ACOL 202 — Lecture 19

Recap

Let $n \geq 2$ and $a \in \mathbb{Z}_n$.
Then a^{-1} exists iff a and n are relatively prime.

(Contradiction) a^{-1} exists $\Rightarrow$ a and n are relatively prime

$\Leftarrow$

$$\boxed{ax + ny = 1}$$

$$\boxed{ax \equiv_n 1}$$

$$\boxed{x \bmod n \rightarrow \text{inverse}}$$

$$\frac{aa^{-1}}{}$$

$$\underline{a(x \bmod n)} \bmod n$$

$$= a\left(\underline{x - \left\lfloor \frac{x}{n} \right\rfloor n}\right) \bmod n$$

$$= \left(ax - a\left\lfloor \frac{x}{n} \right\rfloor n\right) \bmod n$$

$$= ax \bmod n$$

$$= 1$$

$\Rightarrow$ if a^{-1} exists $\boxed{ax \equiv_n 1}$

$(ax + ny) = 1$

Corollary If p is prime, every non-zero $a \in \mathbb{Z}_p$ has a multiplicative inverse.

inverse (a, n) where $a \in \mathbb{Z}_n$, $n \geq 2$

x, y, d = Extended-Euclid

if $d = 1$ then return $x \bmod n$

else "there is no inverse"

Lemma

$\{1, 2, 3, \ldots, p-1\}$

and $\{1a, 2a, \ldots, (p-1)a\}$

are equivalent mod p where p is prime, $a \in \mathbb{Z}/p$, $a \neq 0$.

Consider the set $\{1a, 2a, \ldots, (p-1)a\}$.

1. All its elements are distinct.
2. None of its elements is zero.

2. $\underline{ia \bmod p} = 0 \Rightarrow p \mid ia$

$p \mid \underline{i}$ or $p \mid \underline{a}$

$\underbrace{\{1 .. p-1\}}$

$\mathbb{Z}_p$ and $\underline{\underline{a \neq 0}}$

1. $\underline{ia \equiv_p ja}$

$iaa^{-1} \equiv_p jaa^{-1}$

$\underline{i \equiv_p j}$

Fermat's Little Theorem

p prime , $a \in \mathbb{Z}_p$, $a \neq 0$

$$a^{p-1} \equiv_p 1$$

$$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv_p 1a \cdot 2a \cdot \ldots (p-1)a$$

$$1 \cdot 2 \cdot 3 \cdots (p-1) \cdot 1^{-1} 2^{-1} 3^{-1} \cdots (p-1)^{-1}$$

$$\equiv_p 1a\, 2a\, 3a \cdots (p-1)a \; 1^{-1} 2^{-1} \cdots (p-1)^{-1}$$

$$1 \equiv_p a^{p-1}$$

Does this give us a primality test?

If $\left(a^{n-1} \equiv_n 1 \text{ for every } a \in \mathbb{Z}_n \text{ where } \gcd(a,n) = 1\right)$, then does this mean that $\underline{n \text{ is prime}}$?

<u>Answer</u> No. $\left[a^{560} \equiv_{\underline{\underline{561}}} 1 \text{ for every } a \in \{1, 2, \ldots, 560\} \text{ where } \gcd(a, 561) = 1 \right.$

|| But 561 is not a prime.

Cryptography

Eve (eavesdropper)

Alice $\xrightarrow{\text{secret message (m) (plaintext)}}$ Bob

encrypt(m)

c ← (cyphertext)

send c

decrypt(c) = m

Necessary properties

→ Bob should be able to decrypt (c) to get m.

→ Eve should not be able to decrypt(c) to get m.

A simple idea

Suppose that Alice and Bob decide the length of the message they would like to communicate $\to n$

Suppose they also agree on a secret bitstring $K \in \{0,1\}^n$

(where each bitstring is chosen independently and uniformly so that each one of the 2^n bitstrings have an equal chance of being chosen as K).

Made with Goodnotes

Alice . encrypt m by doing a bitwise XOR of m and k to obtain c

a	b	$a \oplus b$	$(a \oplus b) \oplus b$
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

Bob decrypt m by doing a bitwise XOR of c and k

$n = 8$

$k = 10111000$

$\boxed{m = 01101110}$

$\boxed{c = 11010110}$

01101110

decrypted c is same as m.

Eve cannot figure out m by knowing c.

Any m can lead to the same c, for an appropriate choice of K.

$c = 11010110$

$m = 10101011$

$K = 0111$

Decryption works

Encryption works

Issues → How do they share the secret key K ?

→ Reusing the same secret key can make the protocol insecure.

Public - Key Cryptography

Every participant has a public key and a private key (is related to the public key).

Alice $\xrightarrow{m}$ Bob

Alice encrypts m using Bob's public key (to produce c)

$\xrightarrow{\text{sends } c}$

Bob decrypts c using his private key to get m.

Eve cannot decrypt c (because the private key is needed for decryption).

Alice $\rightarrow$ Bob
(public key, private key)

Here is what Bob does :

1. Bob chooses two large prime nos. p, q.

2. $n_{Bob} = p \cdot q$

3. Bob chooses $e \, (\neq 1)$ such that e and $(p-1)\cdot(q-1)$ are relatively prime.

4. Bob computes $d = e^{-1}$ modulo $(p-1)(q-1)$

5. Bob publishes $\langle e, n \rangle$ as his public key and keeps $\langle d, n \rangle$ as his private key.

Encryption $\quad m \in \{0, \ldots, n_{Bob}-1\}$

$$\boxed{c} = m^{e_{Bob}} \bmod n_{Bob}$$

Decryption $\quad \boxed{m} = c^{d_{Bob}} \bmod n_{Bob}$

Example $\quad$ Suppose Bob picks $p = 13$, $q = 17$

$n = 13 \times 17 = 221$

$e (\neq 1)$ which is relatively prime to $12 \times 16 = 192$

$e = 5$

$d = \text{inverse}(5, 192)$

$$\boxed{\begin{aligned} &\text{Extended-Euclid}(5, 192) \\ &\qquad = 77, -2, 1 \end{aligned}}$$

$= \underline{77}$

Public key

$\langle 5, 221 \rangle$

Private key

$\langle 77, 221 \rangle$

Suppose Alice wants to send $m = 202$ to Bob.

$$c = 202^5 \mod 221$$

$$\boxed{c = 206}$$

Alice sends to Bob.

$$m = \underbrace{206^{77} \mod 221}$$

This should evaluate to 202.

Let us see if it really does.

We will use the following facts for the simplification.

1. $ab \mod K = [(a \mod K).(b \mod K)] \mod K$
2. $a^b \mod K = [(a \mod K)^b] \mod K$

$206^{77} \bmod 221$

$= 206\,(206^{76}) \bmod 221$

$= [(206 \bmod 221) * (206^{76} \bmod 221)] \bmod 221$ (using 1)

$= [206\,(206^2 \bmod 221)^{38} \bmod 221] \bmod 221$ (using 2)

$= [206\,(4^{38} \bmod 221)] \bmod 221$ $(206^2 \bmod 221 = 4)$

$= [206\,(16^{19} \bmod 221)] \bmod 221$ $(4^{38} = (4^2)^{19} = 16^{19})$

$= [206\,([(16 \bmod 221)(16^{18} \bmod 221)] \bmod 221)] \bmod 221$ (using 1)

$= [206\,(16\,(256 \bmod 221)^9 \bmod 221) \bmod 221] \bmod 221$

$= [206\,(16\,(35^9 \bmod 221) \bmod 221] \bmod 221$

$= [206\,(16\,(35 \cdot (35^8 \bmod 221) \bmod 221) \bmod 221] \bmod 221$

$= [206\,(16\,(35\,[(35^2 \bmod 221)^4 \bmod 221] \bmod 221) \bmod 221] \bmod 221$

$$= [206\ (16\ [35\ (120^4 \bmod 221) \bmod 221]\ \bmod 221)] \bmod 221$$

$$= [206\ (16\ [35\ (120) \bmod 221]\ \bmod 221)]\ \bmod 221$$

$$= [206\ (16\ [\ 1\ ]\ \bmod 221)]\ \bmod 221$$

$$= [206\ (\ 16\ )]\ \bmod 221$$

$$= 3296 \bmod 221 = 202.$$

Exercise Suppose $p = 11$, $q = 13$ are the primes chosen by Bob. Further, suppose that he chooses the smallest e bigger than 1 that satisfies the condition necessary for choice of e (that e is relatively prime to $(p-1)(q-1)$), and publishes his public key as $\langle e, n \rangle$ where n is pq.
What ciphertext would you send to Bob if you wanted to send him the plaintext message 95?