 28$

$(28^{10} \bmod 47) = 4$

Shared key

Public/Asymmetric Key Cryptosystem (cont.)

Fast Experimental Modular Arithmetic

Purpose: computation of M^e mod n

Steps:

- Expand e in Binary
- Initially assume d = 1
- Until all e bits exhausted (loop)
  - d = (d × d) mod n
  - if (e bit == 1)
    - d = (d × m) mod n

Public/Asymmetric Key Cryptosystem (cont.)

Example 1: $(3^8) \bmod 47 = 1$

$3^8 \bmod 47$

$3 \to m$, $8 \to e$, $47 \to n$

Assume $d=1$

e	1	0	0	0
	1	9	34	28
	3	X	X	X

$(d \times d) \bmod n$ — 1×1

$(d \times m) \bmod n$ — 1×3

$(d \times d) \bmod n$ — 3×3

$(d \times d) \bmod n$ — 9×9

$(d \times d) \bmod n$ — 34×34

$\therefore 3^8 \bmod 47 = 28$

Public/Asymmetric Key Cryptosystem (cont.)

Example 2: $(28^{10}) \bmod 47 = 1$

$28^{10} \bmod 47$

$10 \rightarrow e$, $28 \rightarrow m$, $47 \rightarrow n$

Assume $d = 1$

e	1	0	1	0
	1	32	37	4
	28	×	2	×

$(d \times d) \bmod n$: 1×1

$(d \times m) \bmod n$: 1×28

$(d \times d) \bmod n$: 28×28

$(d \times d) \bmod n$: 32×32

$(d \times m) \bmod n$: 37×28

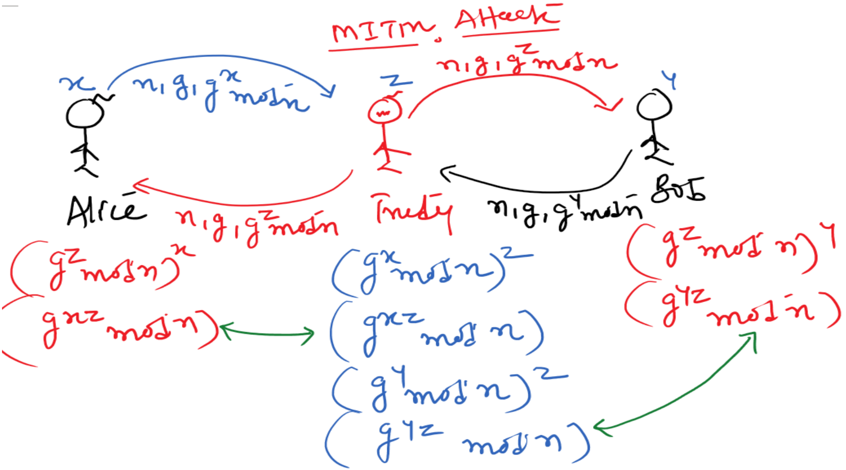
$(d \times d) \bmod n$: 2×2

$\therefore 28^{10} \bmod 47 = 4$

Public/Asymmetric Key Cryptosystem (cont.)

Attack on Diffie-Hellman Key Exchange Algorithm

Man-in-the-Middle Attack (MITM)



Reason: lack of authentication