UNIVERSIDAD
NACIONAL
DE COLOMBIA

Mathematics is the queen of sciences and number theory is the queen of mathematics.

— *Carl Friedrich Gauss*

Criptografía

Number Theory Background
RSA Cryptosystem

Yoan Pinzón, PhD
Universidad Nacional de Colombia
Facultad de Ingeniería
Departamento de Ingeniería de Sistemas e Industrial
`ypinzon@unal.edu.co`
`www.pinzon.co.uk`

Content

- **Number Theory Background & RSA**
  - ▷ Divisibility
  - ▷ Division Theorem
  - ▷ Congruent Modulo n
  - ▷ Equivalent Class Modulo n
  - ▷ Integer Modulo n $(\mathbb{Z}_n)$
  - ▷ Multiplicative Inverse
  - ▷ Factorization
  - ▷ GCD
  - ▷ Relatively Prime
  - ▷ Multiplicative Group of $\mathbb{Z}_n$
  - ▷ Euler's Theorem
  - ▷ Fermat's Little Theorem
  - ▷ EEA - Extended Euclidean Algorithm
  - ▷ PowerMod
  - ▷ CRT - Chinese Remainder Theorem
  - ▷ The Order of an Integer
  - ▷ Primitive Elements in $\mathbb{Z}_p^*$
  - ▷ Public-key Cryptography (PKC)
  - ▷ A Postal Analogy
  - ▷ RSA Public-Key Cryptosystem

Divisibility

$\mathbb{N}$ ={1,2,3,4,$\cdots$}	Set of **natural** numbers
$\mathbb{Z} = \{\cdots$,-3,-2,-1,0,1,2,3,$\cdots\}$	Set of **integer** numbers
$\mathbb{Z}^+ = \{1, 2, 3, \cdots\}$	Set of positive integer numbers
$\mathbb{Z}^- = \{\cdots, -3, -2, -1\}$	Set of negative integer numbers

Divition: $a|b$ (read a divides b), if $\exists\, c \in \mathbb{Z} : b = a \cdot c$.

Divisibility Properties:

(i) $a|a$

(ii) $a|b \ \wedge \ b|c \Rightarrow a|c$

(iii) $a|b \ \wedge \ a|c \Rightarrow a|(bx + cy), \forall x, y \in \mathbb{Z}$

(iv) $a|b \ \wedge \ b|a \Rightarrow a = \pm b$

$a|b$ does not imply $b|a$. Find a counterexample.

Division Theorem

$\forall a, b \in \mathbb{Z}, \exists$ unique $q, r \in \mathbb{Z} : a = qb + r, 0 \leq r \leq |b|$.

- $q = \lfloor a/b \rfloor$ is called **quotient** of the division.
- $r = a$ mod b and is called **remainder** (or **residue**).

Example: $a = 36,\ b = 16$

$$a = qb + r$$

$$36 = 2 \cdot 16 + 4$$

$q = 2, r = 4$

Divisor, GCD, Prime, Composite

Divisor: c is a common divisor of a, b if $c|a \wedge c|b$.

Greatest Common Divisor (GCD): $d = \gcd(a, b)$ if d is a common divisor of a and b, and $\forall c, c|a \wedge c|b \wedge c|d$, Note that $d \geq 1$.

The integer $p > 1$ is a **prime** if its only divisors are 1 and p.

An integer $a > 1$ that is not a prime is called a **composite number** (or a **composite**).

Integer 1 (one) is neither prime nor composite but a *unit*.

Integer 2 (two) is a prime (the only even one).

Congruent Modulo n

$$a \equiv b \pmod{n} \text{ iff } \begin{cases} n|(a-b) \\ a \bmod n = b \bmod n \end{cases}$$

Proof:

$$\begin{aligned} a \bmod n &= b \bmod n \\ a - kn &= b - k'n \\ a - b &= k''n \qquad \Rightarrow \qquad n|(a-b) \end{aligned}$$

$$\begin{array}{|l} \hline a \bmod n = \\ a - n\lfloor a/n \rfloor = \\ a - nk \\ \hline \end{array}$$

□

Example: $24 \equiv 9 \pmod{5}$

$$a = b \bmod n \quad \Rightarrow \quad a \equiv b \pmod{n}$$
$$a \equiv b \pmod{n} \quad \not\Rightarrow \quad a = b \bmod n$$

Equivalence Class Modulo n

$$[r]_n = \{r + kn : k \in \mathbb{Z}\}$$

Example:

$[0]_7 = \{\cdots, -21, -14, -7, 0, 7, 14, \cdots\}$
$[1]_7 = \{\cdots, -20, -13, -6, 1, 8, 15, \cdots\}$
$[2]_7 = \{\cdots, -19, -12, -5, 2, 9, 16, \cdots\}$
$[3]_7 = \{\cdots, -18, -11, -4, 3, 10, 17, \cdots\}$
$[4]_7 = \{\cdots, -17, -10, -3, 4, 11, 18, \cdots\}$
$[5]_7 = \{\cdots, -16, -9, -2, 5, 12, 19, \cdots\}$
$[6]_7 = \{\cdots, -15, -8, -1, 6, 13, 20, \cdots\}$

$a \in [b]_n$ is equivalent to writing $a \equiv b(\text{mod } n)$.

Integers Modulo n $(\mathbb{Z}_n)$

$$\mathbb{Z}_n = \{[r]_n : 0 \leq r \leq n-1\} = \{0, 1, 2, \cdots, n-1\}$$

Example:

$\mathbb{Z}_3 = \{0, 1, 2\}$
$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
$\mathbb{Z}_{14} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$
$\mathbb{Z}_{18} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17\}$

Multiplicative Inverse

$$x \in \mathbb{Z}_n \text{ s.t. } ax \equiv 1 \pmod{n}$$

x is denoted by $a^{-}1$

Example: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, $3x \equiv 1 \pmod{4}$, $\boxed{x{=}3}$

<u>Fact 1:</u> $a \in \mathbb{Z}_n$; a is invertible iff $\gcd(a, n) = 1$

$$\begin{array}{lrcl} (\Leftarrow) & ax + ny & = & 1 \\ & n(-y) & = & ax - 1 \quad \rightarrow \quad n|(ax-1) \quad \rightarrow \quad ax \equiv 1 (\bmod n). \end{array}$$

□

Exercise: in $\mathbb{Z}_9$ which integers are invertible and what are their inverse.

Factorization

$n \geq 2$ has a *unique* factorization as a product of distinct prime powers.

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},\ p_i = \text{prime},\ e_i \in \mathbb{Z}^+ \quad 1 \leq i \leq k$$

Example: 24

$$\begin{array}{r|l} 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array}$$

$24 = 2^3 3^1$

GCD

$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$
$b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$

$$gcd(a,b) = p_1^{\mathrm{min}(e_1,f_1)} p_2^{\mathrm{min}(e_2,f_2)} \cdots p_k^{\mathrm{min}(e_k,f_k)}$$

Example: Compute $gcd(210, 126)$

$$\begin{array}{r|l} 210 & 2 \\ 105 & 3 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array} \qquad 210 = 2^1 3^1 5^1 7^1 \qquad \begin{array}{r|l} 126 & 2 \\ 63 & 3 \\ 21 & 3 \\ 7 & 7 \\ 1 & \end{array} \qquad 126 = 2^1 3^2 7^1$$

$\mathrm{gcd}(210, 126) = 2^1 3^1 5^0 7^1 = 2 \cdot 3 \cdot 7 = 42$

Relatively Prime

Two integers a, b are called **relatively prime** if $\mathrm{gcd}(a, b) = 1$

Example:

- 234 and 67 are relatively prime because $\mathrm{gcd}(234, 67) = 1$
- 321 and 34 are relatively prime because $\mathrm{gcd}(321, 34) = 1$
- 762 and 105 are NOT relatively prime because $\mathrm{gcd}(762, 105) = 3$

Exercise: Are 123 and 45 relatively prime?

Multiplicative Group of $\mathbb{Z}_n$

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \text{gcd}(a,n) = 1\}$$

$\phi(n)$=$|\mathbb{Z}_n^*|$= number of integers $[0, n-1]$ which are relatively prime to n

a) $\phi(p) = p - 1$ if p is prime

b) $\phi(nm) = \phi(n)\phi(m)$ if gcd$(n,m) = 1$

c) $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$ if $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$

Exercise: Proof **a)** using **c)** [Hint: use $n = pq$]

Example: Find $\phi(21)$

$\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$, $\phi(21) = \phi(3)\phi(7) = 12$

Euler's Theorem

$$\text{if } a \in \mathbb{Z}_n^*,\ a^{\phi(n)} \equiv 1 \pmod{n}$$

Proof:

$g^{\phi(n)} \equiv 1 \pmod{n}$

$a \in \mathbb{Z}_n^* \Rightarrow \exists x : a \equiv g^x \pmod{n}$

$a^{\phi(n)} \equiv (g^x)^{\phi(n)} \pmod{n} \equiv (g^{\phi(n)})^x \equiv 1 \pmod{n}$

□

Fermat's Little Theorem

$$\text{if } \gcd(a,p) = 1,\ a^{p-1} \equiv 1 \pmod{p}$$

p is prime.

Proof:

Using Euler's Theorem

□

EEA - Extended Euclidean Algorithm

INPUT: $a, b \in \mathbb{Z}^{+}$, $a \geq b$
OUTPUT: (d, x, y), d=gcd(a, b), $x, y \in \mathbb{Z} : ax + by = d$

Pseudo-code:

```
procedure EEA($a,b$)    { $q \leftarrow \lfloor a/b \rfloor$ }
begin
    if $b$=0 then return ($a$, 1, 0)
    $(d', x', y') \leftarrow$ EEA($b, a$ mod $b$)
    $(d, x, y) \leftarrow (d', y', x' - qy')$
    return $(d, x, y)$
end
```

EEA - Extended Euclidean Algorithm

Example

Compute EEA(372, 321)

a	b	q	d	x	y	
372	321	1	3	-44	51	▷ $-44 \times 372 + 51 \times 321 = 3$
321	51	6	3	7	-44	▷ $7 \times 321 + -44 \times 51 = 3$
51	15	3	3	-2	7	▷ $-2 \times 51 + 7 \times 15 = 3$
15	6	2	3	1	-2	▷ $1 \times 15 + -2 \times 6 = 3$
6	3	2	3	0	1	▷ $0 \times 6 + 1 \times 3 = 3$
3	0	–	3	1	0	▷ $1 \times 3 + 0 \times 0 = 3$

PowerMod - Modular Exponentiation

INPUT: $a, b, n \in \mathbb{Z}$
OUTPUT: $z = a^b \bmod n$

Pseudo-code:

```
procedure PowerMod($(a, b, n)$)     { $\langle b_k, b_{k-1}, \ldots, b_0 \rangle_2 \leftarrow b,\ z \leftarrow 1$ }
begin
    for $i \leftarrow k$ downto 0 do
        if $b_i$=1 then $z \leftarrow (z^2 \times a) \bmod n$
        else $z \leftarrow z^2 \bmod n$
    od
return $z$
end
```

PowerMod - Modular Exponentiation

Example

Compute PowerMod(5,18,17)

$a = 5$
$b = 18_{10} = \langle 10010 \rangle_2$
$n = 17$

i	4	3	2	1	0
b_i	1	0	0	1	0
z	5	8	13	12	8

Then $5^{18} \bmod 17 = 8$

Exercise: Compute PowerMod(7,452,31)

CRT - Chinese Remainder Theorem

The following problem was posed by Sunzi [Sun Tsu] (4th century AD) in the book Sunzi Suanjing:

> *"There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?"*

CRT was commonly known as General Sun counting the soldiers or General Han counting the soldiers.

Oystein Ore mentions another puzzle with a dramatic element from Brahma-Sphuta-Siddhanta (Brahma's Correct System) by Brahmagupta (born 598 AD):

> *"An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?"*

Problems of this kind are all examples of CRT

CRT - Definition

Let $n_1, n_2, \ldots, n_k$ be *pairwise relatively prime* integers. If $a_1, a_2, \ldots, a_k$ are any integers, then the system of simultaneous congruences

$$x \equiv a_i \pmod{n_i} \quad \forall i \in \{1 \ldots k\}$$

has a unique solution modulo $N = n_1 n_2 \ldots n_k$

$$x = \sum_{i=1}^{k} N_i y_i a_i \bmod N$$

where $N_i{=}N/n_i$ and $y_i{=}N_i^{-1} \bmod n_i$

Example

k=2, n_1=5, n_2=3

N=$n_1 n_2$=5×3=15

$\pi(x)$=(x mod 5, x mod 3) : $\mathbb{Z}_{15} \rightarrow \mathbb{Z}_5 \times \mathbb{Z}_3$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\pi(x)$	(0,0)	(1,1)	(2,2)	(3,0)	(4,1)	(0,2)	(1,0)	(2,1)	(3,2)	(4,0)	(0,1)	(1,2)	(2,0)	(3,1)	(4,2)

	0	1	2
0	0	10	5
1	6	1	11
2	12	7	2
3	3	13	8
4	9	4	14

$$N_1 = N/n_1 = 15/5 = 3$$
$$N_2 = N/n_2 = 15/3 = 5$$

$$y_1 = N_1^{-1} \text{ mod } n_1 = 3^{-1} \text{ mod } 5 = 2$$
$$y_2 = N_2^{-1} \text{ mod } n_2 = 5^{-1} \text{ mod } 3 = 2$$

$$\begin{aligned} x = \pi^{-1}(a_1, a_2) &= (N_1 y_1 a_1 + N_2 y_2 a_2) \text{ mod } N \\ &= (3 \times 2a_1 + 5 \times 2a_2) \text{ mod } 15 \\ &= (6a_1 + 10a_2) \text{ mod } 15 \end{aligned}$$

for a_1=1 and a_2=2 we get

$$x \equiv 1 \pmod 5$$
$$x \equiv 2 \pmod 3$$

$$\begin{aligned} x = \pi^{-1}(1, 2) &= (6 \times 1 + 10 \times 2) \text{ mod } 15 \\ &= (6 + 20) \text{ mod } 15 \\ &= 26 \text{ mod } 15 \\ &= 11 \end{aligned}$$

$$11 \text{ mod } 5 = 1$$
$$11 \text{ mod } 3 = 2$$

The Order of an Integer

Let $a \in \mathbb{Z}_n^*$.

$$\text{ord}(a) = \min(t : a^t \equiv 1 \pmod{n}\ )$$

Exercise: Find the order of 5 with the following moduli

i) 7
ii) 11
iii) 21

Primitive elements in $\mathbb{Z}_p^*$

for p=prime, α is called a **primitive element modulo p** if

$$\mathbb{Z}_p^* = \{\alpha^i \bmod p : i \in \mathbb{Z}_p^*\}$$

Example

For p=13 find all the possible *primitive elements modulo 13*.

t	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
2^t mod 13	2	4	8	3	6	12	11	9	5	10	7	1
3^t mod 13	3	9	1	3	9	1	3	9	1	3	9	1
4^t mod 13	4	3	12	9	10	1	4	3	12	9	10	1
5^t mod 13	5	12	8	1	5	12	8	1	5	12	8	1
6^t mod 13	6	10	8	9	2	12	7	3	5	4	11	1
7^t mod 13	7	10	5	9	11	12	6	3	8	4	2	1
8^t mod 13	8	12	5	1	8	12	5	1	8	12	5	1
9^t mod 13	9	3	1	9	3	1	9	3	1	9	3	1
10^t mod 13	10	9	12	3	4	1	10	9	12	3	4	1
11^t mod 13	11	4	5	3	7	12	2	9	6	8	10	1
12^t mod 13	12	1	12	1	12	1	12	1	12	1	12	1

a	1	2	3	4	5	6	7	8	9	10	11	12
ord(a)	1	**12**	3	6	4	**12**	**12**	4	3	6	**12**	2

Hence, the *primitive elements modulo 13* are 2, 6, 7 and 11.

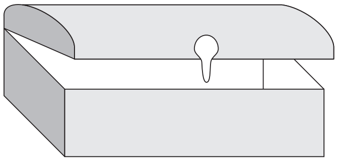
Public-key Cryptography (PKC)

- PKC is also known as asymmetric cryptography.
- A problem with symmetric key cryptosystems is *key distribution* and *key management*.
- In PKC key management is much simpler
  - only decryption key must be kept secret
  - encryption key can be published
  - computing private key from their corresponding public key is infeasible
- In PCK no key exchange between users is necessary
- PCK not only simplify key management but can also be used to generate digital signatures.

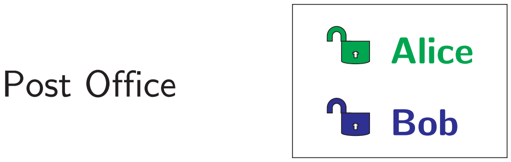
A Postal Analogy

In this example Alice has the secret message and wants to send it to Bob, after which Bob sends a secret reply.

Assume that the message is send in a box with a clasp ring.



Bob and Alice have separate open padlocks with their names, freely available in a place such as a post office.



Post Office

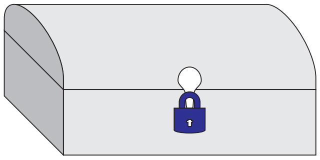
Alice

Bob

Firstly, Alice gets Bob's open padlock from the postoffice.

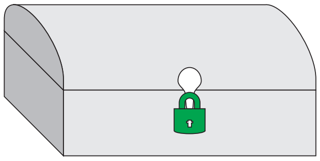
A Postal Analogy (cont.)

Alice uses Bob's padlock to lock a box containing her message, and sends the locked box to Bob.



Bob can then unlock the box with his key and read the message.

To reply, Bob must similarly get Alice's open padlock to lock the box before sending it back to her.

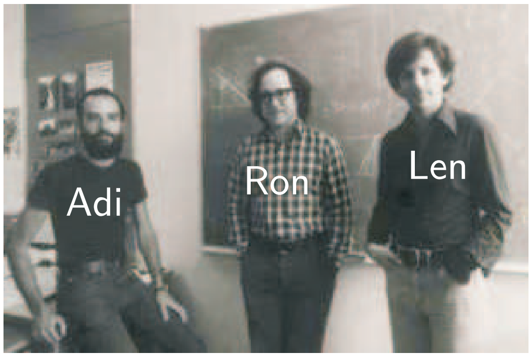


The critical advantage in an asymmetric key system is that Bob and Alice never need send a copy of their keys to each other.

RSA Public-Key Cryptosystem

Ronald **R**ivest, Adi **S**hamir, Leonard **A**dleman, 1977

RSA was named after its developers Ronald **Rivest**, Adi **Shamir**, and Leonard **Adleman**.

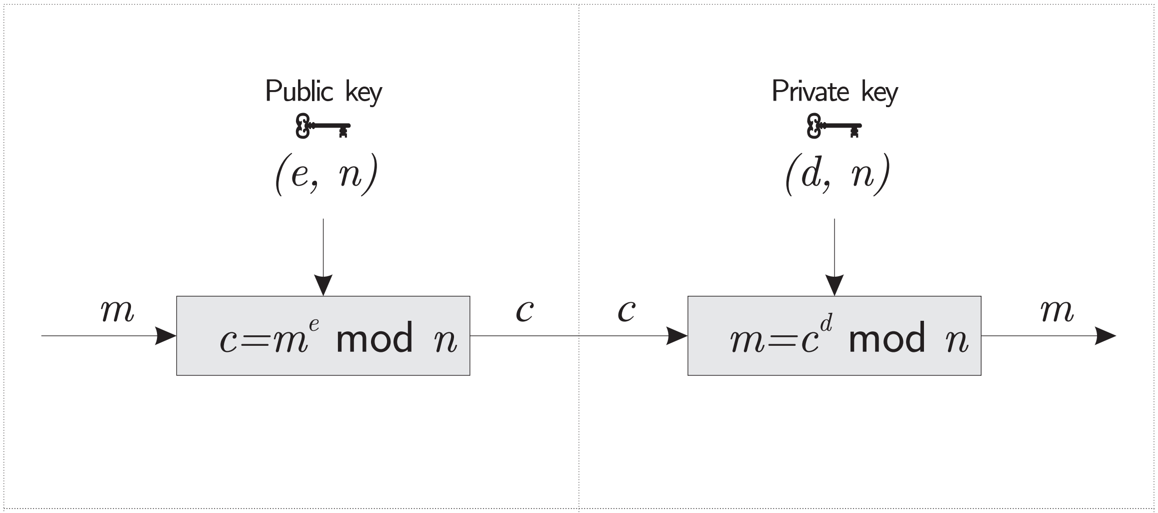


RSA Security released the patent into the public domain in 2000.

RSA is the most widely use PKC.

Its security is based on the intractability of the integer factorization problem.

RSA Crytosystem



Public key

$(e,\ n)$

m $\longrightarrow$ $\boxed{c = m^e \bmod n}$ $\longrightarrow$ c

Private key

$(d,\ n)$

c $\longrightarrow$ $\boxed{m = c^d \bmod n}$ $\longrightarrow$ m

(a) Encipherment

(b) Decipherment

RSA Crytosystem (cont.)

(a) Key Generation:

1) Generate two large random primes p and q ($p \neq q$ and $|p| \approx |q|$)

2) Compute $n = pq$ and $\phi = (p-1)(q-1)$

3) Select a random integer e, $1 < e < \phi$ such that GCD(e, ϕ)=1

4) Use EEA(ϕ, e) algorithm to find y (d) such that $ed \equiv 1$(mod ϕ)

5) Publish (e, n) as RSA public key

6) Keep (d, n) as RSA secret key

RSA Crytosystem (cont.)

(b) Encryption:

1) Compute $m = m_1, m_2, \ldots, m_t$ such that $m_i < n \, \forall i \in \{1, \ldots, t\}$

2) Compute c_i=PowerMod(m_i, e, n) $\forall i \in \{1, \ldots, t\}$

(c) Decryption:

1) Compute m_i=PowerMod(c_i, d, n) $\forall i \in \{1, \ldots, t\}$

Example

Doing business on the internet requires you (*client*) to send personal information (e.g. credit card numbers) to a business (*server*). To do this securely, your client software must encrypt your credit card number so that others cannot intercept it. It is currently done with RSA encryption software. The following is a much too simple example, but it doesn't burden us with large numbers.

(a) Key Generation:

1) Let p=47, q=71

2) Let $n = pq$ =3337, $\phi = 46 \times 70 = 3220$

3) Choose e (at random) to be 79

4) Compute EEA(3220, 79) to find d

ϕ	e	q	gcd(ϕ, e)	x	y	
3220	79	40	1	-25	**1019**	$\triangleright$ $d = 1019$
79	60	1	1	19	-25	
60	19	3	1	-6	19	
19	3	6	1	1	-6	
3	1	3	1	0	1	
1	0	–	1	1	0	

5) Public key = (79, 3337)

6) Private key = (1019, 3337)

(b) Encryption:

To encrypt a credit card m=6882 3268 7966 6683 we break it into smaller numbers such that $m_i < n \ \forall i \in \{1, \ldots, t\}$. For example.

m_1=688, m_2=232, m_3=687, m_4=966, m_5=668, m_6=3

c_i=PowerMod(m_i, 79, 3337) $\forall i \in \{1, \ldots, 6\}$
$b = 79_{10} = \langle 1001111 \rangle_2$
$n = 3337$

i	6	5	4	3	2	1	0	
b_i	1	0	0	1	1	1	1	
m_1	688	2827	3151	2564	1574	595	**1570**	$=c_1$
m_2	232	432	3089	3253	1862	391	**2756**	$=c_2$
m_3	687	1452	2657	3085	2647	1308	**2091**	$=c_3$
m_4	966	2133	1358	1637	2463	80	**2276**	$=c_4$
m_5	668	2403	1399	364	77	2890	**2423**	$=c_5$
m_6	3	9	81	2998	1052	3134	**158**	$=c_6$

c = 1570 2756 2091 2276 2423 158

This message is then sent across the network to the server

(c) Decryption:

Decrypting the message is done at the server. The server knows d, which the client doesn't, so the server can decrypt the above message.

m_i=PowerMod(c_i, 1019, 3337) $\forall i \in \{1, \ldots, 6\}$
$b = 1019_{10} = \langle 1111111011 \rangle_2$
$n = 3337$

i	9	8	7	6	5	4	3	2	1	0	
b_i	1	1	1	1	1	1	1	0	1	1	
c_1	1570	796	735	1308	1733	2752	2880	1955	2535	**688**	$=m_1$
c_2	2756	2560	2206	740	654	57	1073	64	2842	**232**	$=m_2$
c_3	2091	605	640	2517	179	782	1665	2515	2814	**687**	$=m_3$
c_4	2276	2407	2752	1582	890	2013	2784	2142	292	**966**	$=m_4$
c_5	2423	374	480	2459	2889	1445	2146	256	2583	**668**	$=m_5$
c_6	158	3315	3058	2033	521	554	2781	2132	1200	**3**	$=m_6$

Getting back the original message m=6882 3268 7966 6683