

ACOL 202

## Public-Key cryptography

### Key generation

Bob can generate his public key and private key } pair  
as follows:

→ chooses two large primes  $p, q$

→  $n = p \cdot q$

→ chooses  $(e \neq 1)$  such that  $e$  and  $(p-1)(q-1)$  are relatively prime

computes  $d = e^{-1} \bmod (p-1)(q-1)$

Publishes	$\langle e, n \rangle$	as his public key
<hr/> (Keep secret)	$\langle d, n \rangle$	as his private key

for some  $m \in \{0, \dots, n_{\text{Bob}}^{-1}\}$

Encryption

$$c = m^e \bmod n$$

Decryption

$$m = c^d \bmod n$$

## Exercise from last lecture

$$p = 11 \quad q = 13$$

$$pq = 11 \times 13 = 143$$

$$(p-1)(q-1) = 10 \times 12 = 120$$

Choose  $e (\neq 1)$  which is relatively prime to 120.

$$e = 7 \quad \left[ \begin{array}{l} 120 \text{ is divisible} \\ \text{by } 2, 3, 4, 5, 6 \end{array} \right]$$

$$d = \text{inverse}(7, 120)$$

## Extended - Euclid (7, 120)

$$x, y, r = \underline{\text{Extended-Euclid}(1, 7)}$$

$$(1, 0, 7)$$

$$(x, y, r)$$

$$\boxed{y - \left\lfloor \frac{m}{n} \right\rfloor x, x, r}$$

$$(0 - \left\lfloor \frac{120}{7} \right\rfloor 1, 1, 7)$$

$$= \underline{-17, 1, 7}$$

$$\text{inverse}(a, n) = \boxed{x} \bmod n$$

$$\frac{m \bmod n = 0}{\text{return } (1, 0, n)}$$

else

$$x, y, r$$

$$= \text{extended-Euclid}(m \bmod n, n)$$

then

$$\text{return } (y - \left\lfloor \frac{m}{n} \right\rfloor x, x, r)$$

$$\text{inverse } (7, 120) = -17 \bmod 120$$

$$= 103$$

Public Key  $\langle \underline{7}, 143 \rangle$

Private Key  $\langle 103, 143 \rangle$

The required ciphertext

$$= 95^7 \bmod 143$$

$$= 17 \quad \text{Ans.}$$

$$95 = 17^{103} \bmod 143$$

# Correctness of RSA

1  $\rightarrow \text{decrypt}(\text{encrypt}(m)) = m$

2  $\rightarrow$  Eve should not be able to figure out what  $m$  is, from the knowledge of  $c, \langle e, n \rangle$ .

lemma

let  $(m^e \bmod n)^d \bmod n = m'$

$$\boxed{m' \equiv_p m} \text{ and } \boxed{m' \equiv_q m}.$$

(Assume that this holds.)  $\rightarrow$  Proved later.

We know that  $m' \equiv_p m$  and  $m' \equiv_q m$

This implies that

$$m' \equiv_{pq} m \quad \left( \text{Tutorial 7, Q6 (d)} \right)$$

$$\underline{m'} = m \bmod pq$$

$$= m \bmod n \quad (n = pq)$$

$$= \underline{m} \quad (m < n)$$

## Proof of the lemma

$$\left[ \left( m^e \bmod n \right)^d \bmod n \right] \bmod p = m \bmod p$$

$$d = e^{-1} \bmod (p-1)(q-1)$$

$$\begin{aligned} ed &= ee^{-1} \bmod (p-1)(q-1) \\ &= 1 \bmod (p-1)(q-1) \end{aligned}$$

$$ed = k(p-1)(q-1) + 1$$



$$[(m^e \bmod n)^d \bmod n] \bmod p$$

$$= [m^{ed} \bmod n] \bmod p$$

Simplification  
↓ (2) from  
lect. 19

$$\left( \begin{aligned} &a^b \bmod k \\ &= \underline{(a \bmod k)^b \bmod k} \end{aligned} \right)$$

$$= [m^{ed} \bmod pq] \bmod p$$

$$= m^{ed} \bmod p$$

why? Tutorial 7,  
Q1

$$= m^{k(p-1)(q-1)+1} \bmod p$$

$$= [(m \bmod p) \cdot (m^{k(q-1)(p-1)} \bmod p)] \bmod p$$

$$= \left[ (m \bmod p) \cdot \left( m^{k(q-1)} \bmod p \right)^{p-1} \bmod p \right]$$

$a$

$$= \left[ (m \bmod p) \cdot (a^{p-1} \bmod p) \right] \bmod p$$

Care!

$$a \not\equiv_p 0$$

Then  $a^{p-1} \bmod p = \underline{1}$

$$\therefore \text{R.H.S} = \left[ (m \bmod p) \cdot \underline{1} \right] \bmod p$$

$$= \underline{\underline{m \bmod p}}$$

Case II

$$a \equiv_p 0$$

$$m^{k(q-1)} \bmod p = 0$$

$$p \mid m^{k(q-1)}$$

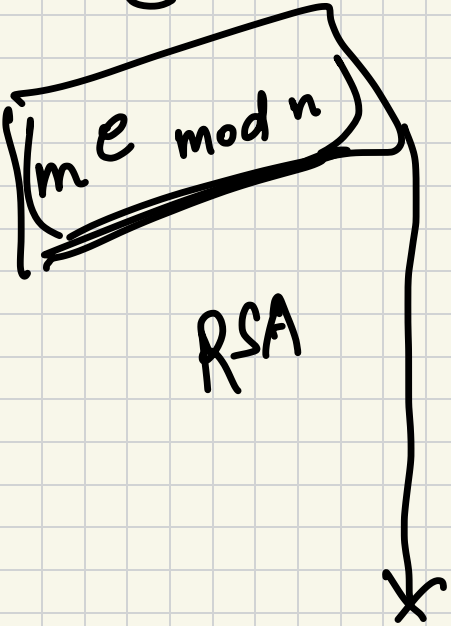
$$p \mid m$$

$$m \bmod p = 0$$

$$\begin{aligned} \therefore \text{RHS} &= 0 \\ &= \underline{\underline{m \bmod p}} \end{aligned}$$

The proof of  $m' \equiv m \pmod{n}$  is similar. (Exercise)

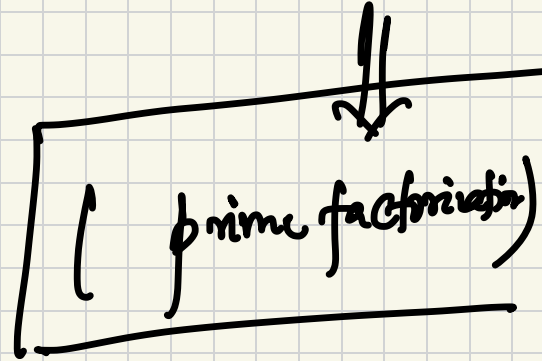
Can Eve figure out what  $m$  is?



$$\textcircled{c}, \langle e, n \rangle$$

$\uparrow$

$p, q$



$$\textcircled{e} \dots \textcircled{d}$$

$$\dots (p-1)(q-1)$$

$$e^{-1} \pmod{(p-1)(q-1)}$$

$$(c^d \pmod{n}) \equiv \underline{\underline{m}}$$

## Q16 (Tutorial 9)

↳ works for large primes  $p$   
and  $q$ .

### Class Poll

Should the tutorial sessions for  
Tutorial 9 be postponed to  
sometime next week?

Yes

No

~ 8 students

~ 15 students

**Decision:** We will have the tutorials as scheduled. )

Counting

Sum  
rule

$$|A \cup B| = |A| + |B|$$

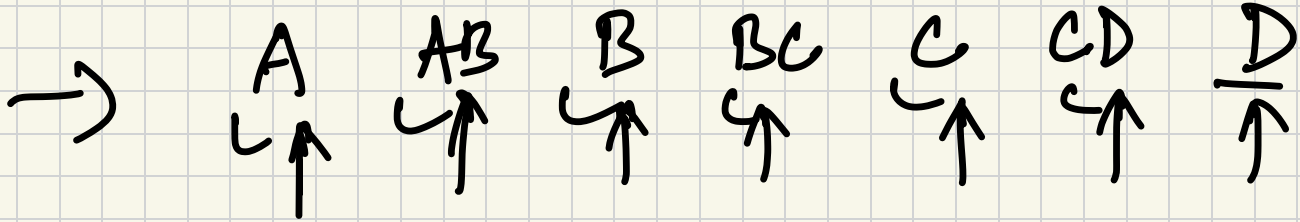
if

$$|A \cap B| = 0$$

$$(\text{or } A \cap B = \emptyset)$$

Counting disjoint unions

$$5 + 4 + 3 + 5 + 4 + 1 + 2 = 24$$



24  
30

students  
students

taking  
who are taking

ACOL 202

AMTL 101

How many students are taking

ACOL 202 or  
AMTL 101?

$$7,30 \leq 54$$

## Inclusion - Exclusion rule

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Example

Consider the set of odd numbers less than 10

$$O = \{1, 3, 5, 7, 9\}$$

the set of prime numbers less than 10

$$P = \{2, 3, 5, 7\}$$

Count the number of numbers that are odd or prime, and less than 10

$$\begin{aligned} &= |O| + |P| - |O \cap P| \\ &= 5 + 4 - |\{3, 5, 7\}| \\ &= 9 - 3 = 6 \\ &\quad \{1, 2, 3, 5, 7, 9\} \end{aligned}$$



What happens when there are three sets?

$$|A \cup B \cup C| = |A| + |B| + |C| -$$

$$\begin{matrix} x \in A, \\ x \in B \\ x \in C \end{matrix}$$

$$(A \cap B) - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

$$A = \{0, 1, 2, 3, 4\}$$

$$B = \{0, 2, 4, 6\}$$

$$C = \{2, 3, 6\}$$

$$A \cup B \cup C = \{0, 1, 2, 3, 4, 6\}$$

$$|A \cup B \cup C| = 5 + 4 + 3 - 3 - 2 - 2 + 1 = 6$$

## Exercise

How many integers between 1 and 1000 (inclusive of 1 and 1000) are evenly divisible by any of 2, 3, or 5?

Q. How many elements of  $\{0,1\}^8$  have precisely two 1's?  $\updownarrow$

1 2 3 4 5 6 7 8

(if the second one comes here)

(then the first one can come at any of these positions)

If the second 1 comes at position  $i$   
then the first 1 can  
come at any of the positions  
between 1 and  $(i-1)$ .

disjoint sets

The second 1 comes at position 1  
→ no. of such bitstrings  $(1-1) = 0$

The second 1 comes at position 2  
→ no. of such bitstrings  $(2-1) = 1$   
(11000000)

⋮  
and so on.

∴ No. of such bitstrings  $= \sum_{i=1}^8 i-1 = 0+1+2+\dots+7 = 28$ . Ans.

## Exercise

Find the number of  $k$ -length bitstrings containing exactly two 1's.