Introduction to Public-Key Cryptography

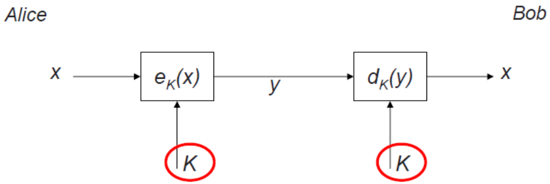
CUI TINGTING

School of Cypberspace, Hangzhou Dianzi University

November 5, 2023

Contents

Symmetric Cryptography revisited



Two properties of symmetric (secret-key) crypto-systems:

- The same secret key K is used for encryption and decryption
- Encryption and Decryption are very similar (or even identical) functions

Symmetric Cryptography: Shortcomings

1. Key Distribution Problem: the secret key must be transported securely.
2. Number of Keys: n users in the network require $\frac{n(n-1)}{2}$ key pairs, each user stores $n-1$ keys without KDC.
3. No Protection Against Cheating: Alice or Bob can cheat each other, because they have identical keys.

Public-key Cryptography: Motivation

1. Key Distribution Problem: No need secure channel
2. Number of Keys: reduce key pairs , each user only store one key.
3. No Protection Against Cheating: nonrepudiation.

Basic protocol for public-key encryption

Alice		**Bob**
	$\xleftarrow{\quad k_{pub} \quad}$	$(k_{pub}, k_{pr}) = k$
$y = e_{k_{pub}}(x)$		
	$\xrightarrow{\quad y \quad}$	
		$x = d_{k_{pr}}(y)$

- public key k_{pub} & private key k_{pr};
- secure depend on: easy to compute k_{pub} from k_{pr}, but hard to comput k_{pr} from k_{pub}
- Good one-way function is needed.

Public-key Cryptography: Applications

1. Encryption: such as RSA, ElGamal, ECC etc. but too slow
2. Digital Signature: RSA, DSA, ECDSA etc. perfectly no cheating
3. Key-exchange: such as DHKE, ECDHKE etc. to solve key distribution problem
4. Important Public-Key Algorithms:
   - Integer-Factorization Schemes
   - Discrete Logarithm Schemes
   - Elliptic Curve (EC) Schemes

Some Notation

- $\mathbb{Z}$: the set of integers: $\{\cdots$ -3, -2, -1, 0, 1, 2, 3, $\cdots\}$
- $a \in A$: this means that a is an element of a set A
  - 2$\in \mathbb{Z}$: 2 is element of set of integers $\mathbb{Z}$, or just 2 is an integer
  - $\frac{4}{5} \in \mathbb{Q}$: $\frac{4}{5}$ is a rational number
- $\forall$: *for all* or *for every*
  - $\forall a \in \mathbb{Z} : a + 1 \in \mathbb{Z}$: for every integer a, a+1 is also an integer
- $\exists$: *there exists*
  - $\forall a \in \mathbb{Z}, \exists b \in \mathbb{Z} : a + b = 0$ means: for every integer there exists an integer that when added to that integer gives 0
- $C = A \setminus B$ (set minus): C contains elements of A that are not in B
- $\#A$: the cardinality of a set, the number of elements it has
  - $\#$ {January, February, $\cdots$, December} $= 12$

Residue classes modulo n

- In cryptography we want to work with finite sets
- One such finite set is the set of integers $\{0, 1, \cdots, n-1\}$
- We can do arithmetic on them, *modulo* n
- The underlying mathematics is the theory of residue classes

One writes $\mathbb{Z}/n\mathbb{Z}$ for the set of residue classes modulo n:

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$$

with $\overline{m} = \{k \mid k \equiv m \pmod{n}\}$
$\#(\mathbb{Z}/n\mathbb{Z}) = n$, We represent $\overline{m}$ of $\mathbb{Z}/n\mathbb{Z}$ by its member in the interval $[0, n-1]$

Modular addition

- $\mathbb{Z}/n\mathbb{Z}$ represented by positive integers smaller than n including zero
- Consider addition modulo n as an operation:
  (1) $c \leftarrow a + b$
  (2) if $c \geq n$, $c \leftarrow c - n$
- Notation: $a + b \bmod n$ or just $a + b$
- Interesting properties
  - the result of $a + b \bmod n$ is in $\mathbb{Z}/n\mathbb{Z}$
  - $a + b \bmod n = b + a \bmod n$: the order does not matter
  - $(a + b \bmod n) + c \bmod n = (a + (b + c) \bmod n) \bmod n$: the order of execution does not matter
  - $a + 0 \bmod n = a$: adding 0 has no effect
  - $a + b \bmod n = 0$ if $b = n - a$. So for every a there is a value b so that their sum is 0

Modular multiplication

- Consider now multiplication modulo n as an operation
  (1) $c \leftarrow a \cdot b$
  (2) do the result modulo n: $c \leftarrow c \bmod n$
- Notation: $a \cdot b \bmod n$ or $a \times b$
- Interesting properties:
  - the result of $a \cdot b \bmod n$ is in $\mathbb{Z}/n\mathbb{Z}$
  - $a \cdot b \bmod n = b \cdot a \bmod n$: the order does not matter
  - $((a \cdot b) \bmod n \cdot c) \bmod n = (a \cdot (b \cdot c) \bmod n) \bmod n$: the order of execution does not matter
  - $a \cdot 1 \bmod n = a$: multiplying by 1 has no effect
  - $a \cdot 0 \bmod n = 0$: multiplying by 0 always gives 0
  - $a \cdot b \bmod n = 1$ if, $\cdots$ well, hmm, let's keep that for later

Group

A group $< G, \circ >$ has the following properties:

1. closed. That is, for all $a, b \in G$, it holds that $a \circ b = c \in G$.
2. associative. That is, $a \circ (b \circ c) = (a \circ b) \circ c$.
3. neutral element (or identity element): $a \circ 1 = 1 \circ a = a$ for all $a \in G$.
4. inverse of a: For each $a \in G$ there exists an element $a^{-1} \in G$, such that $a \circ a^{-1} = a^{-1} \circ a = 1$.

A group G is abelian (or commutative) if, furthermore, $a \circ b = b \circ a$ for all $a, b \in G$.

Terminology: Group order

Order of a finite group $< G, \circ >$, denoted $\#G$, is a number of elements in G

Examples of groups and non-groups

- Groups
  - $<\mathbb{Z},+>, <\mathbb{Q},+>, <\mathbb{R},+>, <\mathbb{C},+>$
  - $<\mathbb{Q}\setminus\{0\},\cdot>, <\mathbb{R}\setminus\{0\},\cdot>, <\mathbb{C}\setminus\{0\},\cdot>$
- Non-groups
  - $<\mathbb{N},+>$: no neutral element, no inverses
  - $<\mathbb{Z}\setminus\{0\},\cdot>$: elements without inverse
  - $<\mathbb{Q},\cdot>$: zero has no inverse

Addition modulo n is a group

- Notation: $<\mathbb{Z}/n\mathbb{Z}, +>$
  - the set $<\mathbb{Z}/n\mathbb{Z}, +>$ with operation modular addition $+$
  - if operation is clear from the context, denoted as $\mathbb{Z}/n\mathbb{Z}$
- satisfies all required group properties and is abelian
- $<\mathbb{Z}/n\mathbb{Z}, +>$ is a group of order n

Multiplication modulo n is a group?

- Notation: $< \mathbb{Z}/n\mathbb{Z}, \times >$
- 0 has no inverse, so $< \mathbb{Z}/n\mathbb{Z}, \times >$ is not a group
- maybe removing 0 may fix the problem?

Multiplication table, e.g., for $n = 7$:

$\mathbb{Z}/7\mathbb{Z}$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Cyclic behaviour in finite groups

- Let $a \in A$ with $< A, \star >$ a group
- Consider the sequence:
  - $i = 1 : a$
  - $i = 2 : a \star a$
  - $\dots$
  - $i = n : [n]a$ (additive) or a^n (multiplicative)
- In a finite group $< A, \star >$:
  - $\forall a \in A$ this sequence is periodic
  - period of this sequence: order of a , denoted ord(a)

Terminology: Order of a group element

The order of a group element a, denoted ord$< a >$, is the smallest integer $k > 0$ such that $a^k = 1$ (multiplicative) or $k[a] = 0$ (additive)

Cyclic groups and generators

- Let $g \in < A, \star >$
- Consider the set $[0]g, [1]g, [2]g, \ldots$
- This is a group, called a cyclic group, denoted: $\langle g \rangle$
  - Composition law: $[i]g + [j]g = [i + j \mod \text{ord}< g >]g$
  - Neutral element $[0]g$
  - Inverse of $[i]g$: $[\text{ord} < g > -i]g$
- g is called the generator of this cyclic group
- Example of cyclic group $< \mathbb{Z}/n\mathbb{Z}, + >$
  - generator: $g = 1$
  - $[i]g = i$

Subgroups

A subset B of A that is also a group (under the same operation) is called a subgroup of A.

- $(B, \star)$ is a subgroup of $(A, \star)$ if
  - B is a subset of A
  - $(B, \star)$ is a group

Lagrange's Theorem

If $(B, \star)$ is a subgroup of $(A, \star)$: $\#B$ divides $\#A$

Case of cyclic Subgroup: $\forall a \in A : \langle a \rangle$ is a subgroup of $(A, \star)$

Corollary (for order of elements)

For any element $a \in A : \mathrm{ord}(a)$ divedes $\#A$

Example of orders: $< \mathbb{Z}/21\mathbb{Z}, + >$

- Order of $\mathbb{Z}/21\mathbb{Z}$: 21
- Order of 0: 1
- Order of 1: 21
- Order of 2: 21
- Order of 3: 7
- ...

Find the smallest i *such that* $i \cdot x$ *is a multiple of* n

Fact: order of an element in $< \mathbb{Z}/n\mathbb{Z}, + >$

ord $(x) = n/gcd(n, x)$ with gcd(n, x) : the greatest common divisor of x and n

Prime numbers and factorization

- A number is prime if it is divisible only by 1 and by itself
- Each number can be written in a unique way as product of primes (possibly multiple times), as in:
  $$30 = 2 \cdot 3 \cdot 5 \qquad 100 = 2^2 \cdot 5^5 \qquad 12345 = 3 \cdot 5 \cdot 823$$
- Finding the prime number factorization is a computationally hard problem
  - Easy for $143 = 11 \cdot 13$ but already hard for $2021 = 43 \cdot 47$
  - Recently, factoring a 250-digit (829 bits) number $n = p \cdot q$ took 2700 Intel Xeon Gold 6130 CPU core-years (2.1GHz)
- One can base public-key cryptosystem on the hardness of factoring

Greatest common divisor

- Definition:
  $gcd(n, m)$: greatest integer k that divides both n and m
- Examples:
  $gcd(20, 15) = 5$ $\quad gcd(78, 12) = 6$ $\quad gcd(15, 8) = 1$
- Properties:
  - $gcd(n, m) = gcd(m, n)$
  - $gcd(n, m) = gcd(n, -m)$
  - $gcd(n, 0) = n$

Terminology: relatively prime (or coprime)

If $gcd(n, m) = 1$, one calls n, m relatively prime or coprime

Euclidean Algorithm

Property (assume $n > m > 0$):

- $gcd(n,m) = gcd(m, n \mod m)$

This can be applied iteratively until one of arguments is 0

$$\begin{aligned} \text{gcd}(171{,}111) &= \text{gcd}(111{,}171 \text{ mod } 111) = \text{gcd}(111{,}60) \\ &= \text{gcd}(60{,}111 \text{ mod } 60) = \text{gcd}(60{,}51) \\ &= \text{gcd}(51{,}60 \text{ mod } 51) = \text{gcd}(51{,}9) \\ &= \text{gcd}((9{,}51 \text{ mod } 9) = \text{gcd}(9{,}6) \\ &= \text{gcd}((6{,}9 \text{ mod } 6) = \text{gcd}(6{,}3) \\ &= \text{gcd}((3{,}6 \text{ mod } 3) = \text{gcd}(3{,}0){=}3 \end{aligned}$$

Variant allowing negative numbers :

$$\begin{aligned} \text{gcd}(171{,}111) &= \text{gcd}(111{,}171 \text{ mod } 111) = \text{gcd}(111{,}\text{-}51) \\ &= \text{gcd}(51{,}111 \text{ mod } 51) = \text{gcd}(51{,}9) \\ &= \text{gcd}(9{,}51 \text{ mod } 9) = \text{gcd}(9{,}\text{-}3) \\ &= \text{gcd}((3{,}9 \text{ mod } 3) = \text{gcd}(3{,}0){=}3 \end{aligned}$$

Extended Euclidean Algorithm

The extended Euclidean algorithm returns a pair $x, y \in \mathbb{Z}$ with $n \cdot x + m \cdot y = gcd(n, m)$

Our earlier example:

$$\begin{aligned} -51 &= 171 - 2 \cdot 111 \\ 9 &= 111 + 2 \cdot (-51) \\ 3 &= (-51) + 6 \cdot 9 \\ 0 &= (-9) + 3 \cdot 3 \end{aligned}$$

And now backward substitution:

$$\begin{aligned} 3 &= (-51) + 6 \cdot 9 \\ 3 &= (-51) + 6 \cdot (111 + 2 \cdot (-51)) \\ 3 &= (-51) + 6 \cdot 111 + 12 \cdot (-51) \\ 3 &= 6 \cdot 111 + 13 \cdot (-51) \\ 3 &= 6 \cdot 111 + 13 \cdot (171 - 2 \cdot 111) \\ 3 &= 6 \cdot 111 + 13 \cdot 171 - 26 \cdot 111 \\ 3 &= 13 \cdot 171 - 20 \cdot 111 \end{aligned}$$

Invertibility modulo n

Invertibility criterion

m has multiplicative inverse modulo n (i.e., in $\mathbb{Z}/n\mathbb{Z}$) iff gcd$(m,n) = 1$

Note: you can compute inverse with extended Euclidean algorithm!

Corollary

For p a prime, every non-zero $m \in \mathbb{Z}/p\mathbb{Z}$ has an inverse.

Euler's Phi Function

how many numbers in $\mathbb{Z}_m$ are relatively prime to m?

Euler's Phi Function

The number of integers in $\mathbb{Z}_m$ relatively prime to m is denoted by $\Phi(m)$.

Example 1

Let $m = 6$. The associated set is $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. then $\Phi(6) =?$

Example 2

Let $m = 5$. The associated set is $\mathbb{Z}_5 = \{0, 1, 2, 3, 4, \}$. then $\Phi(5) =?$

Euler's Phi Function

Theorem 3

Let m have the following canonical factorization

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_n^{e_n},$$

where the p_i are distinct prime numbers and e_i are positive integers, then

$$\Phi(m) = \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i - 1})$$

Example 4

Let m $= 240$, so $\Phi(m) =?$

Fermat‘s Little Theorem

Theorem 5 (Fermat‘s Little Theorem)

Let a be an integer and p be a prime, then:

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

Especially, in finite fields $GF(p)$, The theorem can be stated in the form:

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

furthermore,

$$a^{-1} \equiv a^{p-2} \pmod{p}.$$

Euler's Theorem

Theorem 6 (Euler)

Let a and m be integers with $gcd(a, m) = 1$, then:

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Example

Calculate $2^{2019} \pmod{107}$

$(\mathbb{Z}/p\mathbb{Z})^*$ with prime p

Multiplicative prime groups

$(\mathbb{Z}/p\mathbb{Z})^*$ is a circle group of order $p-1$

Alternative way of seeing it:

- Find a generator $g \in (\mathbb{Z}/p\mathbb{Z})^*$
- Write elements as power of generator: g^i
- Multiplication: find c such that $g^c = g^a \times g^b$
- Clearly: $g^a \times g^b = g^{a+b} = g^{a+b \ mod \ p-1}$
- So $c = a + b \ mod \ p - 1$

$(\mathbb{Z}/p\mathbb{Z})^*$ is just $\mathbb{Z}/(p-1)\mathbb{Z}$ in disguise!
These groups are isomorphic, such as $< (\mathbb{Z}/23\mathbb{Z})^*, \times >$ and $< (\mathbb{Z}/22\mathbb{Z}), + >$

Properties of multiplication in $\langle G \rangle$

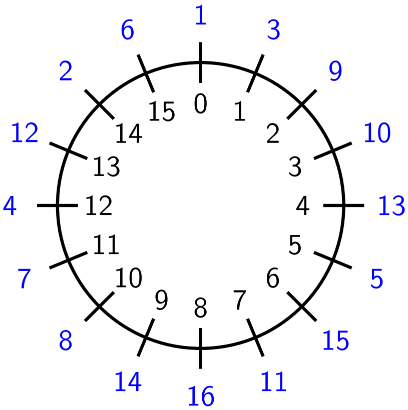
- If $A, B \in \langle G \rangle$ then $A \times B \in \langle G \rangle$
- If the order of G modulo p is q, then
  - for any integer $x : G^x = G^{x \ mod \ q}$
  - $G^q = G^0 = 1$
  - $A \times B = G^a \times G^b = G^{a+b} = G^{a+b \ mod \ q}$

Correspondence between $\langle G \rangle$ and $\mathbb{Z}/q\mathbb{Z}$

For every $A \in \langle G \rangle$ there is a number $a \in \mathbb{Z}/q\mathbb{Z}$ such that $A = G^a$

- We call a the exponent of A
- We denote elements of $\langle G \rangle$ as X and their exponents as x
- There is a one-to-one mapping between $\mathbb{Z}/q\mathbb{Z}$ and $\langle G \rangle$

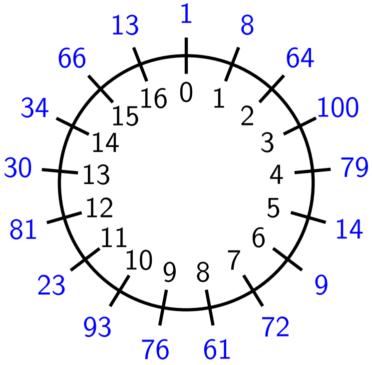
Illustration with circle diagram: $(\mathbb{Z}/17\mathbb{Z})^*$ and $\mathbb{Z}/16\mathbb{Z}$



For a black element $i \in \mathbb{Z}/16\mathbb{Z}$, we have a blue element $3^i \in (\mathbb{Z}/16\mathbb{Z})^*$

Illustration with a circle subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$

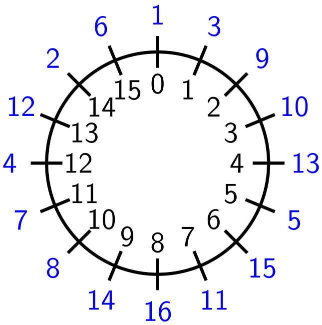
Any cyclic group $\langle g \rangle$ is isomorphic to $\mathbb{Z}/ord(g)\mathbb{Z}$



Here $g = 8 \in (\mathbb{Z}/103\mathbb{Z})^*$ and $ord(g) = 17$

For each $i \in \mathbb{Z}/17\mathbb{Z}$ we have $8^i \in (\mathbb{Z}/103\mathbb{Z})^*$

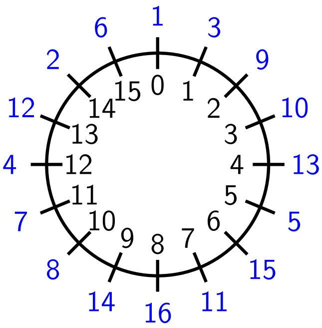
Illustration for $p = 17$ and $G = 3 : q = 16$



For each blue element $3^i \in \langle 3 \rangle$ we have a black element $i \in \mathbb{Z}/16\mathbb{Z}$

- $C = A \times B = A \cdot B \ mod\ 17$ maps to c $=$ a $+$ b mod 16
- $C = A^e \ mod\ 17$ maps to c $=$ a $\cdot$ e mod 16

Discrete log



- given x,compute Xsuch that $X = 3^x \ mod\ 17$: exponentiation
- given X, compute x such that $X = 3^x \ mod\ 17$: discrete log
- exponentiation is easy but discrete log is hard in general

Thanks & Questions