

# 01204211 Discrete Mathematics

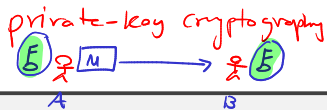
## Lecture 9b: RSA Review and Euler's Theorem

Jittat Fakcharoenphol

October 14, 2025

# RSA

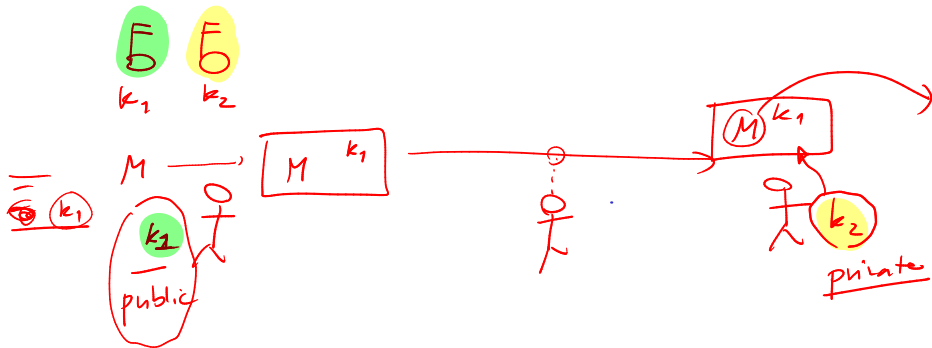
private-key cryptography



Alice (A) has a green circle with 'E' and a blue box with 'M'. An arrow points to Bob (B) who has a green circle with 'E'.

public-key cryptography

- ▶ Private key:  $(d, n)$ , Public key:  $(e, n)$
- ▶ Encryption  $E(m) = m^e \bmod n$ , Decryption:  $D(w) = w^d \bmod n$ .
- ▶ Goal: Select  $e, d, n$  such that  $D(E(m)) = m^{ed} \bmod n = m$ .



# RSA

65537

$$\underline{n} = \boxed{pq}$$

- ▶ Private key:  $(\underline{d}, \underline{n})$ , Public key:  $(\underline{e}, \underline{n})$
- ▶ Encryption  $E(\underline{m}) = \underline{m}^e \bmod \underline{n}$ , Decryption:  $D(\underline{w}) = \underline{w}^d \bmod \underline{n}$ .
- ▶ Goal: Select  $e, d, n$  such that  $D(E(m)) = m^{ed} \bmod n = m$ .

$$\underbrace{\left( \underbrace{m^e \bmod n}_{\text{encrypted msg}} \right)^d}_{\text{decn}} \bmod n = \underbrace{m^{ed}}_{\substack{\parallel \checkmark \\ \boxed{m} \bmod n}} \bmod n$$

## Recap: Congruences

### Definition (congruences)

For an integer  $m > 0$ , if integers  $a$  and  $b$  are such that

$$a \bmod m = b \bmod m,$$

we write

$$a \equiv b \pmod{m}.$$

We also have that

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad m \mid (a - b)$$

## Recap: Multiplicative inverse modulo $m$

### Definition

The multiplicative inverse modulo  $m$  of  $a$ , denoted by  $a^{-1}$ , is an integer such that

$$a \cdot a^{-1} \equiv 1 \pmod{m}.$$

### Theorem 1

*An integer  $a$  has a multiplicative inverse modulo  $m$  iff  $\gcd(a, m) = 1$ .*

## Theorem 2 (Fermat's Little Theorem)

*If  $p$  is prime and  $a$  is an integer such that  $\gcd(a, p) = 1$ ,*

$$a^{p-1} \equiv 1 \pmod{p}.$$

## Special case of Euler's theorem

### Theorem 3 (Euler's theorem)

*If  $p$  and  $q$  are different primes, for  $a$  such that  $\gcd(a, pq) = 1$ , we have*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

## Special case of Euler's theorem

### Theorem 4 (Euler's theorem)

*If  $p$  and  $q$  are different primes, for  $a$  such that  $\gcd(a, pq) = 1$ , we have*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

*Is this useful?*



## Special case of Euler's theorem

### Theorem 4 (Euler's theorem)

*If  $p$  and  $q$  are different primes, for  $a$  such that  $\gcd(a, pq) = 1$ , we have*

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

*Is this useful?* Yes! In the RSA algorithm.

# RSA

- ▶ Private key:  $(d, n)$ ,    Public key:  $(e, n)$
- ▶ Encryption  $E(m) = m^e \bmod n$ ,    Decryption:  $D(w) = w^d \bmod n$ .
- ▶ Goal: Select  $e, d, n$  such that  $D(E(m)) = m^{ed} \bmod n = m$ .

# RSA

- ▶ Private key:  $(d, n)$ , Public key:  $(e, n)$
- ▶ Encryption  $E(m) = m^e \bmod n$ , Decryption:  $D(w) = w^d \bmod n$ .
- ▶ Goal: Select  $e, d, n$  such that  $D(E(m)) = m^{ed} \bmod n = m$ .

- ▶ Pick two primes  $p$  and  $q$ . Let  $n = pq$ .
- ▶ Pick  $e$  (usually a small number)
- ▶ Pick  $d$  such that  $d = e^{-1} \pmod{(p-1)(q-1)}$  i.e.,  $ed \equiv 1 \pmod{(p-1)(q-1)}$ , or  $ed = k \cdot (p-1)(q-1) + 1$ , for some integer  $k$ .
- ▶ What is  $m^{ed} \bmod n$ ?

$$ed = \underline{e \cdot e^{-1}} \equiv \underline{1} \pmod{(p-1)(q-1)}$$

$$\underline{d} \equiv \boxed{e^{-1}} \pmod{(p-1)(q-1)} \quad ed = \underline{e \cdot e^{-1}} = 1 + \underbrace{k \cdot (p-1)(q-1)}_{\text{divisible by } k}$$

# RSA

- ▶ Private key:  $(d, n)$ , Public key:  $(e, n)$
- ▶ Encryption  $E(m) = m^e \bmod n$ , Decryption:  $D(w) = w^d \bmod n$ .
- ▶ Goal: Select  $e, d, n$  such that  $D(E(m)) = m^{ed} \bmod n = m$ .

- ▶ Pick two primes  $p$  and  $q$ . Let  $n = pq$ .
- ▶ Pick  $e$  (usually a small number)
- ▶ Pick  $d$  such that  $d = e^{-1} \pmod{(p-1)(q-1)}$ , i.e.,  $ed \equiv 1 \pmod{(p-1)(q-1)}$ , or  $ed = k \cdot (p-1)(q-1) + 1$ , for some integer  $k$ .
- ▶ What is  $\underline{m^{ed}} \bmod n$ ?

$$\begin{aligned} \underline{m^{ed}} &\equiv m^{k(p-1)(q-1)+1} \pmod{n} \\ &\equiv (m^{(p-1)(q-1)})^k \cdot m \pmod{n} \\ &\equiv 1^k \cdot m \pmod{n} \\ &\equiv m \pmod{n} \end{aligned}$$

Assume  
 $\gcd(m, pq) = 1$

$$\begin{aligned} m^{(p-1)(q-1)} &\bmod pq \\ &\equiv 1 \end{aligned}$$

# RSA

- ▶ Private key:  $(d, n)$ , Public key:  $(e, n)$
- ▶ Encryption  $E(m) = m^e \bmod n$ , Decryption:  $D(w) = w^d \bmod n$ .
- ▶ Goal: Select  $e, d, n$  such that  $D(E(m)) = m^{ed} \bmod n = m$ .

- ▶ Pick two primes  $p$  and  $q$ . Let  $n = pq$ .
- ▶ Pick  $e$  (usually a small number)
- ▶ Pick  $d$  such that  $d = e^{-1} \pmod{(p-1)(q-1)}$ , i.e.,  $ed \equiv 1 \pmod{(p-1)(q-1)}$ , or  $ed = k \cdot (p-1)(q-1) + 1$ , for some integer  $k$ .
- ▶ What is  $m^{ed} \bmod n$ ?

$$\begin{aligned} m^{ed} &\equiv m^{k(p-1)(q-1)+1} \pmod{n} \\ &\equiv (m^{(p-1)(q-1)})^k \cdot m \pmod{n} \\ &\equiv 1^k \cdot m \pmod{n} \\ &\equiv m \pmod{n} \end{aligned}$$

What is the requirement for  $m$ ?

# RSA

- ▶ Private key:  $(d, n)$ , Public key:  $(e, n)$
- ▶ Encryption  $E(m) = m^e \bmod n$ , Decryption:  $D(w) = w^d \bmod n$ .
- ▶ Goal: Select  $e, d, n$  such that  $D(E(m)) = m^{ed} \bmod n = m$ .

- ▶ Pick two primes  $p$  and  $q$ . Let  $n = pq$ .
- ▶ Pick  $e$  (usually a small number)
- ▶ Pick  $d$  such that  $d = e^{-1} \pmod{(p-1)(q-1)}$ , i.e.,  $ed \equiv 1 \pmod{(p-1)(q-1)}$ , or  $ed = k \cdot (p-1)(q-1) + 1$ , for some integer  $k$ .
- ▶ What is  $m^{ed} \bmod n$ ?

$$\begin{aligned} m^{ed} &\equiv m^{k(p-1)(q-1)+1} \pmod{n} \\ &\equiv (m^{(p-1)(q-1)})^k \cdot m \pmod{n} \\ &\equiv 1^k \cdot m \pmod{n} \\ &\equiv m \pmod{n} \end{aligned}$$

What is the requirement for  $m$ ?  $\gcd(m, n) = 1$ , otherwise you can use the message to factor  $n$ .