15 November 2025 15:46

handbook of applied cryptography

chapter 2

Mathematical Background

$\pi \approx 3.14159$ $\quad$ $\sum_{i=1}^{n} a_i$ $\quad$ $\prod_{i=1}^{n} a_i$

$e \approx 2.71828$ $\quad$ $n!$ factorial $\quad n(n-1)(n-2)\cdots$

intersection of sets A and B, union of sets, difference of set, Cartesian product of set $A \times B$

subset and proper subset $\quad R \subseteq B \quad A \subset B$

$f: A \to B$ function or mapping; which assigns each element of set A, a element b in B, a is the preimage of b is the image of a | A is called domain of f, B is called co-domain of f

Types of function, injective, onto or surjective; bijection

f: A to B is one to one function, if b of B is the image of at most one a of A

b of B is the image of at least one a of A

b of B is the image of exactly one a of A, here f is called permutation

$\ln x$ natural logarithm of x, to base e

$\lg x$ logarithm of x to base 2

$\exp(x)$ e^x exponential function

2.1 Probability theory

- Sample events, sample space (discrete sample space)

If the simple event of the sample space (S) be denoted as $s_1, s_2, s_3, s_4 \cdots$

Probability distribution P on S is a sq of numbers p_1, p_2, p_3, p_4 ($\sum p_i = 1$) p_i which is for the i^{th} event that the outcome of the experiment.

$P(E) \quad P(E=3) \quad P(\omega)$

complementary event $\bar{E}$

$P(\bar{E}) = 1 - P(E)$ ... if $S = E \cup \bar{E}$

mutually exclusive if $P(E_1 \cap E_2) = 0$

if $E_1 \subseteq E_2 \quad P(E_1) \leq P(E_2)$

$P(E_1 \cup E_2) = P(E_1 \cap E_2) = P(E_1) + P(E_2) \rightarrow P(E_1 \cup E_2) = P(E_1) + P(E_2) - P(E_1 \cap E_2)$

here E_1 and E_2 are mutually exclusive

then $P(E_1 \cup E_2) = P(E_1) + P(E_2)$

Conditional probability

Conditional probability of E_1 given E_2, denoted by $P(E_1 | E_2) = \frac{P(E_1 \cap E_2)}{P(E_2)}$

- Events E_1 & E_2 are independent $P(E_1 \cap E_2) = P(E_1) P(E_2)$

then the conditional probability will be $P(E_1 | E_2) = \frac{P(E_1 \cap E_2)}{P(E_2)} = \frac{P(E_1) \cdot P(E_2)}{P(E_2)} = P(E_1)$

also $P(E_2 | E_1) = \frac{P(E_2 \cap E_1)}{P(E_1)} = \frac{P(E_2) \cdot P(E_1)}{P(E_1)} = P(E_2)$

* Bayes' theorem → if E_1 and E_2 are events with $P(E_2) > 0$

then, $P(E_1 | E_2) = \frac{P(E_1) P(E_2 | E_1)}{P(E_2)}$ $\qquad P(A|B) = \frac{P(A) P(B|A)}{P(B)}$

$S = \{B_1, B_2, B_3\}$

E bolt is defective

$P(B_1) = 0.25 \quad P(E|B_1) = 0.05$

$P(B_2) = 0.35 \quad P(E|B_2) = 0.04$

$P(B_3) = 0.40 \quad P(E|B_3) = 0.02$

happened

$P(B_2|E) = \frac{P(B_2) P(E|B_2)}{P(E)}$

$= \frac{P(B_2) \cdot P(E|B_2)}{P(E|B_1) \cdot P(B_1) + P(E|B_2) \cdot P(B_2) + P(E|B_3) \cdot P(B_3)}$

$= \frac{(0.35)(0.04)}{(0.05)(0.25) + (0.04)(0.35) + (0.02)(0.40)}$

=

Random variables

A random variable X is a function from the sample space S to the set of real numbers

$f: S \to X$

X=1 head X=0

expected value or mean $E(X) = 0.5(0) + 0.5(1)$

expect. $E(0) = P(X=0) \cdot 0 = 0.5(0) = 0$

Mean $E(X) = \sum_{x \in R} x \cdot P(X=x)$

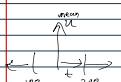
Variance: $\mathrm{Var}(X) = E((X-\mu)^2)$

Standard deviation: σ a non-negative square root of $\mathrm{Var}(X)$

Chebyshev's inequality: let X be a random variable with mean $\mu = E(X)$ and variance $\sigma^2 = \mathrm{Var}(X)$ then for any $t > 0$,

$P(|X-\mu| \geq t) \leq \frac{\sigma^2}{t^2}$

If a random variable has small variance then large deviations from the mean are unlikely to be observed. this statement is made precise below:



K = the number of standard deviations

$t = K\sigma$; represents the actual distance (or deviation) from the mean.

$P(|X-\mu| \geq t) \leq \frac{\sigma^2}{t^2}$

the variance of the daily visitor is $\sigma^2 = \mathrm{Var}(X) = 100000$

mean 5000

we have to find the distance from the mean to either end of this range

$t = 5500_{(\text{upper bound})} - 5000_{(\text{mean})} = 500$

$t = 5000_{(\text{mean})} - 4500_{(\text{lower bound})} = 500$

$t = 500$

same as probability that the distance from the mean is 500 or more

$P(|X-\mu| \geq t) \leq \frac{\sigma^2}{t^2}$

$P(|X-5000| \geq 500) \leq \frac{100000}{(500)^2}$

$P(|X-5000| \geq 500) \leq 0.4$

The question: what is the maximum probability that on a given day the number of visitors will be less than 4500 or more than 5500

Answer: there is at most a 40% probability that the daily visitor count will be outside the 4500 to 5500 range.

Binomial distribution

for n and k be non-negative integers

The binomial coefficient $\binom{n}{k}$ is the number of different ways of choosing k distinct objects from a set of n distinct objects, where the order of choice is not important.

properties of binomial coefficients: let n and k be non-negative integers $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

$\binom{3}{2} = \frac{3!}{2!(3-2)!} = \frac{3 \times 2!}{2! \, 1!} = 3$

binomial theorem $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

$n=2: \quad \sum_{k=0}^{2} \binom{2}{k} a^k b^{2-k} = \frac{2!}{0!(2-0)!} a^0 b^2 + \frac{2!}{(1!)(2-1)!} a^1 b^1 + \frac{2!}{(2!)(2-2)!} a^2 b^0$

$(a+b)^2 = b^2 + 2ab + a^2$

$(a+b)^2 = a^2 + 2ab + b^2$

→ Bernoulli trial is an experiment with exactly two possible outcomes, called success and failure.

$\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

$a = p, \quad b = (1-p)$

$\sum_{k=0}^{n} \binom{n}{k} p^k (1-p)^{n-k}$ → is the probability distribution is called the binomial distribution.

The expected number of success in a sequence of n independent Bernoulli trials, with probability p of success in each trial is np. The variance of the number of successes is $np(1-p)$

law of large number: let X be the random variable denoting the fraction of success in n independent Bernoulli trials with probability p of success in each trial. then for any $\epsilon > 0$

$P(|X-\mu| > \epsilon] \rightarrow 0$ as $n \rightarrow \infty$

Var(X) = np(1-p) = npq

law of large number: Let X be the random variable denoting the fraction of success in n independent Bernoulli trials with probability p of success in each trial. then for any $\epsilon > 0$

$$P(|X - u| > \epsilon) \to 0, \text{ as } n \to \infty$$

In other words, as n get larger the proportion of success should be close to p, the probability of success in each trial

The falling factorial $m^{(n)}$ — It is a product of n numbers, starting from m and falling (decreasing) by 1 each time

$$m^{(n)} = m(m-1)(m-2)\cdots(m-n+1)$$

it counts the number of ways to pick n items from a set of m items where the order matters and you don't put them back

Eg: 5 people, 3 rewards (1st, 2nd, 3rd).

$$m^{(n)} \quad 5^3 = 5(5-1)(5-2) = 60 \text{ ways}$$

Stirling Number of the second kind : $\left\{ {m \atop n} \right\}$

it counts the number of ways to divide (or partition) m distinct objects into n non-empty, identical group

Eg: just find $\left\{ {3 \atop 2} \right\}$ How many way can you split 3 distinct objects $\{A, B, C\}$ ($m=3$) and into 2 non-empty groups ($n=2$)

① $\{A,B\}\ \{C\}$
② $\{B,C\}\ \{A\}$
③ $\{C,A\}\ \{B\}$

$\left\{ {3 \atop 2} \right\} = 3$

The classical occupancy problem:

The setup:
- you have an urn with m different balls
- you draw a ball, note its number and put it back
- you do this n times

question: What is the probability that in your list of n numbers you end up with exactly t different (unique) numbers?

The formula:

$$P_t(m,n,t) = \frac{\left\{ {n \atop t} \right\} m^{(t)}}{m^n}$$

$\left\{ {n \atop t} \right\}$ group your draws possible groupings. → Successful possibilities

$m^{(t)}$ assign the balls to the groups (falling factorial)

m^n total number of possible outcomes

if we draw 4 times ($n=4$) and get 2 unique balls ($t=2$) say "Ball A" and Ball B

- E.g. Draw 1, Draw 3 → got "Ball A"
- & Draw 2, Draw 4 → got "Ball B"

$\left\{ {4 \atop 2} \right\} = 7$

eg: birthday problem calculate $P_t(m,n,t)$ in a group of 23 people atleast two share a birthday different birthday

$$P_t(m,n,t) = \frac{\left\{ {n \atop t} \right\} m^{(t)}}{m^n}$$

m = total birthday is 365

n (draws) = group is 23

t (different balls) we are looking first that all 23 have different birthday so, $n=t=23$

$$P_{23} = \frac{\left\{ {23 \atop 23} \right\} \times 365^{(23)}}{365^{23}}$$

$\left\{ {23 \atop 23} \right\}$ Falling factorial 365^{23} $365 \times 364 \times 363 \cdots (365 - 23 + 1)$

365^{23} $365 \times 365 \times 365 \cdots$ (23 times)

put 23 objects into 23 non-empty group : only one way

$\left\{ {23 \atop 23} \right\} = 1$

$$= \frac{1 \times 365^{(23)}}{365^{23}} = 0.4927 \quad 49.27\%.$$

The probability that at least two people having a birthday is $1 - P_t(m,n,t)$

$= 1 - 0.4927 = 0.5073$ in a group of 23 people

2.2 INFORMATION THEORY

- **Entropy** : it is a mathematical measure of the amount of information provided by an observation of X. it is an uncertainty about the outcome before an observation of X

$$H(X) = -\sum_{i=1}^{n} P_i \lg P_i$$

where P_i is the probability $P(X=x_i) = P_i$ where $0 \le P_i \le 1$ for each i, $i \le i \le n$ and $\sum_{i=1}^{n} P_i = 1$

$$H(X) = \sum_{i=1}^{n} P_i \lg\left(\frac{1}{P_i}\right)$$

- $0 \le H(X) \le \lg n$
- $H(X) = 0$ if $P_i = 1$ for some i, and $P_j = 0$ for all $j \neq i$ (there is no uncertainty)
- $H(X) = \lg n$ if and only if $P_i = 1/n$ for each i, $1 \le i \le n$ (this is all outcomes are equally likely)

Joint Entropy

$$H(X,Y) = -\sum_{x,y} P(X=x, Y=y) \lg\left(P(X=x, Y=y)\right)$$

- if X and Y are random variables, the $H(X,Y) \le H(X) + H(Y)$, with equality if and only if x and Y are independent

Conditional Entropy, also called as **Equivocation of Y about X**

$$H(X|Y=y) = -\sum_{x \in X} P(X=x|Y=y) \lg\left(P(X=x|Y=y)\right)$$

$$H(X|Y) = \sum_{y} p(Y=y)\, H(X|Y=y)$$

→ property of conditioned entropy ← no uncertainty.

- $H(X|Y) \ge 0$ and $H(X|X) = 0$
- $H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$
- $H(X|Y) \le H(X)$: with equality if and only if X and Y are independent.

mutual information or **transinformation** of random variables X and Y is

$I(X;Y) = H(X) - H(X|Y)$ can be thought as the information Y reveals about X

similarly the transinformation of X and the pair Y,Z is defined by

$I(X;Y,Z) = H(X) - H(X|Y,Z)$ can be thought as the amount of information that Y and Z together reveals about X

Conditional transinformation of the pair X,Y given Z is defined as to

$$I_Z(X;Y) = H(X|Z) - H(X|Y,Z)$$

Properties of conditional transinformation

$I_Z(X;Y) = H(X|Z) - H(X|Y,Z)$

$I(X;Y,Z) = H(X) - H(X|Y,Z)$

$I(X;Y,Z) = I(X;Y) + I_Y(X,Z)$

$I_Z(X;Y) = I_Z(Y;X)$

2.1.6 Random mappings → ? (is no. of edge, rho-length, tree size, component size, predecessors size of u imp for exam)

2.3 Complexity theory

measured based on time, storage, randomness, number of processors

The number of bits in the binary representation of a positive integer n is $1 + \lfloor \lg n \rfloor$ or simply $\lg n$

if f is a polynomial of degree k then the size of f is $(k+1)\lg n$ bits

if A is a matrix with r rows, s column, and non negative integers at most n then size of A is $rs \lg n$ bit

- running time
  - worst case running time — eg: cooking for 1 to 10 guest
  - average-case — no. of guest n just looking at the cooking style is not the proper way to quantify the runtime so
- **Asymptotic notation**:
  we look at the trend, or how the time grows as the number of guests (n) gets huge.
  Upper Bound = $f(n) = O(g(n))$ $f(n) \le c\,g(n)\ldots$
  logarithmic growth. $O(\log n)$
- O ignores the small details (like actual time) "how fast is the computer" and just tells how the fundamental "growth category" of the algorithm as the input gets massive.

order notation

		(Recipe is)	
asymptotic upper bound	no slower than this	$f(n) = O(g(n))$	– My recipe grows no faster than some factor.
asymptotic lower bound	no faster than this	$f(n) = \Omega(g(n))$	– My recipe grows at least as fast as some category.
asymptotic tight bound	exactly this fast	$f(n) = \Theta(g(n))$	– My recipe grows at the same rate as this category.
o-notation (small o)	insignificant so much faster it's a rounding error	$f(n) = o(g(n))$	– My recipe grows so much slower than this category that it's not even in the same league

Fact: don't care about slower $g(n) + O(n^2)$ then it is $O(n^2)$

approximation: polynomial $n^3 + 5n^2 + 100$: highest power/term = $\Theta(n^3)$

comparative growth rates — Polynomial-time algorithm : If your algorithm's running time is $O(n^k)$ for simple (like n^3 or even n^{100}) it's considered "efficient" and gets put in this group.

Algorithm not in this group like (2^n while exponential) are considered inefficient because their time explodes when n gets even a little bit bigger.

eg: $1 < \ln\ln n < \ln n < \exp(\sqrt{\ln n \ln\ln n}) < n^c < n^{c'} < n^{\ln n} < c^n < n^n < c^{c^n}$

Fact: don't care about slow $g(n) + O(n^2)$ then it is $O(n^2)$

approximation: polynomial n^3+5n^2+100 highest power/term = $\Theta(n^3)$

comparative growth rates

Polynomial-time algorithm: If some algorithm's running time is $O(n^k)$ for some k. (like n^2 or even n^{100}) it's considered "efficient" and gets put in this group.

Algorithm not in this group like 2^n which exponential are considered inefficient because their time explodes when n gets even a little bit bigger

eg: $1 < \ln\ln n < \ln n < \exp(\ln n \ln\ln n) < n^2 < n^3 < n^{\ln n} < e^n < n^n < e^{e^n}$

(exponential time algorithm)

A polynomial time algorithm is an alg. whose worst-case running time function is of the form $O(n^k)$ where n is the input size and k is constant.

↓ an bounded.

(subexponential algorithm) is an algorithm whose worst-case run time function $e^{o(n)}$ ⟷ is faster than any arbitrary algebraic base but slower than/~~same~~ polynomial time adj. $O(n^k)$

subexponential running time $L_n[\alpha, c] = O\left(\exp\left((c+o(1))(\ln n)^{\alpha}(\ln\ln n)^{1-\alpha}\right)\right)$

critic: exponential runtime is inefficient! whereas polynomial runtime is categorized as good + efficient

2.4 Number Theory

$\mathbb{Z}$ $\{\cdots -3, -2, -1, 0, 1, 2, 3, \cdots\}$

$a \mid b$ read as a divides b $\quad b = ac$

$-3 \mid 18 \quad -18/3 = 6 \rightarrow c$

properties:

$a \mid a$

$a \mid b$ $b \mid c$ then $a \mid c$

$a \mid b$ $a \mid c$ then $a \mid (bx + cy)$ for all $x, y \in \mathbb{Z}$

$a \mid b$ $b \mid a$ then $a = \pm b$

$a = hq + r$ (quotient) $\quad a \bmod b$ remainder $\quad a \operatorname{div} b$ quotient (q)

An integer c is a common divisor of a and b if $c \mid a$ & $c \mid b$

$\gcd(a,b) = d$ $\quad d \mid a$ $\quad d \mid b$

Common divisors of 12, 18 are $\{\pm 1, \pm 2, \pm 3, \pm 6\}$

and $\gcd(12, 18) = 6$

d largest positive integer.

* ($\gcd(a,b) = 1$, then a, b are co-prime or relatively prime)

→ fundamental theorem of arithmetic → every integer $n \geq 2$ has a factorization of product of prime power

$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}$ $\quad p_i$ are distinct prime $\quad e_i$ are positive intr.

ex $a = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}$ $\quad b = p_1^{f_1} p_2^{f_2} p_3^{f_3} \cdots p_k^{f_k}$ the

$\gcd(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} p_3^{\min(e_3,f_3)} \cdots p_k^{\min(e_k,f_k)}$

$a = 4864 = 2^8 \cdot 19$

$b = 3458 = 2 \cdot 7 \cdot 13 \cdot 19$

$\gcd(4864, 3458) = 2^{\min(8,1)} \cdot 7^{\min(0,1)} \cdot 13^{\min(0,1)} \cdot 19^{\min(1,1)}$

$= 2^1 \cdot 19^1$

$= 2 \cdot 19$

$= 38$

$\operatorname{lcm}(a,b) = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \cdots p_k^{\max(e_k,f_k)}$

$\operatorname{lcm}(4864, 3458) = 2^8 \cdot 7 \cdot 13 \cdot 19 = 442624$

Φ Euler totient function (Euler phi function)

for $n \geq 1$, let $\phi(n)$ denote the number of integers in the interval $[1, n]$ which are relatively prime to n ($\gcd(a,b) = 1$) the function ϕ is called Euler phi function.

properties of Euler phi function:

- If p is a prime, then $\phi(p) = p - 1$
- Euler phi function is multiplicative, that is if $\gcd(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$ $\quad (mn-1) \quad (m-1)(n-1)$
- If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime factorization of n then $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$

$\phi(n)$ → no of element in $[1, n]$ which are relatively prime to n

for $n \geq 5$

$\phi(n) > \frac{n}{6 \ln\ln n}$

8 if a and b are positive integers with $a > b$, then $\gcd(a,b) = \gcd(b, a \bmod b)$

Euclidean Algorithm for computing gcd: two non-negative a, b, $a \geq b$

1. While $b \neq 0$ do the following:
   1.1 set $t \leftarrow a \bmod b$, $a \leftarrow b$, $b \leftarrow t$
2. Return (a)

running time is $O((\lg n)^2)$

x 1769 868
y 868 434
g 1 2

$x \leftarrow x/2$ $\quad y \leftarrow y/2$ $\quad g \leftarrow 2g$

$t \leftarrow |x - y|/2$

$x \leftarrow t$

Return $(g \cdot y)$

binary gcd algorithm.

INPUT: two positive integers x and y with $x \geq y$

OUTPUT: $\gcd(x, y)$

1. $g \leftarrow 1$
2. while both x and y are even do $x \leftarrow x/2$, $y \leftarrow y/2$, $g \leftarrow 2g$
3. while $x \neq 0$ do the following (once it is now not even)
   3.1 while x is even do $x \leftarrow x/2$
   3.2 while y is even do $y \leftarrow y/2$
   3.3 $t \leftarrow |x - y|/2$
   3.4 If $x \geq y$ then $x \leftarrow t$, otherwise $y \leftarrow t$ (basically, we replace larger number)
4. Return $(g \cdot y)$

solve: gcd (1360, 792)

step 1 a: $1360/2 = 680$

b: $792/2 = 396$

$g = 1 \rightarrow 2$

step 2 $680/2 = 340$

$396/2 = 198$

$g = 2g = 2 \rightarrow 4$

step 3 a $340/2 = 170$

b $198/2 = 099 \rightarrow 8$

$g = 2g = 4$

b odd, a even

step 4 $a = 170/2 = 85$

$b = 99$

$g = 4$

step 5 a, b odd

$a = 85$

$b = (99 - 85)/2 = 4/2 = 2$

step 6 a odd, b even

$a = 85$

$b = 2/2 = 1$

step 7 add

$1360 = 792(\quad) + 8 = 8$

$\gcd(x, y)$

Start with $a = x$, $b = y$, $g = 1$

then see if both even $x/2, y/2$ $\quad g = 2g$

then see if a = even, then $a = a/2$, $b = y$ (coz it is)

then see if b = even, then $b = y/2$, $a = x$ (coz it is)

then see if both odd, reduce the largest number and keep the rest coz it's.

do until $x \geq y$, $t \leftarrow |x - y|$

$x \neq 0$

if $a = b$, the GCD is a

gcd (1360, 792)

x	y	g=1
1360/2	792/2	
680	396	g=2g=2
680/2=340	396/2=198	g=2g=4
340/2=170	198/2=99	g=2g=8
odd 170/2=85	99	g=8
85	99-85/2=2	g=8
odd =85	2/2=1	g=8
85-1/2=84/2=42	1	g=8
42/2=21	1	g=8
odd 21-1/2=20/2=10	1	g=8
10/2=5	1	g=8
5-1/2=4/2=2	1	g=8
2/2=1	1	g=8

gcd: g.y

$= 4 \cdot 1 = 4 = 8$

a = 85
b = (99-85)/2 = 14/2 = 2

Step 6 a odd, b = even
a = 85
b = 2/2 = 1

Step 7 odd
a = (85-1)/2 = 84/2 = 42
b = 1

Step 8 even odd
a = 42/2 = 21
b = 1

Step 9 odd, odd
a = (a-b)/2 = (21-1)/2 = 20/2 = 10
b = 1

step 10 a = even b = odd
a = 10/2 = 5
b = 1

Step 11 a = odd, b = odd
a = (5-1)/2 = 4/2 = 2
b = 1

Step 12 = a even b = odd
= a = 2/2 = 1
b = 1

step 13 odd, odd
= |a-b|/2 = 0
g·y 4·(1) = 4

↳ $x \neq 0$
if $a = b$, the GCD is a
if $b = 0$, the GCD is b.

The integers modulo n

Let n be a positive integer

- If a and b are integers, then a is said to be congruent to b modulo n, $a \equiv b \pmod n$ if n divides $(a - b)$. The integer n is called the modulus of the congruence.

i) eg $24 \equiv 9 \pmod 5$
$(24-9)/5 = 15/5$ $3 \cdot 5/5$ ✓

$-11 \equiv 17 \pmod 7$ -11 -17 $-28/7$ ✓
$-4 \cdot 7$

eg can also be written as
$8 \equiv 14 \pmod 3$ $8 = 3(2) + 2$ (2 = remainder) $14 \div 3 = 12$ remainder 2 ($3 \times 4 = 12$)
$8 \equiv 2 \pmod 3$ → $(8-2)/3$ then it is called congruent.
$6/3$ $2 \cdot 3/3$ ✓ So it is congruent.

Properties of congruences:
- For all $a, a_1, b, b_1, c \in \mathbb{Z}$
- $a \equiv b \pmod n$ if and only if a and b leaves the same remainder when divided by n.
- (reflexivity) $a \equiv a \pmod n$
- (symmetry) $a \equiv b \pmod n$ then $b \equiv a \pmod n$
- (transitivity) if $a \equiv b \pmod n$ and $b \equiv c \pmod n$ then $a \equiv c \pmod n$
- If $a \equiv a_1 \pmod n$ and $b \equiv b_1 \pmod n$ then
  $a+b = a_1 + b_1 \pmod n$
  $a \cdot b = a_1 \cdot b_1 \pmod n$
  $a \equiv b \pmod n$

each integer a is congruent modulo n to a unique integer between 0 to n-1 called the least residue of a modulo n
$a \equiv b \pmod n$
$a \equiv r \pmod n$

$\mathbb{Z}_{25}$ {1, 2, ... 25}
In $\mathbb{Z}_{25}$ $13 + 16 = 29$ $= 4$ $\equiv 4 \pmod{25}$
$13 \cdot 16 = 8$ in $\mathbb{Z}_{25}$

Multiplicative inverse of a modulo n is an integer $x \in \mathbb{Z}_n$ such that $ax \equiv 1 \pmod n$ if such x exists then it is unique and a is said to be invertible or a unit. the inverse of a is denoted by a^{-1}

FACT: let $a \in \mathbb{Z}_n$ a is invertible if and only if $\gcd(a, n) = 1$

$\mathbb{Z}_9$ $ax = 1 \bmod n$ let's say we need to find inverse of $a = 4$
$4x = 1 \bmod 9$
$4 \cdot (x) = 1 \bmod 9$
$a \cdot x + b \cdot y = 1$
$4 \cdot x + b \cdot y = 1$

$g(a, n) = 1$
$g(4, 9) =$
$9 = 4(2) + 1$ $1 = 9 - 4(2)$
$4 = 1(4) + 0$ $1 = (-2)4 + (1) \cdot 9$
(-2) to get it into the $\mathbb{Z}_9$ add it with 9

$-2 + 9 = 7$
So the inverse of 4 is 7
$\mathbb{Z}_9$ is {1, 2, 3, 4, 5, 6, 7, 8} $4^{-1} = 7$

CRT Theorem Chinese remainder theorem
If the integers $n_1, n_2 \ldots n_k$ are pairwise relatively prime then the system of simultaneous congruences

$x \equiv a_1 \pmod{n_1}$
$x \equiv a_2 \pmod{n_2}$
$x \equiv a_3 \pmod{n_3}$
$\vdots$
$x \equiv a_k \pmod{n_k}$

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

CRT CRT is a powerful result in number theory the system of simultaneous linear congruences

Def: The theorem essentially states that if you know the remainder of a number when it's divided by several different numbers, you can determine the number itself, provided their divisors are relatively prime

unknown integer x solve
$x \equiv a_1 \bmod n_1$
$x \equiv a_2 \bmod n_2$
$\vdots$
$x \equiv a_k \bmod n_k$

Provided $\gcd(n_i, n_j) = 1$ for all $i \neq j$
unique solution modulo the product of all the moduli $n_1, n_2 \ldots n_k$ i.e. N
$N = n_1 n_2 \ldots n_k$
$0 \leq x < N$

$x \equiv 2 \pmod 3$ $a_1 = 2$ $n_1 = 3$ $N = 3 \times 5 = 15$ $M_1 = N/n_1 = 15/3 = 5$
$x \equiv 3 \pmod 5$ $a_2 = 3$ $n_2 = 5$ $M_2 = N/n_2 = 15/5 = 3$
(find the inverse of M_1) M_2 i.e y_1, y_2)

$x \equiv 1 \bmod 4$
$x \equiv 2 \bmod 5$
$x \equiv 3 \bmod 7$

Gauss's algo

$x \equiv 2 \pmod 3$ ($a_1 = 2$, $n_1 = 3$) $N = n_1 n_2 = 3 \cdot 5 = 15$, $M_1 = N/n_1 = 15/3 = 5$
$x \equiv 3 \pmod 5$ ($a_2 = 3$, $n_2 = 5$) $M_2 = N/n_2 = 15/5 = 3$
(Find the inverse of M_i) i.e y_1, y_2

check CRT: $\gcd(n_1, n_2) = 1$; $\gcd(2,3) = 1$ true ✓ CRT exists i.e one solution

Construct the equation:
$x = a_1 M_1 y_1 + a_2 M_2 y_2 \pmod N$
$= 2(5) y_1 + 3(3) y_2 \pmod N$

$M_1 y_1 \equiv 1 \bmod n_1$: $5 \cdot y_1 = 1 \bmod 3$
$\gcd(5,3)$: $5 = 3(1) + 2$; $3 = 2(1) + 1$; $2 = 1(2) + 0$
$1 = 3 - 2(1)$
$1 = 3 - 1(5 - 3(1))$
$1 = 3 + 3(1) - 1(5)$
$1 = 3(2) - 1(5)$
$5 \cdot (-1) = 1 \bmod 3$
$5 \cdot (2) = 1 \bmod 3$ ✓
$y_1 = 2$

$M_2 y_2 \equiv 1 \bmod n_2$: $3 \cdot y_2 \equiv 1 \bmod 5$
$\gcd(5,3)$: $5 = 3(1) + 2$; $3 = 2(1) + 1$; $2 = 1(2) + 0$
$1 = 3 - 2(1)$
$1 = 3 - 1(5 - 3(1))$
$= 2(3) - 1(5)$
$\equiv -1 \pmod 5$
$-1 + 5 = 4$
$y_2 = 4$

$= 2(5)(2) + 3(3)(4) \bmod 15$
$= 20 + 36 \bmod 15$
$= 56 \bmod 15$ $\quad 56 = 3 \cdot 15 + 11$
$= 11 \bmod 15$
Unique solution is $x = 11$

→ Algorithm Gauss's Algorithm : The solution x to the simultaneous congruences in the Chinese remainder theorem may be computed as $x = \sum_{i=1}^{r} a_i N_i M_i \bmod n$
where $N_i = n/n_i$
$M_i = N_i^{-1} \bmod n_i$
$O((\lg n)^2)$ bit operations

eg: $x \equiv 3 \pmod 7$ $\quad x \equiv 7 \pmod{13}$
check CRT exists
$\gcd(3,7)$ should be 1 $\quad \gcd(n_1, n_2) = 1$
$7 = 3(2) + 1$ ✓
$3 = 1(3) + 0$

$x \equiv 3 \pmod 7$ $\quad a_1 = 3$, $n_1 = 7$ $\quad N = n_1 n_2$ $\quad M_1 = N/n_1 = 91/7 = 13$
$x \equiv 7 \pmod{13}$ $\quad a_2 = 7$, $n_2 = 13$ $\quad N = 7 \cdot 13 = 91$ $\quad M_2 = N/n_2 = 91/13 = 7$

$M_1 y_1 = 1 \bmod n_1$: $13 \cdot y_1 = 1 \bmod 7$
$\gcd(13,7)$: $13 = 7(1) + 6$; $7 = 6(1) + 1$; $6 = 1(6) + 0$
$1 = 7 - 6(1)$
$= 7 - 6(13 - 7(1))$
$= 7(2) - 13$
(-1)
$y_1 = 7 + (-1) = 6$

$M_2 y_2 = 1 \bmod n_2$: $7 \cdot y_2 = 1 \bmod 13$
$\gcd(13,7) = 1$
$13 = 7(1) + 6$; $7 = 6(1) + 1$; $6 = 1(6) + 0$
$1 = 7 - 6(1)$
$= 7 - 6(13 - 7(1))$
$= -13 + 2(7)$
$y_2 = 2$

$x = a_1 M_1 y_1 + a_2 M_2 y_2 \bmod N$
$= 3(13)(6) + 7(7)(2) \bmod 91$
$= 234 + 98$
$332 \bmod 91$
$59 \bmod 91$

Fact: $\gcd(n_1, n_2) = 1$ ⇒ unique solution $x \equiv a \pmod{n_1}$, $x \equiv a \pmod{n_2}$ ⇒ $x \equiv a \pmod{n_1 n_2}$

Multiplicative group of $\mathbb{Z}_n$ is $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a,n) = 1\}$
eg → Find the multiplicative group of $\mathbb{Z}_{10}$ i.e $\mathbb{Z}_{10}^*$
→ $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ → Numbers in $\mathbb{Z}_{10}$
→ filter for numbers relatively prime to 10 (factors of 10 are 2, 5)
$\gcd(9,10) = 1$ in
$\gcd(2,10) = 2$ out
$\gcd(3,10) = 1$ in
$\gcd(4,10) = 2$ out
$\gcd(5,10) = 5$ out
$\gcd(6,10) = 2$ out
$\gcd(7,10) = 1$ in
$\gcd(8,10) = 2$ out
$\gcd(9,10) = 1$ in
$\therefore \mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$

order of the multiplicative group of integers modulo n, denoted by $\mathbb{Z}_n^*$ or U_n
$\phi(n)$ Euler's totient function ← counts the number of positive integers less than n that are relatively prime to n
$|\mathbb{Z}_n^*| = \phi(n)$
$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$

eg: $\mathbb{Z}_{12}^*$ i.e find no. of relative prime number in $\mathbb{Z}_{12}^*$
$n = 12$
1st prime factorisation of n:
$12 = 2^2 \cdot 3$
factors are 2 and 3
$p_1 = 2$, $p_2 = 3$
$\phi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$
this find the elements also!
$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$
for element to be in $\mathbb{Z}_{12}^*$ has to be relative prime to n
$\gcd(1,12) = 1$ in
$\gcd(2,12) = 2$ out
$\gcd(3,12) = 3$ out
$\gcd(4,12) = 4$ out
$\gcd(5,12) = 1$ in
$\gcd(6,12) = 6$ out
$\gcd(7,12) = 1$ in
$\gcd(8,12) = 4$ out
$\gcd(9,12) = 3$ out
$\gcd(10,12) = 2$ out
$\gcd(11,12) = 1$ in.

$\phi(n)$ multiplicative group $\mathbb{Z}_{23}^* = \{1, 2, 3 \ldots\}$
$\gcd(e, 23) = 1$
$\gcd(1, 23) = 1$
$\mathbb{Z}_{23}^* = \{1, 2 \ldots$
$(2, 23) = 1$
$(3, 23) = 1$

$k \cdot 23 = 1 \bmod 22$

$\mathbb{Z}_{23} = \{1, 23, 47, 5, 61, 7, 8, 9, 10, 11 \ldots\}$ 22

order of group n
$\phi(n)$
$\mathbb{Z}_n^* = \{1, 2 \ldots$
$\mathbb{Z}_{23}^* = \{1, 2 \ldots$
ormw

gcd(6,12) = 6 out
gcd(7,12) = 1 in
gcd(8,12) = 4 out
gcd(9,12) = 3 out
gcd(10,12) = 2 out
gcd(11,12) = 1 in.

$\mathbb{Z}_{12}^* = \{1,5,7,11\}$ and $\phi(12) = 4$ ✓

Let $n \geq 2$ be an integer
i) Euler's theorem: if $a \in \mathbb{Z}_n^*$ then $a^{\phi(n)} \equiv 1 \pmod n$

ii) if n is a product of distinct primes
$r \equiv s \pmod{\phi(n)}$? special case of Euler's theorem & little theorem
then $a^r \equiv a^s \pmod n$

Let p be prime
1) Fermat's theorem: if $\gcd(a,p)=1$ $a^{p-1} \equiv 1 \pmod p$
2) If $r \equiv s \pmod{p-1}$ then $a^r \equiv a^s \pmod p$
3) $a^p \equiv a \pmod p$

order of group = $|\mathbb{Z}_n^*|$
order of element = $\text{ord}(a)$

Def: $a \in \mathbb{Z}_n^*$, the order of a, denoted by $\text{ord}(a)$, is a least positive integer k such that $a^k \equiv 1 \pmod n$

eg: $\mathbb{Z}_{10}^*$ find $\text{ord}(3)$
$a^k \equiv 1 \pmod n$
$3^k \equiv 1 \pmod n$
for k=1 $3^1 \equiv 3 \bmod 10$ 3 ✗
for k=2 $3^2 = 3 \cdot 3^1 \bmod 10 \equiv 9 \bmod 10 = 9$
for k=3 $3^3 = 3 \cdot 3^2 \bmod 10 \equiv 3 \cdot (9 \bmod 10) = 27 \bmod 10 = 7$
for k=4 $3^4 = 3 \cdot 3^3 \bmod 10 = 3 \cdot 7 \bmod 10 = 21 \bmod 10 = 1$ ✓ stop
k=4
$\text{ord}(3) = 4$

$\text{ord}(5)$ in $\mathbb{Z}_{21}^*$
$a^k \equiv 1 \bmod n$
$5^k \equiv 1 \bmod 21$
k=1 $5^1 \bmod 21$ 5
k=2 $5^2 \bmod 21$ 4
k=3 $5^3 = 5 \cdot 5^2 \bmod 21$
$= 5 \cdot 4$
$= 20 \bmod 21$ 20
k=4 $5^4 = 5 \cdot 20 = 100 \bmod 21 = 16$
k=5 $5^5 = 5 \cdot 16 = 80 \bmod 21 = 17$
k=6 $5^6 = 5 \cdot 17 = 85 \bmod 21 = 1$

Key observation: lagrange's theorem
Notice that every order in the table $\{1,2,3,6\}$ is a divisor of the group order, $|\mathbb{Z}_{21}^*| = 12$. This is illustration of Lagrange's theorem the fundamental theorem in group theory which states that the order of any element in a finite group must divide the order of the group.
$|\mathbb{Z}_n^*|$ ← order of group
$\text{ord}(a)$ ← order of element

p_1, p_2 are prime factor of n

$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots$

$\text{ord}(a)$ $a^k \equiv 1 \bmod n$

$\text{ord}(a) = \phi(n)$ then a is called as a generator or primitive element of $\mathbb{Z}_n^*$

If $\mathbb{Z}_n^*$ has a generator then $\mathbb{Z}_n^*$ is said to be cyclic

$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)$

$\phi(21) = 21 \cdot \left(1-\frac{1}{7}\right)\left(1-\frac{1}{3}\right)$

$= 21 \cdot \left(\frac{7-1}{7} \cdot \frac{3-1}{3}\right)$

$= 21 \cdot \frac{6}{7} \cdot \frac{2}{3}$

$\phi(21) = 12$

$\phi(n) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1)$

$N = p_1^{e_1} \cdots p_r^{e_r}$

$N = 72 = 2^3 3^2$

$\left(2^{3-1}(2-1)\right)\left(3^{2-1}(3-1)\right)$

$= 24$

very important

How to find $\mathbb{Z}_n^*$ is cyclic
if $\text{ord}(a) = \phi(n)$
(or) $a \in \mathbb{Z}_n^*$ if n is $2, 4, p^k, 2p^k$

$\phi(21) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)$

$21 \Rightarrow p\ q$

$\phi(21) = 21\left(1-\frac{1}{7}\right)\left(1-\frac{1}{3}\right)$

$= 21\left(\frac{2}{3}\right)\left(\frac{2}{3}\right)$

$= \frac{21}{3} \times 2 \times 2 = 12$

Properties of generators of $\mathbb{Z}_n^*$
i) $\mathbb{Z}_n$ has a primitive if and only if $n = 2, 4, p^k$ and $2p^k$ where p is an odd prime $k \geq 1$
ii) generator α is a generator of $\mathbb{Z}_n^*$ then $\mathbb{Z}_n^* = \{\alpha^i \bmod n \mid 0 \leq i \leq \phi(n)-1\}$
iii) Suppose that α is a generator of $\mathbb{Z}_n^*$. Then $b = \alpha^i \bmod n$ is also a generator of $\mathbb{Z}_n^*$ if and only if $\gcd(i, \phi(n)) = 1$
if $\mathbb{Z}_n^*$ is cyclic then the number of generators is $\phi(\phi(n))$
iv) $\alpha \in \mathbb{Z}_n^*$ is generator of $\mathbb{Z}_n^*$ if and only if $\alpha^{\phi(n)/p} \neq 1 \pmod n$ for each prime divisor p of $\phi(n)$

$\mathbb{Z}_n^*$ gcd(1,21)
$\mathbb{Z}_{21}$ 1 2 3 4 5 6 7 8 9 10 11 ...
1 1 3 1 1 3
$\mathbb{Z}_{21}^* = \{1, 2, 4, 5\}$

Quadratic residues modulo n or Square modulo n
a is said to be $\cdot$ $a \in \mathbb{Z}_n^*$
if $x^2 \equiv a \bmod n$

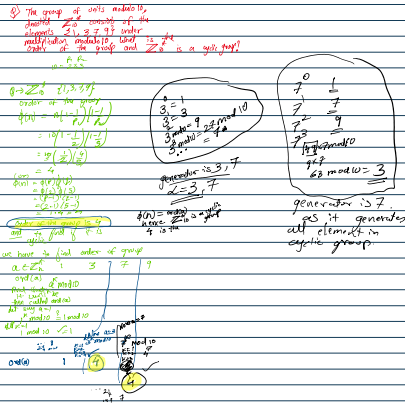
set of all quadratic residues modulo n is denoted by Q_n
and $\bar{Q}_n$ quadratic non-residues modulo n

eg: $\mathbb{Z}_8^*$
find Q_8 and $\bar{Q}_8$
$n = 8$
$x \equiv u^2 \bmod n$ $x \in \mathbb{Z}_8^*$
$\mathbb{Z}_8 = \{1,2,3,4,5,6,7\}$
$\mathbb{Z}_8^* = \gcd(1,n) = \gcd(1,8) = 1$
$\gcd(2,8) \neq 1$
$\therefore \mathbb{Z}_8^* = \{1,3,5,7\}$
Now take x, x^2, then mod 8
$x=1$, $x^2 = 1^2 = 1 \bmod 8 = 1$
$x=3$ $x^2 = 9$ $9 \bmod 8 = 1$
$x=5$ $x^2 = 25$ $25 \bmod 8 = 1$
$x=7$ $x^2 = 49$ $49 \bmod 8 = 1$
all unique numbers will be
$Q_8 = \{1\}$
$\bar{Q}_8 = \{3,5,7\}$

$\mathbb{Z}_{21}^*$	$x^2 \bmod 21$
1	1
2	4
3	9
4	16
5	4
6	
7	
8	
9	
10	

5 is repeated

Modular exponential can be performed efficiently with the repeated square and multiply algorithm (Alg. 2.143)



Modular exponentiation:

$5^{596} \bmod 1234$

Base (a) = 5
Exponent (k) = 596
Modulus (n) = 1234

K 596 can be written as a binary representation

$512 + 64 + 16 + 4$

$2^9 + 2^6 + 2^4 + 2^2$

in binary $K = (1001010100)_2$

means K has 1's at bits from K_0 to K_9 positions P_2, P_4, P_6, P_9

i	0	1	2	3	4	5	6	7	8	9
K_i	0	0	1	0	1	0	1	0	0	1

shows value of $A \leftarrow A^2 \bmod n$

A	5	25	625	681						
b	1	1	1	625	625					

$a^{2^i} \bmod n$

b: The multiply part is the running result, which is updated only when the bit K_i is 1

Initial $A = 5$, $b = 1$

bit i: $K_i = 1$, the $b \leftarrow b \times A \bmod n$

stays 1 if $K_i = 0$

$5^{596} \bmod 1234$

$5^{256} \bmod 1234 = 625$

$5^{512} \bmod 1234 = 625^2 \bmod 1234 = 390625 \bmod 1234 = 681$

$5^{1024} \bmod 1234 = 681^2 \bmod 1234 = 463761 \bmod 1234 = 625$

1013 ✓

it's still wrong without calculations

Algorithm in Z_n

- Computing multiplicative inverse in Z_n
- Repeated squared - and - multiply algorithm for exponentiation in Z_n
- Modular exponentiation

$596 \bmod 1234$

$a^k \bmod n$

initial phase	i	0	1	2	3	4	5	6	7	8	9
set	K_i	0	0	1	0	1	0	1	0	0	1
$a=5$	A	5	25	625	681						
$b=1$	b	1	1	625	625						

$K_0 = 0$, set $b \leftarrow 1$, $A \leftarrow a$

(or) $K_0 = 1$, set $b \leftarrow a$

$625^2 \bmod 1234$

390625

(1) what if $K_i = K_0 = 1$ then what will be the initialization

(2) what will the result

return b

$3^5 \bmod 7$

$5 = 2^0 + 2^1 + 2^2$

1 0 1

$K = 2$

$5 = 2^2 + 2^0$

i	0	1	2
K_i	1	0	1

A: 3 (A mod n)

b: 1

b

⇒ Jacobi symbol and Legendre symbol

→ Blum integer:
is a special composite number n that is a product of two distinct prime numbers, p and q where both primes

$n = p \times q$

$p \equiv 3 \pmod 4$

$q \equiv 3 \pmod 4$

$pq = 21 = 3 \times 7$

2·4·6

Blum integers $n = pq$

groups:

identity element in additive group is 0
identity element in multiplicative group is 1

$(G, *)$

A group G is cyclic if there is an element $\alpha \in G$ such that for each $b \in G$ there is an integer i with $b = \alpha^i$

Such an element α is called a generator of G

order of a cyclic group: $(p-1)$

Z_{19}^*, $p = 19$; $p - 1 = 18$ order (n)

$Z_{19}^* = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\}$

gcd (1, 19) = 1
gcd (2, 19) = 1
gcd (3, 19) = 1
gcd (4, 19) = 1
gcd (

$Z_{19}^* = \{1, 2, \ldots 18\}$

order = 18

Schnoor Signature

FOR-RSA

SK, m

results into different signature

how many

multiplicative group Z_7^*

1. what is the order of the group (n)?
   - $n = p - 1 = 7 - 1 = 6$
2. list all the possible subgroup orders
   - $Z_7^* = \{1, 2, 3, 4, 5, 6\}$
   - 6 divisor 6/1, 6/2, 6/3, 6/6
3. Given that $\alpha = 3$ is a generator of Z_7^* find the subgroup of order 2

Subgroup	Generators	Order
$\{1, 6\}$	6	2
$\{1, 2, 3, 4, 5, 6\}$	2, 5	3, 6

$\alpha = 3$ (generator of main group)
$d = 2$ order of subgroup
$n = 6$ order of group Z_7^* (group size)

we will calculate the generator for this specific subgroup using $3^{n/d}$

$3^{6/2} = 3^3$

$3^3 \bmod 7$ ⇒ $b = \alpha^i \bmod n$

6

So 6 is the generator of subgroup

to find subgroup

$6^1 \bmod 7 = 6$, $6^2 \bmod 7 = 1$

Z_{19}^* $n - 1 = 18$ order of group = 18

$n = p - 1$

$n = 23 - 1$

$= 2 \cdot 3 \cdot 3$

The setup
$\alpha = 3$
$d = 2$
$n = 6$ $(p-1)(7-1)$

The seed	order
Find the 'seed' generator.	1
We use the formula	2
exponent = Total order (n) / Target order of α	3

$3^{6/6} \bmod 7$

generator = $\alpha^{n/d}$

$= 3^{6/6} = 3^1 = 3$

generate the list

$3^1 \bmod 7 = 3$
$3^2 \bmod 7 = 2$
$3^3 \bmod 7 = 6$
$3^4 \bmod 7 = 4$
$3^5 \bmod 7 = 5$
$3^6 \bmod 7 = 1$

$$S = (Z_{31}^{*}, \times)$$

odd (2)

$\phi(22)$: $n = p_1 \times p_2 = 2 \times 11$ $\quad \phi(p) = p - 1$

$\phi(mn) = \phi(m) \times \phi(n)$

$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$

$= 22\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{11}\right)$

$= 22\left(\frac{2-1}{2}\right)\left(\frac{11-1}{11}\right)$

$= \frac{22}{11}\left(\frac{1}{2}\right)\left(\frac{10}{11}\right)$

$= 10$

$\alpha =$

$59 =$

$2 | 59 \quad (n-1)$

$59 =$

$Z_{59} = \{0, 1, \ldots, 58\}$ — order of $Z_{59} = n - 1 = 58$

$\phi(n)$

$\phi(58) = \phi(2)\,\phi(29)$

$= n\left(1 - \frac{1}{p_1}\right)(1 - 1$

$\phi(n) =$ no. of generators

(gen) $\alpha^{\phi(n)} \equiv 1 \bmod n$

$\alpha^{1} \bmod n$

$\alpha^{2} \bmod 100$

$\alpha^{3} \bmod 100$

$\alpha^{4} \bmod 100$

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

$\alpha^{20} = 1$

$\alpha^{?} =$

Z_{10}^{*}

$\alpha =$ $10^2/4$

* Lectures :- Elgamal encryption

public key encryption scheme

Let $G_q = \{g^0, g^1, \ldots g^{q-1}\}$ be a cyclic group of order q

Next :- exponent x used to generate G_q are in $\{0, \ldots q-1\}$

For any $h \in G_q$ there exists a unique solution $x \in \{0, \ldots q-1\}$ such that $g^x = h$

Taking log on both side to base g $\quad \log_g g^x = \log_g h$ $\quad x \log_g g = \log_g h$ $\quad x = \frac{\log h}{\log g}$

x is discrete logarithm of h with respect to g i.e $x = \log_g h$

since DL problem is assumed to be hard it can be used to generate cryptographic private/public key

$sk \in \{1, \ldots q-1\}$

public $pk = g^{sk}$

Key generation

$x \in \{1, \ldots q-1\}$ — public key : Pick random x — then $y = g^x$ $\quad pk = y = g^x$

private key $SK = x$

public key $(Pk) = g^x = y$ | Private key (x)

Encryption

Input message m as an element in G_q

Pick random $r \in \{0, \ldots q-1\}$ compute $c_1 = g^r$

Compute c_1 and c_2 $\quad c_2 = y^r \cdot m$

$c_2 =$ (public key^r) $\cdot m$

output cipher text $c = (c_1, c_2)$

Decryption

Take cipher text $c = (c_1, c_2)$ and private key $sk = x$

output $m = c_2 / c_1^x$

$= y^r \cdot m / g^{rx}$

$= (g^x)^r \cdot m / g^{rx}$

$= m$

Following Yeamini Week 8

$\phi(N)$

Z_{72}^{*}

72

$2^3 \cdot 3^2$

$p^{e_1} \cdot p^{e_2}$

$2 | 72$

$3 | 36$

$2 | 12$

$2 | 6$

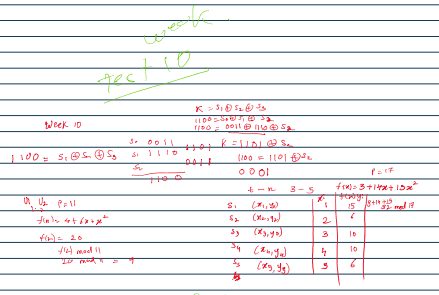
3

1

$(1-\frac{1}{2})(1-\frac{1}{3})72$

RSA encryption

study → Application of Integer factorisation problem



RSA encryption

study → Application of Integer factorisation problem

Textbook RSA encryption Scheme

SK (private Key) SK = (N, d)

PK (public Key) PK = (N, e)

m message

$c = m^e \bmod N$

$C = 2157^{318} \bmod 17$

$72 = 2^3 \cdot 3^2$

$p^{e_1} \cdot p^{e_2}$

$72\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)$

$72 \times \frac{2-1}{2} \times \frac{3-1}{3}$

$\frac{72}{12} \times \frac{1}{2} \times \frac{2}{3}$

24

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ $\gcd(a, 7) = 1$, $1 \bmod 7$

Is it cyclic?

No. of generator

Assume

$g = 1$

$1^k \equiv 1 \bmod 7$

How to check if the group is cyclic

$n = 2$

$n = 4$

$n = p^k$

$n = 2p^k$

$g^{\frac{\phi(n)}{p}} \not\equiv 1 \bmod n$

$\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$

$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$

$p = 3$ $3^2 \in \mathbb{Z}_9$ is cyclic

$\mathbb{Z}_9$ $n = 9$, $p = 3$, $p = 3$

$\phi(n) = 3 \cdot 3$

$= 9\left(1-\frac{1}{3}\right)\left(1-\frac{1}{3}\right) = 9\left(\frac{2}{3}\right)\left(\frac{2}{3}\right)$

unique primes for orders to

$n\left(1-\frac{1}{3}\right) = 9\left(1-\frac{1}{3}\right) = 3 \times 2 = 6$

$g \in \mathbb{Z}_n^*$

to call it cyclic there has to be an element which belong to $\not\equiv 1 \bmod N$

$a^k \bmod 9$

$1^k \bmod 9$ ×

$2^k \bmod 9$

$2^1 \bmod 9 = 2$

$2^2 \bmod 9 = 4$

$2^3 \bmod 9 = 8$

$2^4 \bmod 9 = 7$

$2^5 \bmod 9 = 5$

$2^6 \bmod 9 = 1$ $K = 6$

$3^k \bmod 9$

$3^1 \bmod 9 = 3$

$4^k \bmod 9$

$4^1 \bmod 9 = 4$

$4^2 \bmod 9 = 7$

$4^3 \bmod 9 = 1$

$5^k \bmod 9$

$5^1 \bmod 9 = 5$

$5^2 \bmod 9 = 7$

$5^3 \bmod 9 = 8$

$5^4 \bmod 9 = 4$

$5^5 \bmod 9 = 2$

$5^6 \bmod 9 = 1$

$G = \{2, 5\}$

$4^3 \bmod 9$

$3^3 \bmod 9$

$3^2 \bmod 9$

$16 \bmod 9 = 7$

$7 \neq 7$

$28 \bmod 9 \neq 1$ ×

$\phi(n) = 6$

prime {2, 3}

$3^6 \neq 1$

$g^2 \bmod 9 \neq 1$

$g^3 \bmod 9$

$g \in \mathbb{Z}_n^*$

very

imp

order of the group = m

Number of generator = $\phi(m)$

generator in the group is found using following step

1) find $\phi(n)$

2) find the prime divisors of $\phi(n)$

3) check the elements g $g^{\frac{\phi(n)}{\text{prime}}} \not\equiv 1 \bmod n$

also found using Euler theorem

$G = \mathbb{Z}_8^*$

order of the group G

Using Euler Totient function

$\phi(n) \cdot \phi(15) = \phi(m \cdot n) = \phi(m) \cdot \phi(n)$

$= \phi(5) \cdot \phi(3)$ ... $\phi(p) = p^{k-1}$

$= (5-1)(3-1)$

$= 4 \cdot 2 = 8$

$p_1 = 3^1$ $p_2 = 5^1$

$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)$

$= 15\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 15\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 8$

2) Determine if the group is cyclic.

→ to determine group is cyclic

∴ atleast one element $g \in \mathbb{Z}_n^*$ such that it finds all element in $\mathbb{Z}_n^*$

$\mathbb{Z}_{15}^* = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$

$\gcd(a, 15) = 1$ $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$g = 2$ $2 \bmod 7 = 2$

$2^2 \bmod 7 = 4$

$2^3 \bmod 7 = 1$

$2^4 \bmod 7 = 2$

$2^5 \bmod 7 = 4$

$2^6 \bmod 7 = 1$

order of element g g

$d = 1$

$d = 2$ 2^3

$d = 3$ 2^2

$d = 4$

$d = 6$ 2

$g = 2$ $\mathbb{Z}_7^*$ $\{1, 2, 3, 4, 5, 6\}$

$\phi(n) = 7\left(1-\frac{1}{7}\right)$

$= p - 1$

$= 6$

cyclic

$g \not\equiv 1 \bmod N$

$g \not\equiv 1 \bmod 7$

Can you identify any element $x \in \mathbb{Z}_7^*$ whose order is 6? that element must be a generator?

→ $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

prime divisor = 7

$\phi(n) = 6$

$x^6 \equiv 1 \bmod 7$ $6 = \frac{\phi(n)}{d}$

$K = s_1 \oplus s_2 \oplus s_3 \oplus s_4 \oplus s_5$

= 01001 } 10011
11010
00101 10110
01011 11101
11011 00110

00110

t out of n
4 out of 4

Z_7 p = 7

$f(x) = 2x^3 + 6x^2 + 3x + 4$

$s_1 = f(1) = 2 + 6 + 3 + 4 = 15 \bmod 7$

$f(2) = 2(2)^3 + 6(2)^2 + 3(2) + 4 = 16 + 24 + 6 + 4$

$f(3) = 2(3)^3 + 6(3)^2 + 3(3) + 4 = 16 + 54 + 9 + 4$

$f(4) = 2(4)^3 + 6(4)^2 + 3(4) + 4 = 128 + 96 + 12 + 4$

4 – 5

n – n
t o n

$s_1 \oplus s_2$

$K = s$

x_1, y_1	(1, 1)
x_2, y_2	(2, 1)
x_3, y_3	(3, 2)
x_4, y_4	(4, 2)

t = 4

$f(x) = f_0 + xf_1 + x^2 f_2 + x^3 f_3$

$f_i = \sum_{i=1}^{t} x_i \lambda_i(x)$

$\lambda^{i=1}(x) = \prod_{j=1, j \neq i}^{t} \frac{x - x_j}{x_1 - x_j}$

$\lambda_{i=1}(x) = \frac{x - x_2}{x_1 - x_2} \cdot \frac{x - x_3}{x_1 - x_3} \cdot \frac{x - x_4}{x_1 - x_4} =$

$\lambda_{i=2}(x) = \frac{x - x_1}{x_2 - x_1} \cdot \frac{x - x_3}{x_2 - x_3} \cdot \frac{x -}{x_2}$

$\lambda_{i=3}(x) = \frac{x - x_1}{x_3 - x_1} \cdot \frac{x - x_2}{x_3 - x_2} \cdot \frac{x -}{x_3}$

$\lambda_{i=4}(x) = \frac{x - x_1}{x_4 - x_1} \cdot \frac{x - x_2}{x_4 - x_2} \cdot \frac{x - x_3}{x_4 - x}$

$f(x) = \sum_{i=1}^{t} y_i \lambda_i(x)$

$= y_1 \lambda_1(x) + y_2 \lambda_2(x)$

$= 1\, \lambda_1(x) + 1\, \lambda_2$

$-6x^3 + 54x^2 - 156x + 144 + 2x^3 - 6x^2$

2&9 $\frac{64}{9}$

7^{+4}

4^9

$7^k \bmod 9$

$7^1 \bmod 9$ 7
$7^2 \bmod 9$ 4
$7^3 \bmod 9$ 1
$7^4 \bmod 9$

X

$8^k \bmod 9$

$8^1 \bmod 9 = 8$
$8^2 \bmod 9 = 1$
$8^3 \bmod 9 = 8$
$8^4 \bmod 9$

X

function $\phi(n)$

a, b ...

n) then g is said to be a generator

$= 1$

$\equiv 1 \pmod 7$

$\equiv 0 \pmod 7$

$\equiv 2 \pmod 7$

$S_2 \oplus S_4 \oplus S_5$

S

$S_2 \oplus S_3 \oplus S_4$

$x+4$

$$\frac{x-2}{1-2}\cdot\frac{x-3}{1-3}\cdot\frac{x-4}{1-4} = \frac{x-2}{-1}\cdot\frac{x-3}{-2}\cdot\frac{x-4}{-3} = \frac{(x-2)(x-3)(x-4)(-6)}{6}$$

$$(x^2-5x+2x+6)(x-4)(-6)$$

$$(x^3-3x^2-2x^2+6x-4x^2+12x+8x-24)(-6)$$

$$(x^3-9x^2+26x-24)(-6) \qquad -6x^3+54x^2-156x+144$$

$$x_4 = \frac{x-1}{2-1}\cdot\frac{x-3}{2-3}\cdot\frac{x-4}{2-4} = \frac{x-1}{1}\cdot\frac{x-3}{-1}\cdot\frac{x-4}{-2} = \frac{(x-1)(x-3)(x-4)(2)}{2}$$

$$(x^2-3x-x+3)(x-4)(2)$$

$$(x^3-3x^2-x^2+3x-4x^2+12x+4x-12)(2)$$

$$2x^3-16x^2+38x-24$$

$$x_4 = \frac{x-1}{3-1}\cdot\frac{x-2}{3-2}\cdot\frac{x-4}{3-4} = \frac{x-1}{2}\cdot\frac{x-2}{1}\cdot\frac{x-4}{-1} = \frac{(x-1)(x-2)(x-4)(-2)}{2}$$

$$(x^2-2x-x+2)(x-4)(-2)$$

$$(x^3-2x^2-x^2+2x-4x^2+8x+4x-8)(-2)$$

$$(x^3-7x^2+14x-8)(-2) \qquad -2x^3+14x^2-28x+16$$

$$= \frac{x-1}{4-1}\cdot\frac{x-2}{4-2}\cdot\frac{x-3}{4-3} = \frac{x-1}{3}\cdot\frac{x-2}{2}\cdot\frac{x-3}{1}$$

$$= (x-1)(x-2)(x-3)\,6$$

$$= (x^2-2x-x+2)(x-3)(1)$$

$$= (x^3-3x^2-x^2+3x-3x+6x+3x-6)(6)$$

$$= (x^3-4x^2+11x-6)(6)$$

$$6x^3-48x^2+66x-36$$

$$+ y_2\lambda_3(x) + y_4\lambda_4(x)$$

$$(x) + 2\lambda_3(x) + 2\lambda_4(x)$$

$$+38x-24 \quad + \quad -2x^3+12x^2-28x+16 \quad + \quad 6x^3-48x^2+66x-36$$

Can you identify any element $x \in \mathbb{Z}_7^*$ whose order is 6? that element must be a generator?

→ $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ prime divisor = 7 $\phi(n) = 6$

$x^6 \equiv 1 \bmod 7$ ↓ $6 = \frac{\phi(n)}{d}$

who are are generators of this group

1^6 $\boxed{2}^6$ $64 \bmod 7 = 1$

7

Find inverse (5) 72

gcd =

$72 = 5(14) + 2$

$5 = 2(2) + 1$

$2 = 1(2) + 0$

$1 = 5 - 2(2)$

$= 5 - 2(72 - 5(14))$

$= 5(1 + 28(5))$

29

PK n, e $(91, 5)$

SK $= (91, 29)$

$m = 4$ $4^5 \bmod 91$ $c = 23$

dec

$23^{29} \bmod 91$

ElGamal encryption

$c_1 = g^y$

$c_2 = y^m \bmod p$

public α y p q

(c_1, c_2)

Computational diffie-Hellman problem

(N, e) public

(N, d) private

$c = m^e \bmod N$

$m = c^d \bmod N$

$(m, 5)$

PK

48, 15

gcd

$48 = 15(2) + 3$

$15 = 48(0)$

$15 = 3(5) + 0$

5 mod 7

$\gcd(5, 7) = 1$

$7 = 5(1) + 2$

$5 = 2(2) + 1$

$1 = 5 - 2(2)$

$1 = 5 - (7 - 5(1))(2)$

$= 5(3)$

(d, x, y)

$\gcd(13, 11)$

$13 = 11(1) + 2$

$11 = 2(5) + 1$

$2 = 1(2) + 0$

$1 = 11 - 2(5)$

$1 = 11 - (13 - 11(1))(5)$

$= 11 + 5(11) - 13(5)$

$= 6(11) - 13(5)$

$1, 6, -5$

d, x, y

$(1, -5, 6)$

$\gcd(a, N) = 1$ there exists integer

$\gcd(a, b) = 1$

$48, 15 = 3$

$5 \bmod 7 = 3$

$(1, -5, 6)$

Week 8

Part 1 → 6, 7

Part 13 → CCA attack.

→ Complaint

Consistency should be maintained in symbolic representation.

Pg: 18 Week 8

It read it should be y

N: m

P: m

RSA: N, e, m

N, e

$c = m^e \bmod N$

$= 5^3 \bmod 55$

$= 125 \bmod 55$

15

25
5
125
55
2
110
15

$\phi(21) = 7 \times 3$

$= \phi(7)\phi(3)$

$= (7-1)(3-1)$

$= 6 \times 2$

$= 12$

$\phi(11) = p-1$

$= 10$

$\phi(10) = 2 \times 5$

$= 4 \times 2$

$\gcd(21, 31) = 1 \bmod 31$