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

(Keep secret) $\langle d, n \rangle$ as his private key

for some $m \in \{0, \ldots, n_{Bob} - 1\}$

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

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

Exercise from last lecture

$$\boxed{p = 11 \qquad q = 13}$$

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

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

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

$e = 7$ [120 is divisible by 2, 3, 4, 5, 6]

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

Extended - Euclid (7, 120)

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

$(1, 0, 7)$

$(x \;\; y \;\; r)$

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

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

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

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

$\underline{m \bmod n = 0}$

return $(1, 0, n)$

else

x, y, r

= extended - Euclid (m mod n, n)

then

return

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

$$\text{inverse}(7, 120) = -17 \bmod 120$$
$$= 103$$

Public key $\langle 7, 143 \rangle$

Private key $\langle 103, 143 \rangle$

The required ciphertext

$$= 95^7 \bmod 143$$

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

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

Correctness of RSA

1 → decrypt (encrypt(m)) = m

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

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

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

(Assume that this holds.) → Proved later.

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

This implies that

$$m' \equiv_{pq} m$$ (Tutorial 7, Q6(d))

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

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

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

Proof of the lemma

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

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

$$ed = ee^{-1} \bmod (p-1)(q-1)$$

$$= 1 \bmod (p-1)(q-1)$$

$$\boxed{ed = K(p-1)(q-1) + 1}$$

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

Simplification (2) from lect. 19

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

$$\left(a^b \bmod k = (a \bmod k)^b \bmod k\right)$$

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

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

[why? Tutorial 7, Q2]

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

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

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

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

case I $\boxed{a \not\equiv_p 0}$ Then $a^{p-1} \bmod p = \underline{1}$

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

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

Made with Goodnotes

Case II

$$\boxed{a \equiv_p 0}$$

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

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

$$p \mid m$$

$$\boxed{m \bmod p = 0}$$

$$\therefore \quad RHS = 0$$

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

The proof of $m' \equiv_q m$ is similar. (Exercise)

Can Eve figure out what m is ?

$\boxed{m^e \bmod n}$

RSA

c, $\langle e, n \rangle$

$\uparrow$

p, q $\Leftarrow$ (prime factorization)

e $\cdots$ $(p-1)(q-1)$

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

$$(c^d \bmod \cancel{pq}\ n) = m$$

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 $|A \cap B| = 0$ (or $A \cap B = \phi$)

Counting disjoint unions

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

$\rightarrow$ A AB B BC C CD D

24 students taking ACOL 202
30 students who are taking AMTL 101

How many students are taking ACOL202 or AMTL101 ?

$\geq 30 \quad \leq 54$

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

$$= |O| + |P| \boxed{- |O \cap P|}$$

$$= 5 + 4 - |\{3, 5, 7\}|$$

$$= 9 - 3 = 6$$

$$\{1, 2, 3, 5, 7, 9\}$$

What happens when there are three sets?

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

$x \in A,$
$x \in B$
$x \in C$

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

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

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

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?

1 (if the second one comes here)

$\sqcup \quad \sqcup \quad \sqcup \quad \sqcup \quad \sqcup \quad \sqcup \quad \sqcup \quad \sqcup$

$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8$

(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 $= \sum_{i=1}^{8} i-1 = 0+1+2+\ldots+7$

$= 28$. Ans.

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