Group (G) -

4 properties / Axioms.

(1) Closure
if a & b are element of G
c = a · b is also an element of G.

(2) Associativity.
if a, b & c are element of G, then
(a · b) · c = a · (b · c)

(3) Identity.
For all a in G,
there exists an element e such that.
a · e = a.

(4) Existence of Inverse.
For each a in G.
there exists an element a' called the inverse of a such that.
a a' = a' a = e. / group

(5) commutativity.
∀ a & b in G a · b = b · a.

If 5th property is also satisfied by G
↓
Commutative Group
Abelian Group. [En always has mod]

where • → −, +, *, ÷

(1) Find out whether G = ⟨Z, +⟩ is a commutative group.

(2) Find out " G = ⟨Z*, *⟩ is an abelian group.

$S = \langle \{a, b, c, d\}, \cdot \rangle$

↓

Group / CG / AG.

a is identity element

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

e.

Finite Group:

- Finite no of element else infinite.
- order of a group $|G|$
  $\Rightarrow$ n of element in a group.

Sub group.

H of a group G, if.

① H itself is a group.

if $G = \langle S, \cdot \rangle$ is a group.

then $H = \langle T, \cdot \rangle$ is a group under same operations

② T is ~~any~~ not ~~empty~~ empty subset of S.

Is the group $H = \langle Z_{10}, + \rangle$ a sub group of $G = \langle Z_{12}, + \rangle$.

No

Cyclic Subgroup:

If a subgroup of a group can be generated using the power then subgroup is called a cyclic subgroup of the element,

power → repeatedly applying the group operation.

$a^n = a \cdot a \cdot a \cdot a \cdots$ (n times)

$\langle a \rangle$

$a^1 = a$

$a^2 = a \cdot a$

duplicate elements are discarded $a^0 = e$.

Find subgroups of $\langle Z_{12}, + \rangle$. $Z_{12} = \{0, 1, 2, \dots 11\}$

- order of $Z_{12} \Rightarrow |Z_{12}| = 12$
- find out divisors of order $\Rightarrow \{1, 2, 3, 4, 6, 12\}$. (6 divisors)
- no of subgroups = no of divisors.

$H_1 = \langle 0 \rangle = \{0\}$ — 1

$H_2 = \langle 1 \rangle = \{0, 1, \dots 11\}$

$H_3 = \langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$

$H_4 = \langle 3 \rangle = \{0, 3, 6, 9\}$

$1^0 = 0$
$1^1 = 1 \bmod 12 = 1$
$1^2 = 1+1 \bmod 12 = 2$
$1^3 = 1+1+1 \bmod 12 = 3$
$\vdots$
11

$2^0 = 0$
$2^1 = 2 \bmod 12 = 2$
$2^2 = 2+2 \bmod 12 = 4$
6
8
10

$3^0 = 0$
$3^1 = 3$
$3^2 = 6$
$3^3 = 9$

$4^0 = 0$
$4^1 = 4$
$4^2 = 8$

not divisor.

$6 = 0$
$6 = 6$

$H_5 = \langle 4 \rangle = \{0, 4, 8\}$ — 3

$H_6 = \langle 6 \rangle = \{0, 6\}$ — 2

$\langle Z_6, + \rangle$. → divisor of 6 is $\{1, 2, 3, 6\}$

$1 \Rightarrow 1^0 = 0$
$1^1 = 1$
$1^2 = 2$
$1^3 = 3$
$1^4 = 4$
$1^5 = 5$

$2 \Rightarrow 2^0 = 0$
$2^1 = 2$
$2^2 = 4$

$3 \Rightarrow 3^0 = 0$
$3^1 = 3$

$6 \Rightarrow 6^0 = 0$

(3) $(Z_{10}^*, *)$

$Z_{10}^* \Rightarrow \{(1,1), (3,7), (9,9)\}$

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

$\langle 1 \rangle$ $H_1 \Rightarrow 1^0 = 1$

$1^1 = 1$

$\langle 3 \rangle$ $H_3 \Rightarrow 3^0 = 1$

$3^1 = 3$

~~$3^2 = 6$~~

$3^2 = 9$

$3^3 = 27 \Rightarrow 7$

$3^4 = 1$

$\langle 3 \rangle$ and $\langle 7 \rangle$ are cyclic subgroup of $(Z_{10}^*, *)$

$\langle 7 \rangle$ $H_7 \Rightarrow 7^0 = 1$

$7^1 = 7$

$7^2 = 49 \Rightarrow 9$

$7^3 \Rightarrow 7 \cdot 3$

$7^4 \Rightarrow 1$

$\langle 9 \rangle$ $H_9 \Rightarrow 9^0 = 1$

$9^2 = 81 \Rightarrow 1$

$9^3 \Rightarrow 9$

$9^4 \Rightarrow 1$

27.8.24

Cyclic group.

(eg) $G = \langle Z_6, + \rangle$

$H_i = G$.

- Generator.
- Element in the cyclic gp $\{0, g^1, g^2, \ldots, g^{n-1}\}$ (n elements)

1, 5 are generators.

Lagrange's Theorm.

- order of a gp to the order of its subgp.

$G \rightarrow$ Group order $= |G|$

$H \rightarrow$ subgroup of G. order $= |H|$

$|H|$ divides $|G|$ or $|H| \mid |G|$

$G = \langle Z_6, + \rangle$

$G \Rightarrow |Z_6| = 6$

$|H_1| = 1$, $|H_2| = 3$ $|H_3| = 2$ $|H_4| = 6$.

Applies of L.T

- orders of potential subgroup. if order of gp is known. divisors.

$|Z_6| = 6 \begin{cases} 1 \\ 2 \\ 3 \\ 6 \end{cases}$

eg. $Z_{17} \begin{cases} 1 \\ 17 \end{cases}$.

② $Z_{10} \Rightarrow 10 \begin{cases} 1 \\ 2 \\ 5 \\ 10 \end{cases}$

Order of an element.

ord(a) in n such that.

$a^n = e$.

n = order of potential subgroup generated.

eg $G = \langle Z_6, +_6 \rangle$.

ord(0) = 1

ord(1) = 6

ord(2) = 3

ord(3) = 2

ord(4) = 3

ord(5) = 6

$G = \langle Z_{10}^*, * \rangle$

ord(1) = 1

ord(3) = 4

ord(7) = 4

ord(9) = 2

Ring

$R = \langle \{\dots\}, \cdot, \square \rangle$

- 2 operations.
- 1st oper → · → 5 properties → closure, Asso, identity, inverse, comm
- 2nd oper → $\square$ → 1st prop → closure, Asso.
  - 2nd group is distributed over the 1st oper.

Distributivity.

$\forall\ a, b, c \in R$.

$a \square (b \cdot c) = (a \square b) \cdot (a \square c)$

$(a \cdot b) \square c = (a \square c) \cdot (b \square c)$

2nd opr distributed over 1st group.

- Commutative ring

  2nd opr → commutative prop.

Find out whether the set $R<Z, +, *>$ is commutative ring or not.

★ The above properties are followed so — it is commutative ring.

Field

$F = \{ \{ \ldots \}, \square \}$ → commutative ring.

- 2 opp → all the five prop
- 2nd opp ⇒ Inverse → avail for non-zero.

1st group ⇒ +|−

∴ 2nd group → *|÷

Finite fields

- Finite no of element
- Galois ⇒ no of element ⇒ p^n.

  where p → prime

  + n → any +ve int.
- Galo is field. $GF(2^n)$

  $GF(p^n)$ ⇒ p^n element.

GF (p) field.

$n = 1$

$Z_p = \{0, 1, \ldots, p-1\}$

⇒ 2 arithmetic — + , *

- every element → Additive Inverse
- non zero element → multiplicative Inverse

Field

$P = 2 \quad Z_2 = \{0, 1\}$.

$GF(2)$

$\langle \{0,1\}, +, * \rangle$

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

"+" ⇒ XOR "*" ⇒ AND

Inverse

$a \cdot a' = a' \cdot a = e$ ($0 \Rightarrow +$, $1 \Rightarrow *$)

a	0	1
-a	0	1

a	0	1
a^{-1}	-	1

4.03.29

Fields

Find out whether GF(5) on the set Z_5 with $+^n$ and $*^n$ oprahon is a field.

GF(5)

$Z_5 = \{0, 1, 2, 3, 4\}$ [+ *]

$P = 5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Inverse

$a \cdot a' = a' \cdot a = e$ — 0 doesn't have multiplicative inverse

a	0	1	2	3	4
-a	0	4	3	2	1

AI

a	0	1	2	3	4
a^{-1}	-	1	3	2	4

MI

So, GF(5) is a field on operations +, *.

Summary of AI

AI	Supported OP	Supported set of Int
Group	(+, -) and (*, ÷)	Z_n or Z_n^*
Ring	(+, -) and (*)	Z
Field	(+, -) & (*, ÷)	Z_p (p is prime)

GF(2^n) Field.

- 4 operations → Cryptography.
- n → n bit word.
  - ↳ $2^n - 1$
  - $n = 2 \Rightarrow 4 \rightarrow 0$ to 3
  - $n = 4 \Rightarrow 16 \rightarrow 0$ to 15 → to $2^n - 1$

Z_p → prime

1. Largest $p < n \Rightarrow n = 4 \Rightarrow$ 0 to 15.
2. n bits → $2^n - 1$ Combinations.
   - ↳ +, -, *, ÷ modulus → prime

Consider GF(2^n) where $n = 2$

GF(2^2) → degree of poly ⇒ 2 → modulus poly ↓ irreducible poly.

{00, 01, 10, 11}
↓ ↓ ↓ ↓
0 0+1 x+0 x+1

n bits → poly of degree n−1.

GF(2^2)

+	0 (00)	1 (01)	x (10)	x+1 (11)
0 (00)	0 (00)	1 (01)	x (10)	x+1 (11)
1 (01)	1 (01)	0 (00)	x+1 (11)	x (10)
x (10)	x (10)	x+1 (11)	0 (00)	1 (01)
x+1 (11)	x+1 (11)	x (10)	1 (01)	0 (00)

*	0 (00)	1 (01)	x (10)	x+1 (11)
0 (00)	00	00	00	00
1 (01)	00	01	10	11
x (10)	00	10	x+1 (11)	01
x+1 (11)	00	11	01	10

for degree 2 ⇒ $(x^2 + x + 1)$.

$x^2 + x + 1 \overline{)\, x^2 + 1 \,(1}$
x^2

Polynomials

GF(2^n) ⇒ n bit representation
↳ degree n−1

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots a_1 x^1 + a_0 x^0$$

(i) 1001 0001

8 bits so poly of degree 7.

$$f(x) = 1x^7 + 0x^6 + 0x^5 + 1x^4 + 0x^3 + 0x^2 + 0x^1 + 1 = x^7 + x^4 + x + 1$$

2) $x^5 + x^2 + x$ using 8 bit word.

00100110

operation $\begin{cases} + \\ * \\ \div \end{cases}$ coeff $\begin{cases} 0 \\ 1 \end{cases} \rightarrow GF(2)$

poly $\rightarrow GF(2^n)$

5.03.24

Operations in polynomials.

- coefficients $\rightarrow$ GF(2) field.
- polynomials $\rightarrow$ $GF(2^n)$ field.

Addition

- Coeff - GF(2)
- $+^n \rightarrow$ XOR.

$GF(2^8)$ $\begin{cases} P_1 \rightarrow x^5 + x^2 + x \Rightarrow 00100110 \\ P_2 \rightarrow x^3 + x^2 + 1 \Rightarrow 00001101 \end{cases}$

$P_1 \oplus P_2$. $x^5 + x^3 + x + 1 \Rightarrow 00101011$

Additive identity $\rightarrow$ 0 term.

Additive Inverse $\rightarrow$ The polynomial itself.

Multiplications.

- Coeffs $\rightarrow$ GF(2)
- x^i with $x^j \Rightarrow x^{i+j}$
- degree $> n-1$

$GF(2^8)$

$P_1 \rightarrow x^5 + x^2 + x$

$P_2 \rightarrow x^7 + x^4 + x^3 + x^2 + x$

Irreducible poly $GF(2^8)$ $(x^8 + x^4 + x^3 + x + 1)$

↳ modulus poly. $P_1 * P_2$.

$P_1 * P_2 \rightarrow x^{12} + x^9 + x^8 + x^7 + x^6 + x^5 + x^8 + x^5 + x^4$

$\Rightarrow x^{12} + x^7 + x^2 + x^7 + x^4 + x^3 + x^6 + x^3 + x^2$

$x^8 + x^4 + x^3 + x + 1$

$x^{12} + x^7 + x^2 \mod (x^8 + x^4 + x^3 + x + 1)$

$\Rightarrow x^5 + x^3 + x^2 + x + 1$

$x^4 + 1$

$x^8 + x^4 + x^3 \mid x^{12} + x^7 + x^2$

$+x+1 \quad x^{12} + x^8 + x^5 + x^4$

$x^5 + x^4 + x^3 + x^2$

$x^5 + x^3 + x^2$

$x^4 + x^3 + x + 1$

$P_1 * P_2 \Rightarrow x^5 + x^3 + x^2 + x + 1$

Division

- Polynomial by a Monomial (1 term).

$24x^3 + 12xy + 9x$ by $3x$

$= 8x^2 + 4y + 3$

- Polynomial by a Binomial (2 terms).

$3x^3 - 8x + 5$ by $x+1$

$= 3x^2 - 3x - 5$

- Polynomial by a polynomial.

$3x^2 - 3x - 5$

$a-1 \mid 3x^3 - 8x + 5$

$3x^3 - 3x^2$

$-3x^2 - 8x + 5$

$-3x^2 + 3x$

$-5x + 5$

Mathematics of Asymmetric Cryptographys

① Prime no

Positive Int.

- 1
- Prime no
- Composite no.

- < 10 ? $\rightarrow$ 2, 3, 5, 7
- < 20 $\rightarrow$ 11, 13, 17, 19

② Coprime.

- gcd (a, b) = 1
- "
- p $\rightarrow$ prime.

all integers from 1 to p-1 $\Rightarrow$ coprime with p.

if p = 5 $Z_p = \{0, 1, 2, 3, 4\}$

Z_n^*

$Z_{10}^* = \{1, 3, 7, 9\}$ element of Z_n^* is coprime to n.

Checking for prime nos.

Give a no n, how to find it is is prime?

- find out $\sqrt{n}$.
- All primes $< \sqrt{n}$.
- n is divisible by all prime? if yes, not prime
  if no ⇒ prime.

eg 97

① $\sqrt{97} \Rightarrow 9$.

② 2, 3, 5, 7

③ No

So 97 is prime.

eg 301

① $\sqrt{301} \Rightarrow 17\ldots$

② 2, 3, 5, 7, 11, 13, 17

③ 7 divides 301.

so not prime.

eg 171

① $\sqrt{171} \Rightarrow 13\ldots$

② 2, 3, 5, 7, 11

③ 3 divides 171

so not prime.

Euler's Phi function / Totient fn ⇒ $\phi(n)$

- Find the no of int that are both.
  ① smaller than n & (2) relatively prime to n.

• Z_p, Z_n^*

Four rules

1. $\phi(1) = 0$.
2. $\phi(p) = p-1$ if p is a prime.
3. $\phi(m*n) = \phi(m) * \phi(n)$ if m & n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

If n can be factored.

$n = p_1^{e_1} * p_2^{e_2} * \dots * p_k^{e_k}$

$\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) * (p_2^{e_2} - p_2^{e_2-1}) * \dots$

$(p_k^{e_k} - p_k^{e_k-1})$

if $n > 2$, $\phi(n) \Rightarrow$ even.

6.03.24

Euler's phi fn $\phi(n)$.

① $\phi(1) = 0$

② $\phi(p) = p-1$,

eg 1. $\phi(13) \Rightarrow 12$ $|Z_{13}^*| = 12$.

2	240
2	120
2	60
2	30
3	15
5	5
	1

eg 2 $\phi(10) \Rightarrow \phi(5 \times 2) = \phi(5) * \phi(2)$

$= 4 \times 1 = 4$.

eg 3 $\phi(49) = \phi(7^2) = 7^2 - 1 \Rightarrow 49 - 7 = 42$.

eg 4. $\phi(240) = \phi(2^4 \times 3 \times 5) = \phi(2^4) \times \phi(3) \times \phi(5)$

$= (2^4 - 2^3)(2)(4)$

$= 8 \times 2 \times 4 = 64$

(4) $\phi(4716)$.

$= \phi(2^2 \times 3 \times 11 \times 13)$

$= (2^2 - 2^1) \times 2 \times 10 \times 12$

$= 2 \times 2 \times 10 \times 12 \Rightarrow 480$.

2	4716
2	2358
3	1179
4	393
13	131
	0

(5) $|Z_{29}^*| = \phi(29) = 28$.

(6) $|Z_{26}^*| = \phi(13 \times 2) = 12 \times 1 = 12$.

5	1615
17	323
19	19
	1

(7) $\phi(1615) = \phi(5 \times 17 \times 19) = 1152$.

(8) $\phi(63) = \phi(3^2 \times 7) = (3^2 - 3) \times 6$

$= 36$

3	165
5	55
11	11
	1

(9) $\phi(165) = \phi(3 \times 5 \times 11) = 2 \times 4 \times 10$

$= 80$

Fermat's Little Thm

First version

If p is a prime and a is an int such that p doesn't divide a, then.

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

(1) Find result of $6^{10} \bmod 11$.

$p \Rightarrow 11 \rightarrow$ prime.

$a \Rightarrow 6$.

$6^{10} \bmod 11 = 6^{11-1} \bmod 11 = 60466176 \bmod 11$

$= 1$

2. $5^{12} \bmod 13$.

$p = 13$

$5^{13-1} \bmod 13 \Rightarrow 1$

3 $a = 10 \quad p = 5$.

$10^4 \bmod 5 = 0$

4. $a = 2; \ p = 17$.

$2^{16} \bmod 17 = 1$

Second version

- remove the condn on a.
- If p is a primer & a is an int.

then $a^p \equiv a \bmod p$.

① Find $3^{12} \bmod 11 = (3 \times 3^{11} \bmod 11)$

$= (3^{11} \bmod 11) * (3 \bmod 11)$

$= 3 * 3 = 9$.

② $a = 2; \ p = 7$

$\Rightarrow 2^7 \Rightarrow 2 \bmod 7$

- Appln

⇒ multiplicative inverses → quickly.

if modulus is a prime

If p is a prime & a is an int such that.
p doesn't divide a.

then $a^{-1} \bmod p = a^{p-2} \bmod p$ ——— (1).

proof.

1st version

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

multiply (1) on both sides with a.

$a \times a^{-1} \bmod p = a^{p-2} \bmod p * a$.

$a \times a^{-1} \bmod p = a^{p-1} \bmod p$.

eg) 1. a=8 ; p=17

$8^{-1} \bmod 17 = 8^{17-2} \bmod 17$

$= 8^{15} \bmod 17$.

$= 35184372088832 \bmod 17$

$= 15 \bmod 17$

2. $5^{-1} \bmod 23 = 5^{23-2} \bmod 23 \Rightarrow 5^{21} \bmod 23$

3. $60^{-1} \bmod 101$

$= 60^{101-2} \bmod 101 \Rightarrow 60^{99} \bmod 101$

4. $22^{-1} \bmod 211 = 22^{213}$

11.03.24

Euler's theorm

- Generalisation of Fermat's thm.
- modulus → FT → prime
  → ET → integer.

1st version of Euler's theorm.

If a & b are coprime $a^{\phi(n)} = 1 \bmod n$ ——— (1)

$a^{p-1} \equiv 1 \pmod{p}$ → FT

2nd version of F.T

• removes condition on a & n ⇒

if $n = p * q$, $a < n$ & k an integer

then $a[(k * \phi(n)) + 1] = a \pmod{n}$

if a is neither multiple of p or q then a & n are coprime.

proof

$a^{(k * \phi(n))+1} \bmod n \equiv (a^{\phi(n)})^k * a \bmod n$.

$\equiv 1^k * a \bmod n = a \bmod n$

Multiplicative inverses.

If a & n are coprime.

then $a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$ — (1).

multiply (1) with a on both side

$a \cdot a^{-1} \bmod n = a^{\phi(n)-1} \cdot a \bmod n$.

$= 1 \bmod n$.

eg 1) $8^{-1} \bmod 77$

$= 8^{\phi(77)-1} \bmod 77$

$= 8^{59} \bmod 77$

$\phi(77) = \phi(7 \times 11)$

$= 6 \times 10 = 60$.

8 2
1 6
1

8 1

eg) ② $7^{-1} \bmod 15$

$= 7^{\phi(15)-1} \bmod 15$

$= 7^{8-1} \bmod 15$

$= 7^{7} \bmod 15$

5×3

$4 \quad 2$

$7^1 \bmod 15 = 7$

7

③ $60^{-1} \bmod 187.$

$= 60^{\phi(187)-1} \bmod 187.$

$= 60^{156} \bmod 187.$

$\Rightarrow$

④ $71^{-1} \bmod 100.$

$\Rightarrow 71^{\phi(100)-1} \bmod 100$

$\Rightarrow 71^{39} \bmod 100$

$\Rightarrow 31 \bmod 100.$

$100 = 2^2 \times 5^2$

$= (2^2 - 2) \times (5^2 - 5)$

$= 2 \times 20 = 40.$

Primality Testing

- prime or not.
  - Deterministic P.T alg
  - probabilistic alg
    - → randomized alg
    - → Monte carlo
    - → las vegas.

Study in book.

Deterministic

- Divisibility test.
- Give $n \Rightarrow$ compute $\sqrt{n}$.
- Find all prime $< \sqrt{n}$.
- if n is divisible by any one of these primes, then n is compsite number.
  else it is prime.

Chinese Remainder Thm. (CRT)

↳ Used to solve a set of congruent eqn with 1 variable but diff moduli.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x = a_k \pmod{m_k}$$

It states that the above eqn have an unique soln with moduli are relatively prime, else more than 1 soln.

Steps :

1. Find $M = m_1 * m_2 * m_3 \ldots m_k$.
   ↳ common modulus.
2. Find $M_1 = M/m_1$;
   $M_2 = M/m_2$
   $M_3 = M/m_3$
   $\vdots$
   $M_k = M/m_k$.
3. Find the MI of $M_1, M_2, \ldots M_k$ using the corresponding modulii $(m_1, m_2, \ldots, m_k)$
   $M_1^{-1}, M_2^{-1}, \ldots M_k^{-1}$
4. The soln to simultaneous eqn is.

$$x = [a_1 * M_1 * M_1^{-1} + a_2 * M_2 * M_2^{-1} + \ldots a_k * M_k * M_k^{-1}] \bmod M$$

Crypto continuation

eg

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

1. $M = m_1 * m_2 * m_3$

$= 3 * 5 * 7 = 105$

2. $M_1 = 35 \quad M_2 = 21 \quad M_3 = 15$

3. $M_1^{-1} = 35^{-1} \bmod 3 = 35^{2-1} \bmod 3 = 2$

$M_2^{-1} = 21^{-1} \bmod 5 = 21^{4-1} \bmod 5 = 1$

$M_3^{-1} = 15^{-1} \bmod 7 = 15^{6-1} \bmod 7 = 1$

4. $x = [(2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1)] \bmod 105$

$= [140 + 63 + 30] \bmod 105$

$= 233 \bmod 105$

$= 23 \bmod 105$

12.03.24

CRT

Given. $x \equiv 3 \bmod 4$

$x \equiv 5 \bmod 6$.

$x \equiv 2 \bmod 5$.

1. $M = 4 \times 6 \times 5 = 120$

2. $M_1 = 30 \quad M_2 = 20 \quad M_3 = 24$

3. $M_1^{-1} = 30^{-1} \bmod 4 = 30^{2-1} \bmod 4 = 2$

$M_2^{-1} = 20^{-1} \bmod 6 = 20^{2-1} \bmod 6 = 2$

$M_3^{-1} = 24^{-1} \bmod 5 = 24^{4-1} \bmod 5 = 4$

4. $x = [(3 \times 30 \times 2) + (5 \times 20 \times 2) + (2 \times 24 \times 4)] \bmod 120 =$

(3) $x \equiv 2 \bmod 7$
$x \equiv 3 \bmod 9$.

(4) $x \equiv 1 \bmod 5$
$x \equiv 1 \bmod 7$
$x \equiv 3 \bmod 11$

Application of CRT

- A quadratic congruence.
  $x^2 \equiv a \pmod{x}$ → prime.
- represent a very large integer in terms of a list of small integer.

(i) $z = x + y$; $x = 123$; $y = 334$ ⇒ $z < 100$.

$x \equiv 24 \bmod 99$
$x \equiv 25 \bmod 98$
$x \equiv 26 \bmod 97$

$y \equiv 37 \bmod 99$
$y \equiv 40 \bmod 98$
$y \equiv 43 \bmod 97$

$x+y \equiv (24+37) \bmod 99 \Rightarrow 61 \pmod{99}$
$x+y \equiv 65 \bmod 98 \Rightarrow 65 \pmod{98}$
$x+y \equiv 69 \bmod 97 \Rightarrow 69 \pmod{97}$

$M = 99 \times 98 \times 97 = 941094$

$M_1 = 9506$ $M_2 = 9603$ $M_3 = 9702$.

$M_1^{-1} = 9506^{-1} \bmod 99$
$M_2^{-1} = 9603^{-1} \bmod 98$
$M_3^{-1} = 9702^{-1} \bmod 97$

Limitation of Symmetric key.

Public key & private key (Asymmetric).

Encryption / Decryption.

$C = f(K_{public}, P)$ $P = g(K_{private}, C)$

Category
- encryp / decrypt
- digital sign
- key exchange (session keys)

RSA, Elliptic curve, Diffie Hellman, DSS.

Trapdoor One-way function.

$y = f(x)$ • f is easy to compute
• f^{-1} is difficult to compute } One-way function

Given y + a trapdoor, x can be computed easily.

1 trapdoor one-way function.

sender: $C = P^e \bmod n$ (polynomial)

receiver: $P = C^d \bmod n$ (polynomial)

intruder: $P = \sqrt[e]{C} \bmod n$ → exponential.

~~Encrypt / Decrypting = R = <Z_n~~

algo: p + q are prime.

$n \leftarrow p * q$

$\phi(n) \leftarrow (p-1) * (q-1)$

$1 < e < \phi(n)$

e is coprime of $\phi(n)$

$d \leftarrow e^{-1} \bmod \phi(n)$

Public key ← (e, n)

private key ← d.

Find d if e = 17, + n = 187 (11, 17)

$p = 11$ $q = 17$

$\phi(n) = 160$.

$d = 17^{-1} \bmod 160$

$= 17^{64-1} \bmod 160$

$= 17^{63} \bmod 160$

160 = 16 × 10; 16 → 4 × 4; 10 → 5 × 2

64 − 32

$2^5 \cdot 5$

$= 2^5 \cdot 2^{5}$ ... 4

(2) $p=7 \quad q=11 \quad e=13$ what is d?

$n = 77$

$\phi(n) = 2 \times 5 \times (2^2-2)$
$= 6 \times 10$
$= 60$

$d = 13^{-1} \bmod 60 \quad = \quad d = 13^{16-1} \bmod 60$

Proof of RSA

Assume that plain text revealed by bob is P_1 Prove that it is equal to P.

2nd version of ET

if $n = p*q$, $a < n$ + k is an int then

$$a^{k * \phi(n) + 1} \equiv a \bmod (n)$$

$x \bmod y = ky + x \bmod y$,

where k is an int.

$P_1 = C^d \bmod \phi(n)$

$= (P^e \bmod \phi(n))^d$

$= P^{ed} \bmod \phi(n)$ — (1)

$ed = 1 \bmod \phi(n)$

$ed = (k * \phi(n) + 1) \bmod \phi(n)$

$P_1 = P^{ed} \bmod \phi(n)$

$= P^{k\phi(n)+1} \bmod \phi(n)$

$= P \bmod \phi(n)$

$= P$

$P = 397 \quad q = 401$ choose $e = 343$;

$d = 120007$.

Show that a can send a msg to b if a

knows e d n.

Msg ⇒ NO → alpha q.
13, 14.

n = 159197.
$\phi(n)$ = 158400. PT = 1314.

$C = (13_{14})^{343} \bmod 159197$.

N =

178
256
128
64
320
16
336

A 0
B 1
C 2
D 3
E 4
F 5
G 6
H 7
I 8
J 9
K 10
L 11
M 12
N 13
O 14.

4*2+1

19.03.24

Q1. 7 + 11 = p + q.
e = 13
PT = 5.

n = 77 $\phi(n) = 60$.

(e × d) mod 60 = 1 d = 37.

$C = 5^{13} \bmod 77 = 26 \bmod 77$

$P = 26^{37} = 5 \bmod 77 = 5 \bmod 77$. 8+4+1

101010111

Q2. e = 13 PT = 63.

$C = 63^{13} \bmod 77 = 28 \bmod 77$
= 28.

$63 \bmod 77 = 63$
$63^2 \bmod 77 = 42$
$63^4 \bmod 77 = 70$
$63^8 \bmod 77 = 49$.

Q3. p = 53 q = 59 Let e = 3 k = 2
public key ? private key ? send msg 41 using RSA.

$n = p * q = 3127$ $\phi(n) = 3016$.

$d = e^{-1} \bmod 3016$
$= e^{1349} \bmod 3016$.

$e^{-1} \bmod \phi(n)$

52 58
26 2 29 2
13 2

or

ed = k $\phi(n)$ + 1

$2^3 \times 13 \times 29$.
$2^3 - 2^2$ 12 28
(8 - 4 = 4)

$d = k\phi(n) + 1/e$

$d = 2011$

HI

$P_T = 0708$

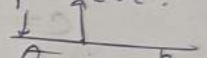
$C = (0708)^3 \bmod 3127$

$= 2301 \bmod 3127$

$P = 2301^{2011} \bmod 3127$

Attacks on RSA

- Factorization → Public key $(e, n) \rightarrow p * q$.
  $d = e^{-1} \bmod \phi(n)$
- Chosen-ciphertext → rand int x [e] in Z_n^*
  $y = C * x^e \bmod n$.
  sends y to B
  $Z = Y$ to B.
  $Z = y^d \bmod n$
  Find out Z.



$Z = y^d \bmod n$.

$= (C * x^e)^d \bmod n$.

$= (C^d \times x^{ed}) \bmod n$

$= (C^d * x) \bmod n$.

$Z = (P * x) \bmod n$

$\Rightarrow \boxed{P = Z \times x^{-1} \bmod n}$.

- Encryption exponent.
- decryption exponent.

Coppersmith

$e = 3$ (small)

$C \rightarrow f(p) = p^e \bmod n$.

If $2/3^{rd}$ bits of P are known the alg can find the remains

Broadcast

$C_1 = p^3 \bmod n_1$

$C_1 = p^3 \bmod n_2$

$C_3 = p^3 \bmod n_3$

30.03.24

ECC — Elliptic curve crypto (163 bits).

- public key Cryptography
- Light weight encrypt cryp.
- key size 163 bits

Non Singular elliptic curve GF(P)

$$y^2 \bmod p = x^3 + ax + b$$

Key Generation:

Private key = x $(1 < x < p-1)$

Public key = y $(y = xG)$ → point in graph.

Encryption k is random number.

$C = (C_1, C_2)$

$C_1 = kG$. $\quad M \Rightarrow P.T.$

$C_2 = M + kY$

Decryption

$$M = C_2 - xC_1$$

$$= M + kY - xkG$$

$$M = M + kxG - xkG \quad \text{proof.}$$

p21
11
132

eg. $y^2 = x^3 + x + 6$ modulus value $p = 11$

$E_p(a, b)$

$p = 11 \quad a = 1 \quad b = 6$

QNR - Quadratic Non residue

x	x^3	$x+6$	$y^2 = x^3 + x + 6$	$y^2 \bmod p$	y
0	0	6	6	6 mod 11 = 6	QNR
1	1	7	8	8 mod 11 = 8	QNR
2	8	8	16	16 mod 11 = 5	(4,7)
3	27	9	36	36 mod 11 = 3	(5,6)
4	64	10	74	74 mod 11 = 8	QNR
5	125	11	136	136 mod 11 = 4	(9,2)
6	216	12	228	228 mod 11 = 8	QNR
7	343	13	356	356 mod 11 = 4	(9,2)
8	512	14	526	526 mod 11 = 9	(3,8)

for x=0

$y^2 \bmod 11 = 6 \bmod 11$

$a^{\frac{p-1}{2}} \bmod p = 1$ ⟹ soln exists

$6^5 \bmod 11 = 1$

$10 = 1$ ✗

for x=1

$8 \bmod 11$

$8^5 \bmod 11 = 10 \neq 1$ QNR

for x=2 ~~for~~ $g^2 \bmod p \equiv 5 \bmod 11$

$5^5 \bmod 11 = 1$ $\boxed{1=1}$ QR.

$a^{\frac{p+1}{4}} \bmod p$ ⟹ $5^3 \bmod 11 = 4$ & $p-4 = 7$.

(4, 7)

for x=3 $y^2 \bmod p = 3 \bmod 11$.

$a^{\frac{p-1}{2}} \bmod 11$ $3^5 \bmod 11 = 1$

$a^{\frac{p+1}{4}} \bmod p$ ⟹ $8^3 \bmod 11 = 5$

(5, 6)

for x=4.

$4^5 \bmod 11$ ⟹ 1

$a^{\frac{p+1}{4}} \bmod p = 4^3 \bmod 11 = 9$ (9, 2)

for x=8

$8^3 \bmod 11 = 3$

9.	729	15	744	$744 \bmod 11 = 7$	QNR
10	1000	16	1016	$1016 \bmod 11 = 4$	(9, 2)

21.03.24

So the points are (2,4) (2,-4) (3,5) (3,6) ~~(5,5)~~
(5,9) (5,2) (7,9) (7,2) (8,3) (8,8)
(10,9) (10,2)

Private key = x. $(1 < x < p-1)$
Public key = y. $(y = xG)$

$x = 2$

$y = xG = 2G = 2(2,4)$

$= (2,4) + (2,4)$
$x_1\ y_1 \quad x_2\ y_2$

(x_3, y_3)
$x_3 = m^2 - 2x_1$
$y_3 = m(x_1 - x_3) - y_1$

} For same point Addition.

Ex eq $y^2 = x^3 x + 6 \mod p$.

$2y \frac{dy}{dx} = 3x^2 + 1 \Rightarrow \frac{dy}{dx} = \frac{3x^2+1}{2y}$ $x_1 = 2$ $y_1 = 4$

$m = \frac{3(2)^2+1}{2(4)} = \frac{3\times4+1}{8} = \frac{13}{8} \mod 11 = 13 \cdot 8^{-1} \mod 11$

$= (13 \cdot 7) \mod 11$

$m = 3$

13
22
13

$x_3 = m^2 - 2x_1$
$= 3^2 - 2(2) = 9 - 4 = 5$ $x_3 = 5$

$y_3 = m(x_1 - x_3) - y_1 = 3(2-5) - 4$
$= -9 - 4 = -13 \mod 11$

$y_3 = 9$

public key $\Rightarrow (5,9)$

Assume $k = 3$; Choose one point as a message to find the ciphertext;

$C = (C_1, C_2)$

$C_1 = kG$

$C_2 = M + kY$

$C_1 = kG \quad C_1 = 3(2,4)$

$= (2,4) + (2,4) + (2,4)$

$= (5,9) + (2,4)$

$x_1 \; y_1 \quad x_2 \; y_2$

22.03.24

$x_3 = m^2 - x_1 - x_2$

$y_3 = m(x_1 - x_3) - y_1$

$m = \frac{y_2 - y_1}{x_2 - x_1} \bmod p$

} for adding different points:

$m = \left(\frac{4-9}{2-5}\right) \bmod 11 = \frac{-5}{-3} \bmod 11 = 5 * 3^{-1} \bmod 11$

$= 5 * 4 \bmod 11 = 20 \bmod 11$

$\boxed{m = 9}$

$x_3 = m^2 - x_1 - x_2 \bmod p$

$= 9^2 - 5 - 2 \bmod 11 = (81 - 7) \bmod 11$

$= 74 \bmod 11$

$\boxed{x_3 = 8}$

$y_3 = m(x_1 - x_3) - y_1 \bmod p$

$= 9(5-8) - 9 \bmod 11$

$= 9(-3) - 9 \bmod 11 = -36 \bmod 11.$

$\boxed{y_3 = 8}$

$C = (8, 8)$

$9(2-8) - 4$

$= -54 - 4$

$= -58 \bmod 11$

66

$= 8$

$C_2 = M + KY$. $M = (2,4)$ $k = 3$ $y = (5,9)$

$= (2,4) + 3(5,9)$

$= \underbrace{(2,4) + (5,9)}_{(8,8)} + \underbrace{(5,9) + (5,9)}_{(10,9)}$

$(5,9) + (5,9) = ?\ (10,9)$

$m = \frac{3x^2 + 1}{2y} \bmod p = \frac{3(5)+1}{18} \bmod 11$ $\quad m = 76 \overline{18} \bmod 11$

$\boxed{m = 3}$

$x_3 = m^2 - 2x_1 \bmod p = 9 - 2(5) \bmod 11 = 9 - 10 \bmod 11$

$= -1 \bmod 11$ $\quad \boxed{x_3 = 10}$.

$y_3 = m(x_1 - x_3) - y_1 \bmod p$

$= 3(5-10) - 9 \bmod 11 = -24 \bmod 11$

$\boxed{y_3 = 9}$

$C_2 = \overset{x_1\ y_1}{(8,8)} + \overset{x_2\ y_2}{(10,9)}$.

$m = \frac{9-8}{10-8} \bmod 11 = \frac{1}{2} \bmod 11 = 1\ 2^{-1} \bmod 11$

$\boxed{m = 6}$

$x_3 = m^2 - x_1 - x_2$

$= 6^2 - 8 - 10$

$= 36 - 18 = 18 \bmod 11$ $\quad \boxed{x_3 = 7}$

$y_3 = m(x_1 - x_3) - y_1$

$= 6(8-7) - 8 = -2 \bmod 11 = 9$ $\quad \boxed{y_3 = 9}$

$C_2 = (7,9)$ the CT $C = ((8,8), (7,9))$

$M = C_2 - xC_1$

$= (7,9) - 2(8,8)$

$= (7,9) - [(8,8) + (8,8)]$

$m = \frac{3x^2+1}{2y} \bmod 11 = \frac{3(64)+1}{2(8)} \bmod 11 = 193 \cdot 16^{-1} \bmod 11$

$= 193 \times 9 \bmod 11.$

$\boxed{m = 9}$

~~$x_3 = m^2 - 2x_1 \bmod p$~~

~~$= 10(8-7) - 8 \bmod 11 = 10 - 8 \bmod 11$~~

~~$y_3 = 2$~~

$x_3 = m^2 - 2x_1 \bmod p = 100 - 16 \bmod p$

$= 84 \bmod 11 = 7$

$\boxed{x_3 = 7}$

$y_3 = m(x_1 - x_3) - y_1 \bmod p$

$= 10(8-7) - 8 \bmod 11$

$= 10 - 8 \bmod 11$

$\boxed{y = 2}$

$M = C_2 - x \cdot C_1$

$= (7,9) - 2(8,8)$

$= (7,9) - (7,2)$

$= (7,9) + (7,-2) \Rightarrow (7,9) + (7,9)$

$m = \frac{3x^2+1}{2y} = \frac{3(49)+1}{2(9)} = 148 \cdot 18^{-1} \bmod 11$

$= 148 \cdot 8 \bmod 11$

$= 1184 \bmod 11$

$m = 7$

$x_3 = m^2 - 2x_1 \mod p.$

$= 49 - 2(7) = 33 \mod 11$ $\quad x_3 = 2$

$y_3 = m(x_1 - x_3) - y_1 \mod p.$

$= 7(7 - 2) - 9 \mod 11$

$= 7(5) - 9 \mod 11 = 35 - 9 \mod 11$

$= 26 \mod 11 = 4$

$y_3 = 4$

$M = (2, 4)$ ✓ verified.