2550 Intro to cybersecurity

Public key Crypto

abhi shelat

Recap

1. Perfect security, one-time pad
2. Symmetric encryption, computational security
   - AES (heuristic)
   - Blum-Micali: PRG

   $\Big\}$ short key, encrypt arbitrarily long messages

3. Asymmetric cryptography, aka public key cryptography
   - RSA

Revisit our model for Encryption

Symmetric key enc has 1 major drawback.

Bob

K_{ab}, K_{bc} K_{bd}
K_{be} K_{bf} K_{bg}

Carol

...

- each pair needs to manage a secret key.

Dave

...

$O(n^2)$ keys.

Alice

K_{ab}, K_{ac}, K_{ad},
K_{ae}, K_{af}, K_{ag}

Evan

...

George

Francis

Symmetric key enc has 1 major drawback.

$k_{ba}, k_{bc}, k_{bd}, k_{be}, k_{bf}, k_{bg}$

Bob

$k_{ca}, k_{cb}, k_{cd}, k_{ce}, k_{cf}, k_{cg}$

Carol

$k_{da}, k_{db}, k_{dc}, k_{de}, k_{df}, k_{dg}$

Dave

Alice

$k_{ab}, k_{ac}, k_{ad}, k_{ae}, k_{af}, k_{ag}$

$O(n^2)$ keys to manage!

Evan

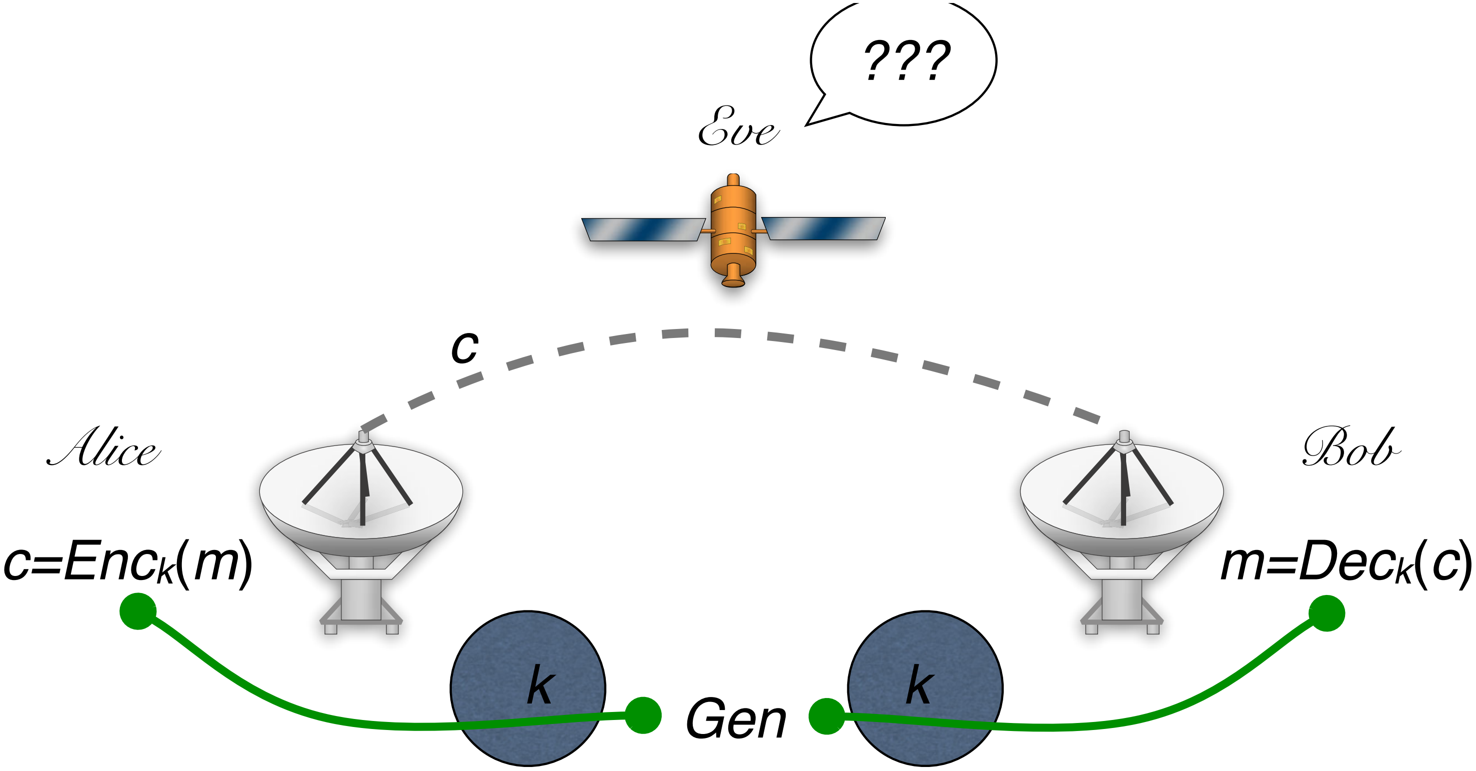
$k_{ea}, k_{eb}, k_{ec}, k_{ed}, k_{ef}, k_{eg}$

George

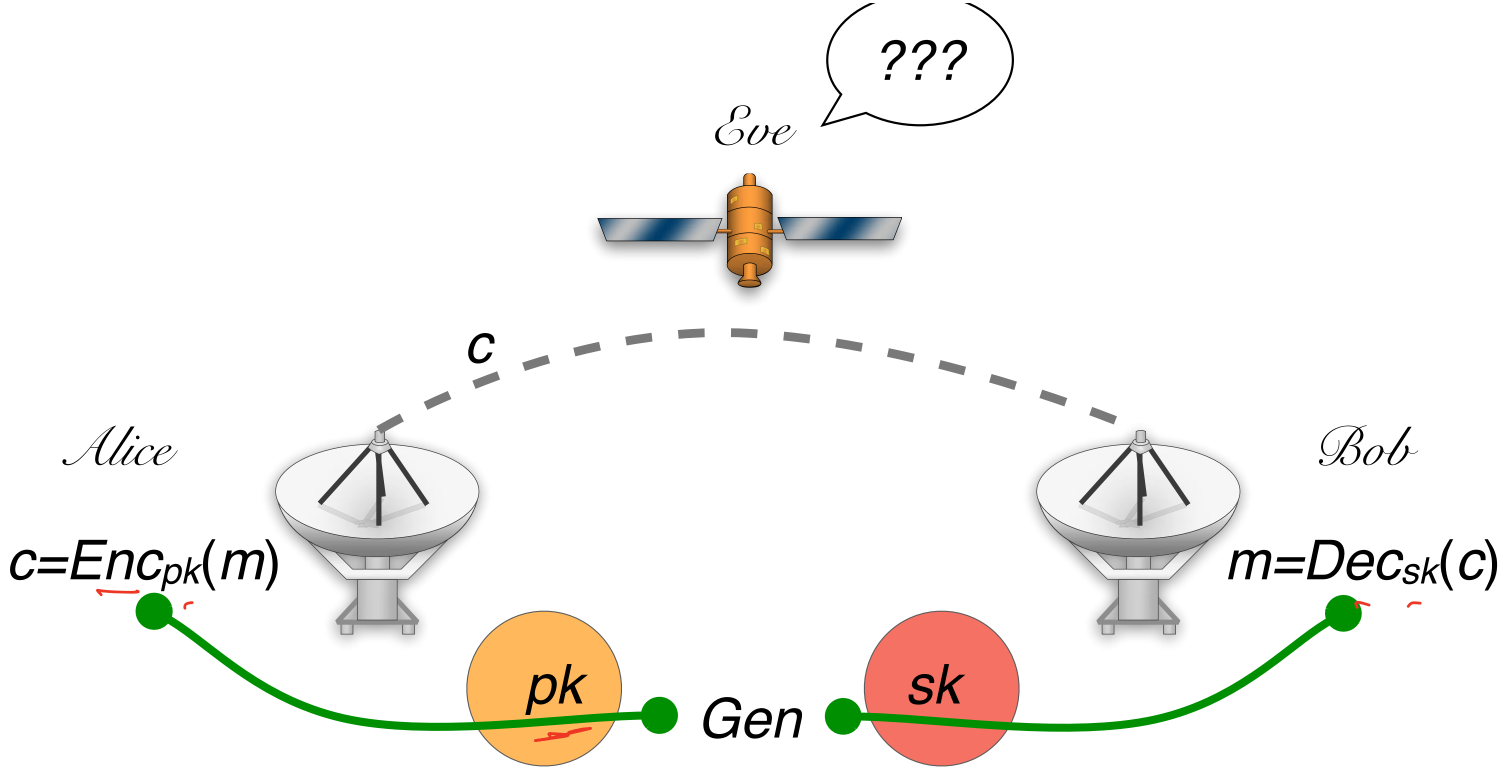
$k_{ga}, k_{gb}, k_{gc}, k_{gd}, k_{ge}, k_{gf}$

Francis

$k_{fa}, k_{fb}, k_{fc}, k_{fd}, k_{fe}, k_{fg}$



- this symmetric key model requires a careful setup process, k must remain a secret.



Pk can be used to encrypt.

sk can be used to decrypt.

Asymmetric cryptography

PKC key enc

sk_b *Bob*

sk_c *Carol*

sk_d *Dave*

Alice sk_a

$pk_a, pk_b, pk_c, pk_d, pk_e, pk_f, pk_g$

Are publicly posted

Evan sk_e

George sk_g

Francis sk_f

Public key encryption

Gen Enc Dec

3 algorithms

Gen (key generation)

$$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$$

security parameter

Enc (encryption)

$$c \leftarrow \mathsf{Enc}_{pk}(m) \text{ for } pk \in \mathcal{K}, m \in \mathcal{M}$$

Dec (decryption)

Public key encryption

Gen Enc Dec

3 algorithms

Gen (key generation)

$$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$$

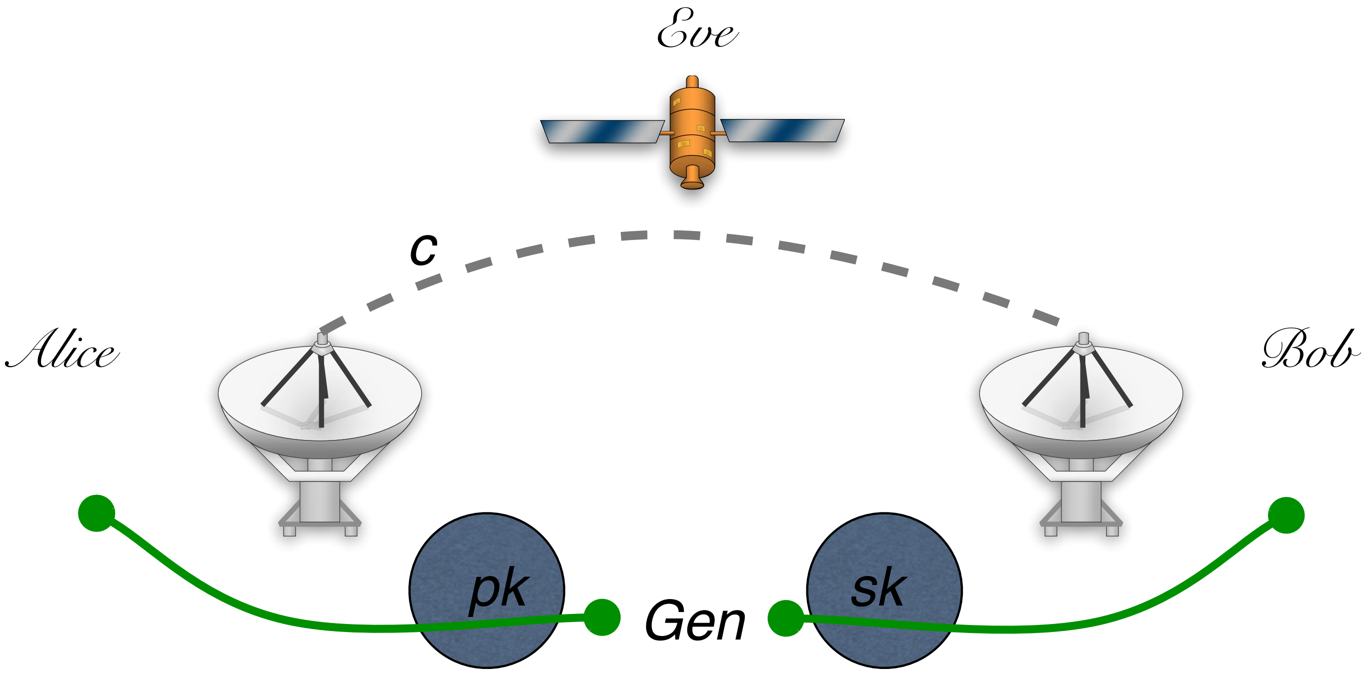
Enc (encryption)

$$c \leftarrow \mathsf{Enc}_{pk}(m) \text{ for } pk \in \mathcal{K}, m \in \mathcal{M}$$

Dec (decryption)

$$\forall m \in \mathcal{M}, (pk, sk) \leftarrow \mathsf{Gen}(1^n)$$

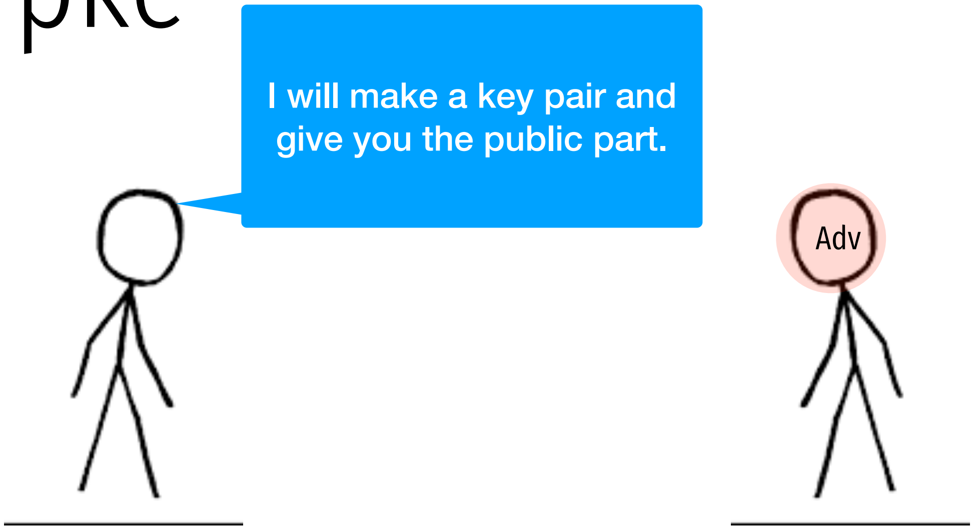
$$\Pr[\mathsf{Dec}_{sk}(\mathsf{Enc}_{pk}(m)) = m] = 1$$



"for any pair of messages m_1,m_2,
Eve cannot tell whether $c = Enc_{pk}(m_i)$."

IND-CPA security for pke

(weakest notion of security)

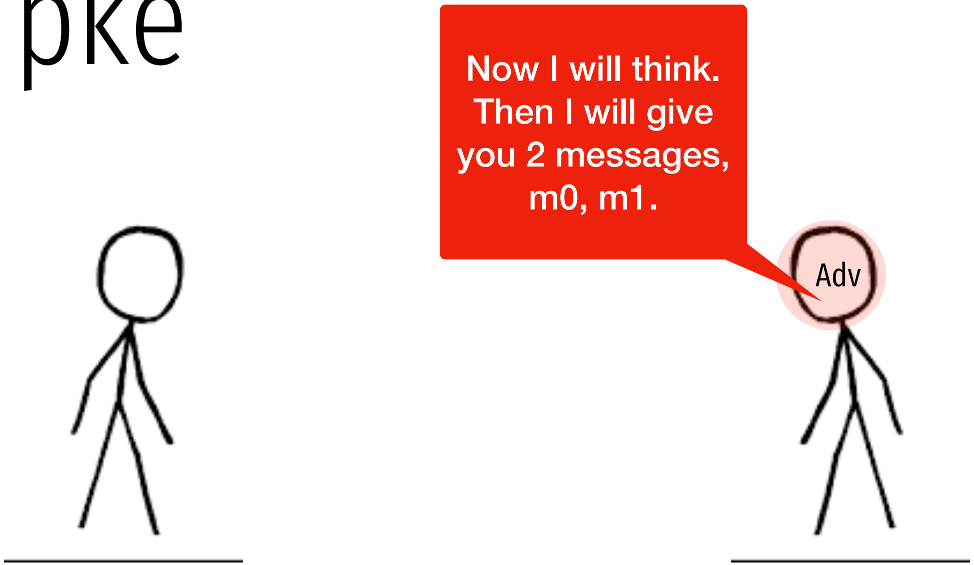


$pk, sk \leftarrow \mathsf{gen}(1^n)$

pk

IND-CPA security for pke

(weakest notion of security)



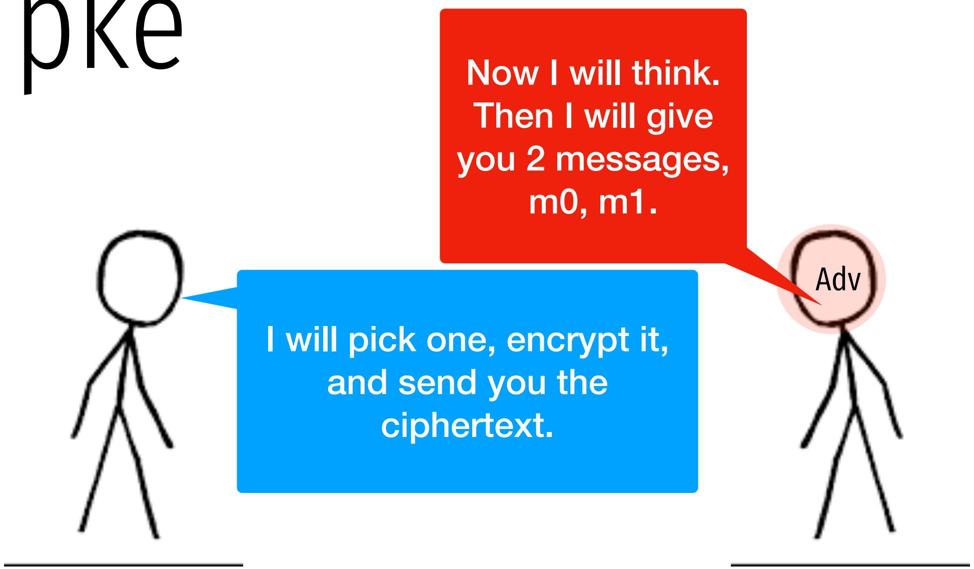
$pk, sk \leftarrow \mathsf{gen}(1^n)$

pk

$m_0, m_1 \leftarrow A(pk)$

IND-CPA security for pke

(weakest notion of security)



$pk, sk \leftarrow \mathsf{gen}(1^n)$

pk

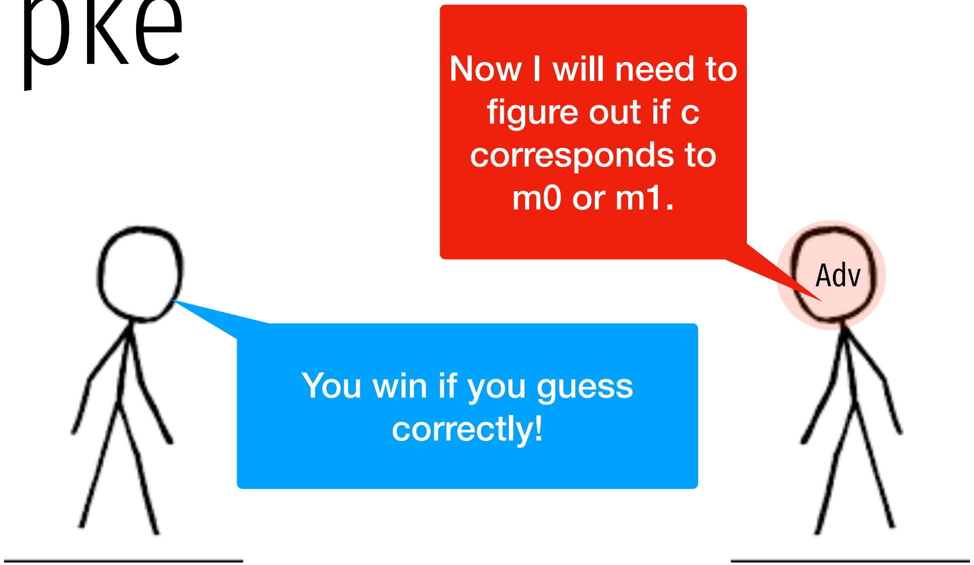
$m_0, m_1 \leftarrow A(pk)$

$b \leftarrow \{0,1\}$

$c \leftarrow \mathsf{enc}_{pk}(m_b)$

IND-CPA security for pke

(weakest notion of security)



$pk, sk \leftarrow \mathsf{gen}(1^n)$

pk

$m_0, m_1 \leftarrow A(pk)$

$b \leftarrow \{0,1\}$

$c \leftarrow \mathsf{enc}_{pk}(m_b)$

$b' \leftarrow A(pk, m_0, m_1, c)$

IND-CPA security for pke

(weakest notion of security)

$$pk, sk \leftarrow \mathsf{gen}(1^n)$$

$$m_0, m_1 \leftarrow A(pk)$$

$$b \leftarrow \{0,1\}$$

$$c \leftarrow \mathsf{enc}_{pk}(m_b)$$

$$b' \leftarrow A(pk, m_0, m_1, c)$$

$$\Pr[b = b'] \leq 1/2 + \epsilon(n)$$

How to build public key encryption?

Lets look @ the first such example,

RSA.

① "textbook" version (insecure)

② RSA-OAEP

Basic Number theory

① Modular Exponentiation (a, x, n)

② (Extended) Greatest Common Divisor (GCD)

③ Euler Totient function

$\Rightarrow$ RSA scheme (1978)

Modular Exponentiation

$(a, x, n) \to a^x \bmod n$

$7^{19} \bmod 31$

$$\underbrace{7 \cdot 7 \cdots 7}_{19 \text{ times}}$$

Modular Exponentiation

$(a, x, n) \to a^x \bmod n$

$7^{19} \bmod 31$

(mod 31)

1	2	4	8	16
7^1	7^2	7^4	7^8	7^{16}
		$18 \cdot 18 = 324$	$14 \cdot 14 = 196$	$10 \cdot 10 = 100$
$\boxed{7}$	$\boxed{18}$	$\boxed{14}$	$\boxed{10}$	$\boxed{7}$

$7^{19} = 7^{16} \cdot 7^2 \cdot 7^1$

$7 \cdot 18 \cdot 7 = \boxed{14}$

Modular Exponentiation $(a, x, n) \to a^x \bmod n$

$$7^{19} \bmod 31$$

Modular Exponentiation $(a, x, n) \to a^x \bmod n$

$$7^{19} \bmod 31$$

$$7^1 \qquad 7^2 \qquad 7^4 \qquad 7^8 \qquad 7^{16} \qquad \pmod{31}$$

Modular Exponentiation

$(a, x, n) \to a^x \bmod n$

$7^{19} \bmod 31$

7^1	7^2	7^4	7^8	7^{16}	(mod 31)
7	18	14	10	7	

Modular Exponentiation

$$(a, x, n) \to a^x \bmod n$$

Algorithm 2: ModularExponentiation(a, x, n)

Input: $a, x \in [1, n]$

```
r ← 1
while x > 0 do
    if x is odd then
        r ← r · a mod n
    x ← ⌊x/2⌋
    a ← a^2 mod n
Return r
```

Modular Exponentiation

$$(a, x, n) \to a^x \bmod n$$

$$a^x \bmod n = \prod_{i=0}^{\ell} x_i a^{2^i} \bmod n$$

Algorithm 2: ModularExponentiation(a, x, n)

Input: $a, x \in [1, n]$

$r \leftarrow 1$
while $x > 0$ **do**
  if x *is odd* **then**
    $r \leftarrow r \cdot a \bmod n$
  $x \leftarrow \lfloor x/2 \rfloor$
  $a \leftarrow a^2 \bmod n$
Return r

Greatest Common Divisor

$$\underbrace{\mathrm{GCD}}\overset{A > B}{(A, B)} = \underline{\mathrm{GCD}}(B, A \bmod B)$$

Greatest Common Divisor

```
GCD(A,B) = GCD(B, A mod B)
```

Greatest Common Divisor

```
GCD(6809,1641)
```

GCD(1641, 245)

GCD(245, 171)

GCD(171, 74)

GCD(74, 23)

GCD(23, 5)

GCD(5, 3)

GCD(3, 2)

GCD(2, 1)

$6809 = 4 \cdot 1641 + 245$

$1641 = 6 \cdot 245 + 171$

$245 = 1 \cdot 171 + 74$

$171 = 2 \cdot 74 + 23$

$74 = 3 \cdot 23 + 5$

$23 = 4 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = \boxed{1} \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

given (a,b), finds (x,y) s.t.
ax + by = gcd(a,b)

Algorithm 1: ExtendedEuclid(a, b)

Input: (a, b) s.t $a > b \geq 0$

Output: (x, y) s.t. $ax + by = \gcd(a, b)$

```
if a mod b = 0 then
    Return (0, 1)
else
    (x, y) ← ExtendedEuclid (b, a mod b)
    Return (y, x − y(⌊a/b⌋))
```

Greatest Common Divisor

GCD(6809,1641)		$6809 = 4 \cdot 1641 + 245$	$(-643, 2668)$
GCD(1641, 245)		$1641 = 6 \cdot 245 + 171$	$(96, -643$
GCD(245, 171)		$245 = 1 \cdot 171 + 74$	$(-67, 96)$
GCD(171, 74)		$171 = 2 \cdot 74 + 23$	$(29, -67)$
GCD(74, 23)	$(-9, 2 - -9 \cdot 3) = (-9, 29)$	$74 = 3 \cdot 23 + 5$	$(-9, 29)$
GCD(23, 5)	$(2, -1 - 2 \cdot 4) = (2, -9)$	$23 = 4 \cdot 5 + 3$	$(2, -9)$
GCD(5, 3)	$(-1, 1 - (-1 \cdot 1)) = (-1, 2)$	$5 = 1 \cdot 3 + 2$	$(-1, 2)$
GCD(3, 2)	(1, 0 - 1*1) $= (1, -1)$	$3 = \boxed{1} \cdot 2 + 1$	$(1, -1)$
GCD(2, 1)	(0,1)	$2 = 2 \cdot 1 + 0$	$(0, 1)$

Greatest Common Divisor

GCD(6809,1641)

$6809 x + 1641 \cdot y = 1$

GCD allows us to compute modular inverses.

$6809*(-643) + 1641*2668 = 1 = GCD(6809, 1641)$

$-4{,}378{,}187 + 4{,}378{,}188 = 1$

$\boxed{1641 \cdot 2688 = 1 + 643 \cdot 6809 \equiv 1 \mod 6809}$

$\Rightarrow$ 2688 is the "inverse" of 1641 mod 6809.

$\times 3 \quad \times \frac{1}{3}$

Euler totient

$\phi(n)$ = # of positive integers that are $\leq n$ and relatively prime to n.

$$\phi(n) = \left| \{ x \mid \gcd(x,n)=1 \text{ and } x \leq n \} \right|$$

Euler totient

$\phi(15) = 15 - 5 - 3 + 1 = 8 = (3-1)(5-1)$

1 2 $\cancel{3}$ 4 $\cancel{5}$ $\cancel{6}$ 7 8 $\cancel{9}$ $\cancel{10}$ 11 $\cancel{12}$ 13 14 $\cancel{15}$

"# of integers ≤ 15 that are relatively prime to 15"

Euler totient

$\phi(7) = 6$

prime $\quad \Phi(p) = p - 1$

product of 2 primes $\quad \Phi(n) = (p-1)(q-1)$

if $n = p \cdot q$

$\phi(77) = (7-1)(11-1)$

$= 6 \cdot 10$

$= 60$

Example of groups

$$(\mathbb{Z}_n, \star)$$

$\{a \mid \gcd(a,n) = 1\}$

multiplicative group, mod n

$$\mathbb{Z}_n^\star$$

Z*_15 = {1,2,4,7,8,11,13,14}

$$|\mathbb{Z}_n^\star| = \Phi(n)$$

" Z -star n "

Euler theorem

$$\forall a \in \mathbb{Z}_n^\star,\ a^{\Phi(n)} = 1 \bmod n$$

$\Phi(31) = 30$

$7^{30} \bmod 31 = 1 \bmod 31$

Examples

$\phi(31) = 30$

$7^{30} \bmod \underline{31} = 1$

1	2	4	8	16
7	18	14	10	$\underline{7}$

$7^{30} = 7^{16} \cdot 7^{8} \cdot 7^{4} \cdot 7^{2}$

$7 \cdot 10 \cdot 14 \cdot 18 = 17640 \equiv 1 \bmod 31$

Examples

$\phi(15) = (3-1)(5-1) = 8.$

$$2^8 \bmod 15 =$$

$256 \bmod 15 = 1$

b/c $15 \cdot 17 = 255$

Implications of Euler

$$a^{10\phi(N)} \bmod N = \left(a^{\phi(N)}\right)^{10} \bmod N = (1)^{10} \bmod N = 1 \bmod N$$

"heart of RSA"

$$a^{k\phi(N)+1} \bmod N = a \cdot a^{k\phi(N)} = a \cdot 1 \bmod N$$
$$= a$$

compute $$11^{30^{2021}} \bmod 23$$ Exercise.

(show your work)

$\phi(23) = 22$

$11^{30^{2021}} \bmod 23 = 11^{30^{2021} \bmod 22} \bmod 23 = 11^{8} \bmod 23$

$\boxed{\begin{aligned} &22 = 2 \cdot 11 \\ &\phi(22) = (2-1)(11-1) \\ &\quad = 1 \cdot 10 \\ &\quad = 10 \end{aligned}}$

$30^{2021} \bmod 22 = 30^{202 \cdot \underset{\phi(22)}{\underline{10}} + 1} \bmod 22$

$= \left(30^{\phi(22)}\right)^{202} \cdot 30 \bmod 22 = 30 = 8 \bmod 22$

“Textbook” RSA (insecure)

public   secret

Pick N = p*q where p,q are primes.

65537

Pick a random e that is relatively prime to N.

Gen

- Compute d s.t. $e \cdot d = 1 \bmod \phi(N)$
- Public key (N, e)
- Secret key (N, d)

“Textbook” RSA (insecure)

Pick N = p*q where p,q are primes.

Pick e,d such that $e \cdot d = 1 \bmod \phi(N)$

"Textbook" RSA (insecure)

Pick N = p*q where p,q are primes.

Pick e,d such that $e \cdot d = 1 \mod \phi(N)$

$\text{Enc}_{N,e}(m) = m^e \mod N$

$\text{Dec}_{N,d}(c) = c^d \mod N$

$$\text{Dec}(\text{Enc}(m)) = (m^e)^d = m^{e \cdot d} \mod N$$

$$= m^{1 + \underline{k \cdot \phi(n)}} \mod N$$

$$= \underline{m}$$

“Textbook” RSA (insecure)

Pick N = p*q where p,q are primes.

Pick e,d such that $e \cdot d = 1 \bmod \phi(N)$

$\text{Enc}_{N,e}(m) = m^e \mod N$

$\text{Dec}_{N,d}(c) = c^d \mod N$

$$(m^e)^d \bmod N = m^{e \cdot d} \bmod N$$

$$= m^{1 + k \cdot \phi(n)} \bmod N$$

$$= m \cdot m^{k \cdot \phi(n)} \bmod N = m \bmod N.$$

Example of Textbook RSA

$m=5$

$PK = (\underline{N=143}, \underline{e=7})$ $SK = (d=103)$

$p=11$ $q=13$

$7 \cdot 103 = 721 = 1 \bmod \phi(N)$

$\phi(N) = (11-1)(13-1)$

$= 120$

$enc_{pk}(5) = 5^7 \bmod 143$

$= 47$

$Dec_{sk}(\underline{47}) = 47^d = 47^{103} \bmod 143$

$= 5$

“Textbook” RSA (insecure)

Pick N = p*q where p,q are primes.

Pick e,d such that $e \cdot d = 1 \bmod \phi(N)$

$\text{Enc}_{N,e}(m) = m^e \mod N$

$\text{Dec}_{N,d}(c) = c^d \mod N$

Why is it insecure
against IND-CPA attack?

pkcs1.5

ENC$_{pk}$(m)

PICK r AS A RANDOM STRING WITH NO 0S

(TYPICALLY 8 BYTES)

$$c \leftarrow (0||2||r||0||m)^e \bmod N$$

"PADDING ORACLE" ATTACK AGAINST THIS SCHEME

RSA-OAEP+

GEN(1^n)

$f, f^{-1} \leftarrow$ TRAPDOOR OWP() → "textbook RSA"

ENC$_{pk}$(m)

$$r \leftarrow U_n$$
$$s \leftarrow R_1(r) \oplus m \,||\, R_2(r||m)$$
$$t \leftarrow R_3(s) \oplus r$$
$$c \leftarrow f(s||t)$$

$$R_1 : \{0,1\}^{k_0} \rightarrow \{0,1\}^n$$
$$R_2 : \{0,1\}^{n+k_0} \rightarrow \{0,1\}^{k_1}$$
$$R_3 : \{0,1\}^{n+k_1} \rightarrow \{0,1\}^{k_0}$$

DEC$_{sk}$(c)

$$(s = (s_1, s_2), t) \leftarrow f^{-1}(c)$$
$$r \leftarrow R_3(s) \oplus t$$
$$m \leftarrow R_1(r) \oplus s_1$$
$$R_2(r||m) \stackrel{?}{=} s_2 \qquad \text{OUTPUT } m \text{ ELSE FAIL}$$