Remarks on functions & Sets

Def A set is just a collection.
we denote sets by $X, Y, \{\dots\}$

Example
$X = \{A, B, \dots\}$, $X = \longleftrightarrow = \mathbb{R}$

Suppose X & Y are sets
Def. a function from X to Y denoted by the rule $f: X \to Y$

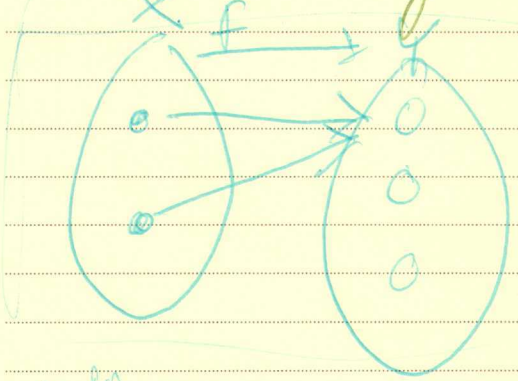
$\{A, B, \dots\}$
$\downarrow$ $\downarrow$
$\{0, \dots 25\}$
$f(A)$ $f(B)$

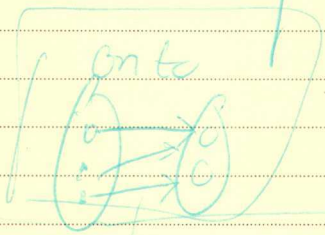
Consider the rule
$f: X \to Y$
$\{A, B, \dots Z\} \to \{0, 1, \dots\}$
x maps to y

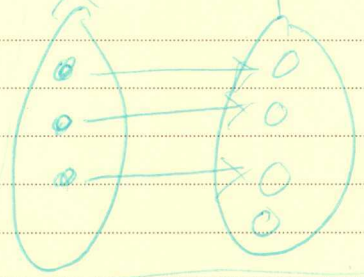
f u A gives $\forall x \in X$ a unique $y \in Y$

f u A we denote by $y = f(x)$

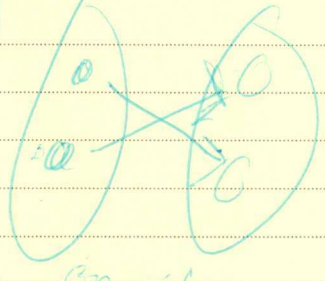
Set theory







Bijection
Invertible
one-to-one



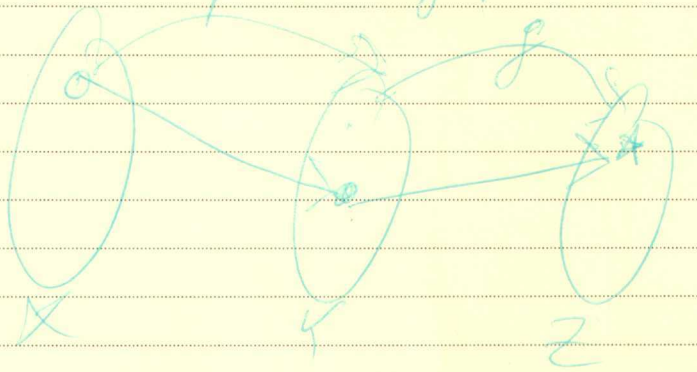
Def
We say that the function is one-to-one
if $\forall x_1 \neq x_2 \in X$ for all in
we have $f(x_1) \neq f(x_2)$

We say that the function is onto
if $\forall y \in Y$, $\exists x \in X$ s.t. $f(x) = y$

We say that the function f is invertible (bijective)
if f is one-to-one / onto

The following are equivalent TFAE

Suppose $X \xrightarrow{f} Y \xrightarrow{g} Z$.



Def: The composition of g and f denoted by $g \circ f$ is given by $X \xrightarrow{g \circ f} Z$

$$(g \circ f)(x) = g(f(x)) = z$$

When Bijective

$$(g \circ f) = \text{Identity} \iff id(x) = x$$

(a) for: $f: X \to Y$

f is bijection (invertible, $\exists!$ inv)

(b) $\exists g: Y \to X$ s.t. $\begin{cases} f \circ g = id_Y \\ g \circ f = id_X \end{cases}$

in this case g is the inverse of f

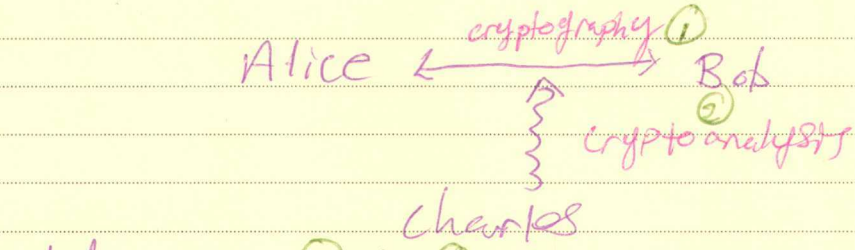
$g = f^{-1}$

① Introduction

Q - What is this about? A: Safe communication

Suppose Alice & Bob went to have a talk.
Suppose Charles might be in the vacinity.
How can Alice & Bob exclude Charles

(map)



Crytology = ① + ②

Example:

① Caesar Cipher – a type of shift cipher

Definition: ① The mapping of letters to another (not itself) — BIJECTIVE (one-to-one/onto) means it has an inverse

$$e_3 : \{A, B, \ldots\} \longrightarrow \{A, B, \ldots\}$$

This is an example of: encryptive transformation

The inverse map d_3 is an example of decryptive transformation

note $d_3 \circ e_3 = id$ ✱ Identity

Remark: In the same way we could use

$$(e_K, d_K), \quad K = 0, \ldots, 25$$

K - "the Key"

TÜL

Notation A cryptosystem is ....

P - set of plain texts
C - set of Cipher texts
K - set of keys

and ....

$\forall x \in K$, two functions

$e_K : P \to C$ encryption
$d_K : C \to P$ decryption

Such that (S.t.o.) $d_K \circ e_K = id_P$

Remark: If our message

$m = x_0, x_1, x_2 \ldots x_K$

$e_K(M) = e_K(x_0) \ldots e_K(x_K)$

$d_K(M)$

(II) Block Cipher
Apply encoding (= encryption) to blocks of letters

e.g. $P = C = \{A, B \ldots\}$

e will shift 1st, 3rd ... letters by one
& 2nd, 4th, ... letters by two

(III) Stream Ciphers
The encryption transformation of a symbol depends on it's position (and maybe the previous symbols)

e.g. $P = \{A, B \ldots\} = C$

e(i-th letter in i pos.) = Shift it the i^{th} prime = encryption of the i^{th} letter to the i^{th} prime

TÜL

Continued →

Remember Integer ($\mathbb{Z}, \mathbb{Z}^+$)

(continued)

e(VENI VIDI VICI)

Fact: Primes can be > 26. ∴ we must use Pi mod 26

VENI VIDI VICI

→ 2,3,5,7 11,13,17,19 23,3,5,11

→ XHSP GVUJ ILHT

Pseudo-random-sequence

(IV) Public-Key System

Knowing K = encryption Key or e_K = encryption transformation

to arrive at the decryption (Key) = d_K

Fact! Numbers are easier than letters

Eg.

A	B	...	Z
↓	↓		↓
0	1		25

Congruences:

Suppose $N > 0$

~~Definition~~ Definition:

Suppose $a, b \in \mathbb{Z}$

Let $a \equiv b$ to be modulo N

$a \equiv b \pmod{n}$

if $b - a$ is a multiple of N

Fact

(i) $a \equiv a \pmod{N}$, $\forall a \in \mathbb{Z}$

(ii) $a \equiv b \pmod{N} \rightarrow b \equiv a \pmod{N}$, $\forall a, b \in \mathbb{Z}$

(iii) $a \equiv b \pmod{N}$ $\forall b \equiv C \pmod{N} \rightarrow a \equiv C \pmod{N}$

TOL

Fix $N > 0$

Fact! $\forall a \in \mathbb{Z}$, $\exists$ $0 \leq b \leq N-1$

S.t. $a \equiv b \pmod N$

Integers mod N

$\mathbb{Z}_N = \{0, \ldots, N-1\}$

Integer Modulo N

Let $a, b \in \mathbb{Z}$

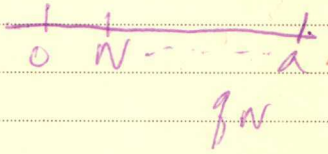
$a \equiv b \pmod N \longrightarrow N \mid a-b$

Fact $\forall a \in \mathbb{Z} \exists!\ b$ s.t. $0 \leq b \leq N-1$

Suppose $a \geq 0$, $N \geq 1$

$\exists!\ q, b \geq 0 \in \mathbb{Z}$ s.t. $a = qN + b$

$0 \leq b \leq N-1$



Show uniqueness
Show existence
$\star\star$

In particular we have a natural mod N map

$\mathbb{Z} \longrightarrow \mathbb{Z}_N$

$a \longmapsto b$ (unique $b \in \mathbb{Z}_N$ $a \equiv b \pmod N$)

For $x, y \in \mathbb{Z}_N$

$x +_N y = x + y$

$N = 26$

$13 +_{26} 14 = 1$

Also:

For $x \in \mathbb{Z}_N$

$-x$ is the unique A

$y \in \mathbb{Z}_N$ s.t. $x +_N y = 0$

$x -_N y = x +_N (-y)$

TÜL

Example: Shift Cipher

$P = C = K = \mathbb{Z}_{26}$

$e_K(x) = x +_N K$

$d_K(x) = x -_N K$

$K \in K$

Operation $\mathbb{Z}_N = \{0, \ldots, N-1\}, N \geq 2$

add $x +_N y = x + y \pmod N$ definition

multiply $x *_N y = x \cdot y \pmod N$

Properties of addition

associative $(x +_N y) +_N z = x +_N (y +_N z)$

commutative $(x +_N y) = y +_N x$

$x +_N 0 = x$

additive inverse $x \in \mathbb{Z}_N \; \exists! \, y \in \mathbb{Z}_N$ s.t. $x +_N y = 0$

associativity of multiplication

$(x \cdot_N y) \cdot_N z = x \cdot_N (y \cdot_N z)$

Commutativity of multiplication

$x \cdot_N y = y \cdot_N x$

$x \cdot_N 1 = x$

Distributive aka addition & multiplication

$x \cdot_N (y +_N z) = x \cdot_N y +_N x \cdot_N z$

$\mathbb{Z}_N = \{0, 1, \ldots N-1\}$

Remark: If $0 \neq x \in R$ Then $\exists! \, y \in R$ s.t. $x \cdot y = 1$

(namely inverse of x x^{-1})

$\mathbb{Z}_4$:

	0	1	2	3
0				
1				
2	0	2	0	2
3				

Let $x \in \mathbb{Z}_N$
We say that x is invertible
If $\exists . y \in \mathbb{Z}_N$ s.t.

$x \cdot_N y = 1$

In this example y is the inverse of x modulo N denoted by x^{-1}

$\mathbb{Z}_3$:

$\cdot_N$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Fact $\mathbb{Z}_N$ a field $\leftrightarrow$ N is prime

Def^n: $\mathbb{Z}_N$ is called a field if every $0 \neq x \in \mathbb{Z}_N$ is invertible

$(\mathbb{Z}_N)^\times = \{$ all $x \in \mathbb{Z}_N$ which are invertible

$(\mathbb{Z}_N)^\times = \{$ all $x \in \mathbb{Z}_N$ s.t. x ... has no non-trivial common prime factors $\}$

$(\mathbb{Z}_N)^\times = (\mathbb{Z}_N)^\times$

Affine Cipher

$\perp$ & $\gcd\{x, y\} = 1$

2/3/2022

$P = C = Z_N$

$a, b \in Z_N$

$e_{a,b}(x) = a \cdot x + b$

recall the mapping $x \mapsto a \cdot x$ on Z_N is 1-1 iff $a \in (Z_N)^*$

So the affine cipher is $P = C = Z_N$ and $K = (Z_N)^* \times Z_N$

and for each $a \cdot (a, b)$

$e_{a,b}(x) = ax + b$

$d_{a,b} = e^{-1}_{a,b}$

$(Z_N)^* = \{a \in Z_N \ (\text{has no trivial common prime factors})\}$

Fact $\subseteq a \in (Z_N)^* \rightarrow$

$\rightarrow \exists y$ s.t. $a \cdot_N y = 1$ in $Z_N \rightarrow$

$\rightarrow \exists k \in \mathbb{Z}$ s.t. $ay + kN = 1$

So $\nexists$ p that divides a and N

We want to show

$a \notin (Z_N)^* \Rightarrow a \notin \{a \perp b\}$

Suppose $N \geq 2$

then $\exists!$ primes $p_1, \dots, p_k$ and integers $m_1, \dots, m_k$	s.t. $N = p_1^{m_1} \cdots p_k^{m_k}$

Let our unit $a \in (\mathbb{Z}_N)^\times$

$a \in (\mathbb{Z}_N)^\times$, so $\exists 0 \leq x < x' \leq N-1$

s.t. $a \odot x = a \odot x'$

$\iff a \odot (x' - x) = 0 \iff \exists k > 0$ s.t. $a \odot (x' - x) = k_N$

Decompose $N = p_1^{m_1} \cdots p_k^{m_k}$

by the fact $\exists i: 1 \leq i \leq k$ s.t.

$p \mid a \rightarrow a \in p$

Euclid Algorithm

Given $y = a \odot x + b$

$x = a \odot (y - b) = d_{a,b}(y)$

Compute a

Def Suppose $u, v \in \mathbb{Z}$

The greatest common divisor (gcd)

$\exists x, y \in \mathbb{Z}$ s.t.

$x \cdot u + y \cdot v = \gcd(u, v)$

In particular if $a \in (\mathbb{Z}_N)^\times$ then

$\exists x, y \in \mathbb{Z}$ s.t.

$x \cdot a + y_N = 1$

TOL

greater common divisor

Algorithm (euclid)

Assume $u \geq v \geq 0$ then $gcd(u,v) = \begin{cases} u, & \text{if } v = 0 \\ gcd(v, u \bmod v), & \text{if } v > 0 \end{cases}$

$$gcd(u,v) = \begin{cases} 0, & u = v = 0 \end{cases}$$

$$a \in (\mathbb{Z}_N)^* \iff gcd(N, a) = 1$$

Fact: $\exists\, x, y \in \mathbb{Z}$ s.t.

$$\boxed{x \cdot u + y \cdot v = gcd(u,v)} \Longrightarrow g \bmod N = a^{-1} \in \mathbb{Z}_N$$

↳ Assume $u \geq v \geq 0$

compute $gcd(u,v) = \begin{cases} \end{cases}$

$O(\log_v(u))$

Recursion:

Since $v > 0$

Let $u = q \cdot v + r$, $0 \leq r < v$

by inductive assumption

$x' \cdot v + y' \cdot r = gcd(v, r)$

① $gcd(u,v)$

② $gcd(v,r)$

③ $= x' \cdot v + y' \cdot r$

$= y' \cdot u + (x' - y' \cdot q) \cdot v$

Alphabetic Cipher

Shift Cipher

$P = C = \mathbb{Z}_N$

$e(x) = x + b$

$e_{a,b}(x) = a \cdot x + b$ Affine Cipher

Hill Cipher $P = C = \mathbb{Z}^N$

Recall $M = (m_{ij}) \in M_{N,N}(\mathbb{Z}_N)$

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} \in \mathbb{Z}_N^n$$

$$Mx = \begin{pmatrix} m_{11}x_1 + \cdots + m_{1N}x_N \\ \vdots \\ m_{N1}x_1 + \cdots + m_{NN}x_N \end{pmatrix}$$

Fact

$e_M : \mathbb{Z}_N^N \to \mathbb{Z}_N^N$

$x \longmapsto Mx \cdot N$

is invertible $\iff M$ is Mvertible

if $\exists B \in M_N(\mathbb{Z}_N)$ s.t. $A \cdot B = B \cdot A = \text{Identity}$

Notated $B = A^{-1}$

Hill Cipher $M \in K$

$e_M(x) = Mx$

Fact: To compute M^{-1} out of M

G.E. $\hookrightarrow$ Gaussian Elimination

order of N^3 operations

Example: $N = 26$ $M_{2\times 2} = \begin{pmatrix} 25 \\ 307 \end{pmatrix} \in M_2(\mathbb{Z}_{26})$

Fact $A \in M_N(\mathbb{Z}_N)$ is invertible iff

$$\det(A) \in (\mathbb{Z}_N)^*$$

Do Hill cipher in blocks in blocks of 2:

R V T H S T R J K E S O U T

17 20 19 7 18 19 17 8 9 10 4 18 19 20 19

4 92

$$\begin{bmatrix} 2 & 5 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 17 \\ 20 \end{bmatrix} = \begin{bmatrix} 134 \\ 191 \end{bmatrix}$$

$(2 \cdot 17 + 5 \cdot 20) \bmod 26 = 4$

(134)

$(3 \cdot 17 + 7 \cdot 20) \bmod 26 = 9$

(191)

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad M^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$[A \mid I_N] \longrightarrow [I_N \mid A^{-1}]$$

Permutation Matrices $M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \in M_3(\mathbb{Z}_N)$

Notes $(M^t \cdot M = I_3) \Longrightarrow M^t = M^{-1}$

$$\begin{pmatrix} 0&1&0 \\ 0&0&1 \\ 1&0&0 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_3 \\ x_1 \end{pmatrix}$$

definition
a matrix $M \in M_{n\times n}(\mathbb{Z}_2)$

Def A matrix $(M_{ij}) = M \in M_{n\times n}(\mathbb{Z}_2)$
is called permutation matrix
(PM) if $m_{ij} \in \{0,1\}$ $\forall\ 1 \le i,j \le n$
and it has only one non-zero entry / 1 in every column.

Note: If M is PM and $m_{ij}=1$, the

$$i\begin{pmatrix} \cdots & j & \cdots \end{pmatrix}\begin{pmatrix} x_1 \\ \vdots \\ x_j \end{pmatrix} = \begin{pmatrix} \\ x_i \\ \\ \end{pmatrix}$$

FACT: If M is PM $\Rightarrow \exists M^{-1} = M^t$
proove the identity transformation

Why?
$M^t \circ M = I_{n\times n}$

Construction $e = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ $1 \le j \le n$

take e_j then $\exists\ 1 \le i \le n$ s.t. $m_{ij} = 1$

e_j $\quad M^t \circ e = e_j$

$M^t e = e$

Perm permutation

Def A permutation of $\{1, \dots n\}$ is a bijection

$\sigma : \{1, \dots n\} \to \{1 \dots n\}$

Notation all permutation

S_n = all permutation

$\#(S_n) = n!$

Q. P_n set of $n \times n$ Perm

$\#(P_n) = ?$

Fact $\#(P_n) = n!$

Claim 2. Natural bijection

$S_n \longrightarrow P_n$

$\sigma \in S_n$ define $M(\sigma)$

Example

$\sigma \in S_3$

$\sigma(1) = 3, \sigma(2) = 1$

$\sigma(3) = 2$

$M(\sigma) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$

$M(\sigma) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma(1)} \\ \vdots \\ x_{\sigma(n)} \end{pmatrix}$

Claim

$M(\sigma)$ is a $P(n)$

and $\sigma \mapsto$ is a bijection of S_n to P_n

2 | 17 | 22

Hill Cipher

$e_A : \mathbb{Z}_{26}^n \longrightarrow \mathbb{Z}_{26}^n$

$x \longmapsto Ax$

A is invertible $d_A(y) = A^{-1} \cdot y$

Permutation Matrices (PM)

$M = (m_{ij})$, $m_{ij} \ldots \in \{0, 1\}$

& in every column and row

$\exists!$ non-zeroth entry

Fact $\exists\, m^{n+1}$, $M^{n+1} = M^1$ — proof of Identity/Inverse

Hill Cipher Setup $P = C = \mathbb{Z}_{26}^n$, $K = P_n$

$e_M(x) = Mx$

Transposition Cipher

$P = C = \{A, B, \ldots\}$ ← this set

Key-Space = permutations of

Key-Word: BOMBE → 1 5 4 2 3

Ordered by alphabet

Now, suppose we have the following message

CRYPTOGRAPHY IS FUN

A^T → C O H [illegible] S Y T P F Z Y R I X G M

Note:
1. map table
2. decrypt task by multiply inverse

$\begin{pmatrix} 1&2&3&4&5 \\ 1&5&4&2&3 \end{pmatrix} \to g^{-1} = \begin{pmatrix} 1&2&3&4&5 \\ 1&4&5&3&4 \end{pmatrix}$

TÜL

CRYPTOGRAPHY IS FUN

Bob

CRYPT
OGRAP
HYISF
UNxyz

COHURGYWYRTxPASyTPFz

$$\begin{pmatrix} 1&2&3&4&5 \\ 1&5&4&2&3 \end{pmatrix} \cdot \sigma^{-1} = \begin{pmatrix} 1&2&3&4&5 \\ 1&4&5&3&4 \end{pmatrix}$$

another way

$$\sigma \rightsquigarrow M(\sigma)\begin{pmatrix} x_1 \\ \vdots \\ x_5 \end{pmatrix} = \begin{pmatrix} x_{\sigma(1)} \\ \vdots \\ x_{\sigma(5)} \end{pmatrix}$$

$$M(\sigma) = \begin{pmatrix} 1&0&0&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&1 \\ 0&0&1&0&0 \\ 0&1&0&0&0 \end{pmatrix} \in M_5(\mathbb{Z}_{26}) = ?$$

$M(\sigma)(e_2) = e_5$

Alice

Suppose we have

CRYPTOGRAPHY IS FUN XYZ

$x_1\ x_2\ x_3\ x_4 \cdots \cdots \cdots x_{26}$

$$M(\sigma) = \begin{pmatrix} x_1 & x_1' & x_1'' & x_1''' & x_1'''' \\ \vdots & & & & \\ x_5 & \cdots & \cdots & \cdots & x_5'''' \end{pmatrix} = \begin{pmatrix} R_1 \\ R_2 \\ R_3 \\ R_4 \\ R_5 \end{pmatrix}$$

R_1 R_2 R_3 R_4

Null Space (A)

$$\text{Neg}^T \begin{pmatrix} R_1 \\ R_2 \\ R_3 \\ R_4 \\ \vdots \end{pmatrix}$$

New topic Introduce Charles

Cryptoanalyst

(e_k) = "Alice" → Charles → (d_k) = "Bob"

What can Charles do?

Assumption:

① Charles knows the system
↳ P, C, K

$\forall k$ knows e_k and from it d_k

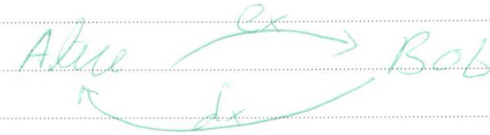
* All security in the Key's!

Let's assume further $(d_k \circ e_k)(m)$ = "noise"

$K' \neq K$

Cryptanalysis 2 22 22

$P = C$ $k \in K$



Charles (CA)

Assumptions: CA knows P, C, K "key space" e_k, $k \in K$, d_k (all sec in key)

Charles does not know ~~little~~ k

Q
1. How long will encryption e_k be secure?
2. What is the cost to recover/compute k?

Attack Models: ~~three~~ standards of stability:

(a) Ciphertext only
Charles knows some of y_n & x_n
$y_n = e_k(x_n)$, $x_n = d_k(y_n)$
~~and other~~ and wishes to get k

(b) → knows plain text "random text"
matched pairs $(x_n, y_n) \ldots (x_n, y_n)$

(3) Charles can choose pairs

Goal: #1 Estimate probability of success of various methods.

#2 Estimate average time until given method is successful

Randomness enters in:

(1) Messages are not deterministic

(2) Keys are (usually) chosen in a random manner

(3) C.A. can choose key at random

Probability

Ω finite/countable — Omega "sample space"

"probability"

$P: \Omega \longrightarrow \mathbb{R}$

(i) $\forall x \in \Omega \quad 0 \leq P(x) \leq 1$

(ii) $\sum_{x \in \Omega} P(x) = 1$

Def: The pair (Ω, P) is the probability space

Example

coin #1 $\Omega = \{h, t\}$

$P(h) = 1/2 \quad P(t) = 1/2$

dice #2 $\Omega = \{1, \ldots, 6\}$, $P(i) = 1/6$

Def. A subset

$X \subseteq \Omega$ is called an event

with $X \subseteq \Omega$

we determine its probability to be

$P(X) = \sum_{x \in X} P(x)$

Note

$$0 \leq Pr(X) \leq 1, \quad Pr(\Omega) = 1,$$

$$Pr(\emptyset) = 0$$

def:

① $Pr(X^c) = 1 - P(X)$ — Complement

② $Pr(X \cup Y) \leq P(X) + P(Y)$ — Union

③ $Pr(X \cap Y) =$ — Intersection

Assumption on P, C, K, e_k, d_k

$\forall x \in P, \; k' \neq k \quad d_{k'}(e_k(x)) =$ "noise"

Model problem

n $(n-1)$

Random Replacement → Place trial back in batch @ each pull

How many draws on average do we expect we randomly draw the blue dot?

Expectation

#1 Def: a function $f: \Omega \to \mathbb{R}$ is called random variable (RV)

#2 Def: If f is a RV on (Ω, P) the

$E(f) = \sum_{x \in \Omega} f(x) P(x)$ is the expected value or the expectation of f

Note: $E(\alpha f + \beta g) = \alpha E(f) + \beta E(g)$

$\forall \alpha, \beta \in \mathbb{R}, \; f, g$ RV

Suppose f_1 is RV on (Ω_1, P) & f_2 RV on (Ω_2, P_2) -

Consider

$(\Omega_1 * \Omega_2, P_1 * P_2)$

Defn We say that if f_1 and f_2 are independent if

$\forall a, b \in \mathbb{R}$

$$Pr\left(\left\{(x,y) \in \Omega_1 * \Omega_2 \;\middle|\; \begin{matrix} f_1(x) = a \\ f_2(y) = b \end{matrix}\right\}\right)$$

$$= Pr\left(\left\{x \in \Omega_1 \mid f_1(x) = a\right\}\right) \cdot Pr\left(\left\{y \in \Omega_2 \mid f_2(y) = b\right\}\right)$$

Note $0 \le \hat{P}(x) \le 1$ $\hat{P}(\Omega) = 1$

$\hat{P}(\emptyset) = 0$

Note: ① $\hat{P}_\bullet(x^c) = 1 - P(x)$

② $\hat{P}$

H.W

$\Omega_1 = \Omega_2 = \Omega = \{u, d\}$

$$\xi_u(x) = \begin{cases} 1 & x = u \\ 0 & x = d \end{cases}$$

$$\xi_d(y) = \begin{cases} 0 & y = u \\ 1 & y = d \end{cases}$$

① Show ξ_u ξ_d are indepin

② & ξ_u ξ_d are not indep

Probability

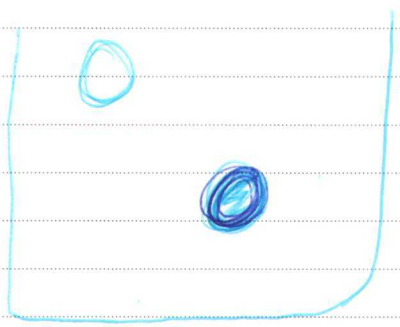
2/24/22

P, C, K $\quad e_K, d_K$

assume: $K' \neq K$ $\quad (d_K \circ e_K)(x_0, \ldots, x_n) =$ "noise"

↑ brute force the key

Model for Search



n "white select"

$n-1$ "Black select"

Search w/ replacement - keeps the ball in the bunch after checking.

* Replacement:

Ω = sequences

$\underbrace{(bbbb\ldots bw)}_{x}$ $(l-1)$

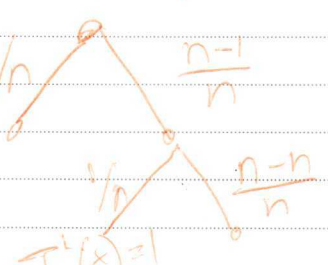
"Probability of x" $P(x) = \left(\frac{n-1}{n}\right)^l \cdot \frac{1}{n}$

$T(x)$ = length (x)

$E(T) = \sum_{x \in \Omega} T(x) \cdot P(x)$

* Claim: $E(T) = n$

Computation by decision tree



$E(T) = 1 \cdot \frac{n}{n} + \left(1 + E(T)\right)\left(\frac{n-1}{n}\right)$

$E(T) = E(T)$

TOL

$$E(T) = 1 \cdot \frac{1}{n} + (1 + E(T)) \frac{n-1}{n}$$

$$\Rightarrow E(T) = n$$

No Replacement

Example $n = 4$

bbbw = 1/4
bbwb = 1/4
bwbb = 1/4
wbbb = 1/4

$$E(T) = \frac{1}{4}(1 + 2 + 3 + 4)$$

$$= \frac{1}{4} \cdot \frac{4(4+1)}{2} = \frac{5}{2}$$

In general... you can see

$$E(T) = \frac{1}{n}(1 + \cdots + n)$$

$$= \frac{1}{n} \cdot \frac{n(n+1)}{2} = \frac{n+1}{2}$$

Consequences

(a) For security, better to have a large set of keys.

(b) unless otherwise stated

We assume that a random choice of the key to test.

what is a good method to choose

of elements in various Key sets

- Shift cipher

$\#(K) = N$

$P = C = \mathbb{Z}_N$, $K = \mathbb{Z}_N$

$e_K(x) = x + K$

- Affine cipher

$P = C = \mathbb{Z}_N$, $K = (\mathbb{Z}_N)^* \times \mathbb{Z}_N$

How many $\#(\mathbb{Z}_N)^* = \varphi(N)$

↑ Euler φ function

Fact 1: $\varphi(N) = N \cdot \prod_{p \mid N} (1 - \frac{1}{p})$

Fact 2:

$$\varphi(N) \geq C \cdot \frac{N}{\log(\log(N))}$$

in particular $\frac{N^2}{\log(\log(N))}$

5/11/2022

$\#(K) = N!$ General Substitution cipher

(permutation cipher)

$P = C = \mathbb{Z}_N$, $K = S_N = \text{perm}(\mathbb{Z}_N)$

$\pi \in K$: $e_\pi(x) = \pi(x)$

$\#(K) = N!$

$\approx \sqrt{N} \cdot \frac{N^N}{e^N} \sim N^N$

Wigenere (polyalphabet)

$P = C = \mathbb{Z}_N^n$

$K = \mathbb{Z}_N^n$

$K = (b_1, \dots, b_n) \in \mathbb{Z}_N^n$

$e_{b_1, b_n}(x_1, \dots, x_N) =$

$(x_1 + b_1, \dots, x_N + b_N)$

Vectors of length $N - \mathbb{Z}^N$

$\neq (x \cdot y)$

$\#(x) \neq \#(y)$

Hill Cipher

$P = C = \mathbb{Z}_N^m$ $\quad K = GL_n(\mathbb{Z}_N)$

$\#(K) = ?$

$e_M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

Continued

3 | 1 | 22

$$\#\left(GL_2\left(\mathbb{Z}_{\mathbb{R}}\right)\right)$$

$$\begin{matrix} v_1 \\ v_2 \end{matrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{s.t.} \quad v_1, v_2 \text{ are lin. Ind.}$$

Fact: $\#\left(GL_n\left(\mathbb{Z}_N\right)\right) = N^{n^2}\left(\prod_{p \mid N}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right)\cdots\right)$

Fact (Jordan)

$$\leq \#(K) \leq N^{n^2}$$

$$c \cdot \frac{N^{n^2}}{\log(\log(n))} \leq \#(K)$$

Summary

Ciphers	$\lfloor \log_2(\#(P)) \rfloor$	$\log_2(\#K)$
Shift	$\log_2(N)$	$\log_2(N)$
Affine	$\log_2(N)$	$2\log_2(N)$
Permutation	$\log_2(P)$	$\approx P\log_2(P)$
Vigenere	$n \cdot \log_2(N)$	$N\log_2(N)$
Hill Cipher	$n \cdot \log_2(N)$	$N^2\log_2(N)$

$$\prod_{i=1}^{n} x_i = x_1 \cdot x_2 \cdots x_n$$

Recall

$$\#\left(GL_n\left(\mathbb{Z}_p\right)\right)$$

Chosen Plain Text

CA - Charles
↳ Choote

$x_1 \dots x_N \in P$

$e_K(y_1 \dots y_N) \in C$

goal find K

measure cost of attack by # of plain text required

Shift Cipher

If $y = x + K \Rightarrow K = y - x$

1 - plain text ☒

Affine Cipher

$y = ax + b$

If $x = 0$, $b = y$

If $x = 1$, $y = a + b$
$a = y - b$

2 - plain text ☒

Vigenere Cipher

blocks size N

$e_{b_1 \dots b_N}(x_1 \dots x_N) = (x_1 + b_1 \dots x_n + b_N)$

Substitute $(a, \dots, g)$

1 - block ☒

Permutation Cipher

$P = C = \mathbb{Z}_N$, $K = Perm(\mathbb{Z}_N)$

$y = \pi(x)$

to get π from pairs $(x_1, y_1, \dots)$

N-plaintext ☒

Hill Cipher

$(P = C = \mathbb{Z}_N^n)$ $K = GL_n(\mathbb{Z}_N)$

$e_M(\vec{x}) = M \cdot \vec{x}$

note!

$M \cdot e_j = g_j(M)$, n vectors ☒

Fact

① Given the system the method we saw are optimal for known plaintext attacks

② In all methods the size of a ciphertext is the size of the plaintext.

③ permutation cipher needs a lot of plaintext.

☆☆ Known plain-text attacks

CA - gets (in a random manner)

several matched pairs

(x_{n+1}, y_n) — goal $K = ?$

Known plain+ext attack

Assumption: CA gets $\exists \cdot (x_1, y_1) \dots$ at random and try to get $K \in K$

Model: CA gets $x_1, x_2 \dots$

Each x is random variable

$$P_r(X_1 = a_1, \dots, X_n = a_n) = \left(\frac{1}{\#(P)}\right)^n$$

Agreed: # of $x \in P$ required until CA gets Level-K is a random variable

Goal: Compute Expected Value of

① Shift Cipher

$$P = C = \mathbb{Z}_n, \quad K = \mathbb{Z}_n$$

$$y = x + K$$

$$K = y - x$$

a plain text is enough & 100% we know K

② Affine Cipher

$$P = C = \mathbb{Z}_n, \quad K = (\mathbb{Z}_n)^* \times \mathbb{Z}_n$$

$$e_{a,b}(x) = yx + b$$

What is the probability for x_1 and x_2 the difference is invertible? (How much time)

$$P_r(x_1 - x_2 \in (\mathbb{Z}_n)^*)$$

Suppose $(x_1, y_1), (x_2, y_2)$

$$y_1 = a \cdot x_1 + b$$

$$y_2 = a \cdot x_2 + b$$

$$= \begin{pmatrix} x_1 & 1 \\ x_2 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

can be computed explicitly

if and only if the det is invertible note: $\exists! \, a, b$ iff $x_1 - x_2 \in (\mathbb{Z}_n)^*$

Continued -

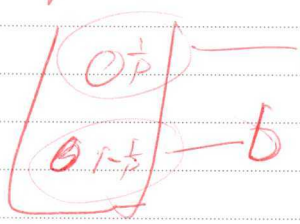
Fix $x_2 = 0$ now compute

$$\Pr(x_1 - x_2 \text{ is } (Z_N)^*) = \frac{N(P(N))}{N^2} = \frac{P(N)}{N}$$

$$\approx \frac{N}{\log(\log(N))} \cdot \frac{1}{N} = \frac{1}{\log(\log(N))}$$

$\Rightarrow$ expected number of trials (time pairs of plaintext need is $\log(\log(N))$)

Remark:



p = Exp. # appearance of (b/a)

General Substitution (Perm.) Cipher

$P = C = Z_N$, K = all permutations of Z_N

$\delta \in K$ $e_\delta(x) = \delta(x)$

to know δ exactly we need to get all of $x \in P$

Model Problem: we have N cards (unpermutated)

(Q) # of times to draw cards uniformly at random from till we expect to have drawn every card at least once

Fact: Expect # of time till we get each card once is at least $N \log(N)$

Vigenere Cipher

$$P = C = \mathbb{Z}_w^n, \quad K = \mathbb{Z}_w^n$$

$$(y_1, \ldots, y_n) = e_{b_1, \ldots, b_n}(x_1, \ldots, x_n)$$

If we have one block $(x_1, \ldots, x_n)$

$(y_1, \ldots, y_n)$

$\Rightarrow$ of text (and cipher)

$$\left.\begin{aligned} y_1 &= x_1 + b_1 \\ &\vdots \\ y_n &= x_n + b_n \end{aligned}\right\} \Longrightarrow \text{get } (b_1, \ldots, b_n)$$

Shift Cipher

$P = C = \mathbb{Z}_N \quad K = \mathbb{Z}_N \quad y = e_K(x) = x + K$

$P = (p_0, p_1, \ldots, p_{N-1})$

(A out of y computes:

$Q = (q_0, q_1, \ldots, q_{N-1})$ ~~take~~ $K \in K$

Compute $\forall x \in K$

$q_0(K) \ldots q_i(K) \ldots N-1$

$Q = (q_{-K}, q_{1-K}, \ldots, q_{N-1-K})$ $\to K \in K$ s.t.

$q_0 \sim p_0$

Soul, more sensitivity

Trig! "average frequency deterr…"

* χ^2 method

Consider $P = (p_0, \ldots, p_{N-1})$

$Q_{N-1} = (q_0^{(K)}, \ldots, q_{N-1}^{(K)})$

$$\|P - Q\|^2 = \sum_{i=0}^{N-1} \left(p_i - q_i^{(K)}\right)^2$$

$$= \sum_{i=0}^{N} p_i^2 + \sum (q_i^{(K)})^2 - 2\sum p_i q_i^{(K)}$$

constant

K time $=$ max $K \in K$

~~FFT~~ Define for P, Q

FFT can be done $O(n\log(n))$ $(P \star Q)(K) = \sum_{i=0}^{N-1} p_i \cdot q_i^{(K)}$

How ∧ on functions from Z_N to $\mathbb{R}$ called

$$f * g = \hat{f} \cdot \hat{g}$$

$O(3N \log(N))$

[Cipher-Text-Only] 3/7/2022

Assumption: $K' \neq K$

$d_{K'}(y_1)\, d_{K'}(y_2) \ldots d_{K'}(y_N)$ "

↳ is not a text of the language

P, C
$\mathcal{K}$
e_K
d_K

Example: English

E ~ 13%, T ~ 9% ....

Cipher-Text only Attack (shift Cipher)

$P = C = Z_N$, $K = Z_N$

$y = e_K(x) = x + K$

We have a vector of frequencies

$P = (p_0, p_1, \ldots, p_{N-1})$

Knowing: $y_1 \ldots y_N$

C_A makes another vector of frequencies on C

$Q = (q_0 \ldots q_{N-1})$

Next, $\forall_K \in K$: consider $Q^{(K)} = (q_K, q_{1+K} \ldots q_{N-1+K})$

Method: find the Kth $\sim K^{th}(-K)$?

$Q^{(K)} \cdot P$

$Q^{(k)} = (q_k, q_{1+k}, \dots, q_{W+1+k})$

actual:

Want to know $Q^{(k)} \sim P$

Method 1: Euclidean distance (correlation method)

note: $P > Q^{(k)} \in \mathbb{R}^N$ $(a-b)^2$

$$\|P - Q^{(k)}\|^2 = \sum_{i=0}^{n-1} \left(p_i - q_i^{(k)}\right)^2$$

$$= \sum_{i=0}^{N-1} p_i^2 + \sum_{i=0}^{W-1} \left(q_i^{(k)}\right)^2 - 2\sum_{i=0}^{W-1} p_i q_i^{(k)}$$

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

$$(P \star Q)(k) = \sum_{i=0}^{N-1} p_i \cdot q_i^{(k)}$$

$\max (P \star Q)(k)$ $k \in K$ ⇝ true key

Fact: Forward Transformation

This Optimization can be solved in $O(W \cdot \log(N))$ operations.

Idea: $\exists \hat{\cdot} : \mathbb{R}^N \to \mathbb{R}^N$ s.t. $P \star Q = \hat{P} \cdot \hat{Q}$ ($\mathbb{R}^N$)

Fact: This can be computed in $O(W \cdot \log(N))$

on Affine Cipher

$P = C = Z_N$, $K = (Z_N)^*$

$e_k(x) = ax + b$

$k \to (a, b)$

$P_{a,b}, Q = (q_0, q_1, \ldots, q_{N-1})$

$q_b \quad q_{a+b} \quad q_{a(N-1)+b}$

3/24/2022

Cipher Text Only Attack for Affine Cipher

$P = Z_N$, $C = Z_N$, $K = (Z_N)^* \times Z_N$, e_K, d_K

on plain text P = plain text

$y_1 \dots y_n$ $n > 0$

we have probability

$P = (P_0, P_1, P_2, \dots P_{N-1}) =$

and CA "crypt analyst" can compute

$Q = (q_0 \dots q_{N-1})$

we assume $n >>> 0$

$\exists!\ k \in K$ s.t. $Q^{(k)} = (q_{f_0}^{(k)}, \dots q_{f_{N-1}}^{(k)}) = f$

Goal: we want to find k_0

- Method 0: apply every k and verify $Q^{(k)} = f$
- Method 1: Find two sets of # q_i, q_j & P_i, P_j s.t. $q_i = P_i$, $q_j = P_j$

continue

$(\text{assume } i-j \in (\mathbb{Z}_N)^*) \wedge \exists!\, k \text{ s.t.}$

$$k(i) = i' \quad \& \quad k(j) = j'$$

we assume $(n \gg 0)$

$\exists!\, k_0 \in K$ s.t. (a,b)

$Q^{(k)}$

Goal: find $k \in K$ s.t.

$$Q^{(k)} \sim P_{N-1}$$

$$\|P-Q\|^2 = \sum_{i=0} (p_i - q_i^{(k)})^2$$

$$= \sum p_i^2 + \sum (q^{(k)})^2 - 2 \sum_{i=1}^{N-1} p_i q_i^{(k)}$$

$P \times Q$

$(P \times Q)_{(k)}$ maximum k

By FFT can be computed by

$O(\log(N) N^2)$ operations

Frequency Analysis

Cipher text only for Vigenere method

$P = C = Z_N^n$, $K = Z_N^n$

So correlation analysis can use method 0 or 1

Hill Cipher. ???

Shift Cipher $= n$

C-T-O Attack for Permutation Cipher

$P = Z_N = C$

$\#(K) = N!$

$K = \{ G_i : Z_N \to Z_N \text{ s.t. } G = G_{ij} \} = Perm(Z_N)$

From $y_0 \ldots y_n$ $n >> 0 \rightsquigarrow Q = (q_0 \ldots q_N)$

$\exists!\ G \in K$ s.t. $Q^{(G)} = (q_{G(0)}, q_{G(1)} \ldots q_{G(N-1)})$

$Q^{(G)} \sim D$

method

method 1: need at least N check. but assume = on of P & Q

method 2: correlation analysis and find G

$O(N!)$

Shannon Theory

Chapter #14

Question: In Cipher text only situation as a function of $n \to \infty$

$(y_1 \dots y_n \in C)$

How certain can we be about a RK we compute to be the true key?

Def of The Entropy of $p = \{p_i, i \in \Omega\}$

is $H(p) = -\sum_{i \in \Omega} p_i \log p(i)$

Remark:

(1) People think of H as measuring the uncertainty in random choice from Ω using $\{p_i\}$

(2) $\log = \log_2$ & people speak of a choice from Ω using p_i's as costing H bits of information per element of Ω

Example: If $\{p_i = \frac{1}{\#(\Omega)} \; \forall i \in \Omega$

then $H(p_{\text{information}}) = -\sum_{i \in \Omega} \frac{1}{\#(\Omega)} \log\left(\frac{1}{\#(\Omega)}\right)$

is Pr uniform $= -\log(\#(\Omega)) = \log(\#(\Omega))$

TOL

Fact: (a) Note! $H(p) \geq 0$

(b) $\max H(p) = \log(\#(\Omega))$

(c) $\delta_{i_0} = \{p_{i_0} = 1, p_i = 0 \; \forall i \neq i_0\}$

$\therefore H(\delta_{i_0}) = 0$

$-\sum_{i \in \Omega} p_i \log(p_i)$

Example: English alphabet

$N = 26 \quad \log(26) \approx 4.17$

Note: we can represent all letters using 5 bits

i.e. sequencing length of 5, 1 and 0

0 A = 00000
1 B = 00001
2 C = 00010
3 D = 00011
4 E = 00100
5 ⋮
25 Z = 11001

$H(p) = 4.18$

We'll see what this number means

How many bits of info. per letter exists for the english language? $N = 5$

Fact: $P_A = 3683/50{,}000$

$P_B = 487/50{,}000$

⋮

$P_Z = 49/50{,}000$

experimental

Data Compression

Fact: H controls the "measure of compressibility" of "language"

Eg. $\Omega = \{A, B, C, D, E\}$

Given $p_A = 0.05$, $p_B = 0.05$, $p_C = 0.1$, $p_D = 0.3$, $p_E = 0.5$

$H(P) = 1.78$

Consider the encoding

A	B	C	D	E
0000	0001	001	01	1
4	4	3	2	1

Note: no code word is a prefix of another code word.

$= 0.05 \times 4 + 0.05 \times 4 + 0.1 \times 3 + 0.3 \times 2 + 0.5 \times 1$

$= 1.8 \approx H(P) = 1.78$

Fact: $\exists$ encoding of A, B, C, D, E s.t. their average is $1.78 + \varepsilon$

Fact: For code s.t. average length $< H(P) - 1.78 \ldots$

Formal statement on this (continued)

Suppose (Ω, P) is a probability space (or "language")

Def. (i) A coding (or code) C for Ω is a mapping

$$C: \Omega \to \bigcup_{n \geq 1} \{0,1\}^n$$

(ii) A code C is called prefix if one-to-one no $C(x)$, $x \in \Omega$, is prefix of another $C(x')$, $x \neq x' \in \Omega$

(iii) the length of $n = l(x) = l(C(x))$ of a code word $C(x)$, $x \in \Omega$ is the unique n s.t. $C(x) \in \{0,1\}^n$

Definition "The Expected Value" $E(l)$

Consider l as a numerical random variable

$$l: \Omega \to \mathbb{R}$$

is called the expected length of C denoted, $L(C)$, $C: \Omega \to \bigcup_{n \geq 1} \{0,1\}^n$

i.e.

$$L(C) = \sum_{x \in \Omega} p(x) l(x)$$

Theorem $\exists$ a code C for Ω, s.t.

$$H(p) \geq L(C) < H(p) + 1, \text{ but } \exists C' \text{ s.t. } L(C') < H(p)$$

Compression Entropy Ω, $P=\{p_1, \dots p_N\}$

$H(p) = -\sum p_i \log(p_i)$ lower bound

Recall: a coding of Ω is a (1-1) mapping

$$C: \Omega \longrightarrow \bigcup_{n\geq 1} \{0,1\}^n$$

(lang.)

$$X \cup Y = \{z \mid \begin{matrix} z\in X \text{ or} \\ z \in Y \end{matrix}\}$$

p_x - probability of x

And we say that C is prefix code if no $c(x)$, $x\in\Omega$ is prefix of other $c(x')$ $x \neq x' \in \Omega$

And finally $n = l(x) = l(c(x))$ - the length of x (, it is the unique n s.t.

$$c(x) \in \{0,1\}^n$$

In particular

$$L(c) = E(l) = \sum_{x\in\Omega} p(x) l(x)$$

$l(c(x))$

is called the Expected length of C

Problem: what is the smallest possible $L(c)$, C runs over all possible codes for Ω?

Theorem: $\forall \varepsilon > 0$ $\exists$ a code $C: \Omega \to \bigcup_{n\geq 1} \{0,1\}^n$ s.t. $H(p) \leq L(c) < H(p) + \varepsilon$

& $\nexists$ code C s.t. $L(c) < H(p)$

Remarks: Denote

by C_{min} a code s.t.

$$\sum_{x \in \Omega} P(x) l(x) = L(C_{min}) = H(P) = \sum P(x) \log\left(\frac{1}{P(x)}\right)$$

to consider

(i) $\log\left(\frac{1}{P(x)}\right)$ as the arrangement bit of information content of $x \in \Omega$

(ii) $H(P)$ as the average information (Ω, P)

Huffman Code (~1950s)

$\Omega, P = \{P_1 \dots P_N\}$

Goal: Construct code which gives $L(C) = H(P)$

① take x_i & x_j with P_i, $x_1 \dots x_N$ smallest and "replace" them by a new letter (add to Ω) with probability

② $P(y) = P_i + P_j$

- Replace until only symbol remains

To do this process we build a binary tree

Leaves: original

after having the code,

path from the root of those leaves

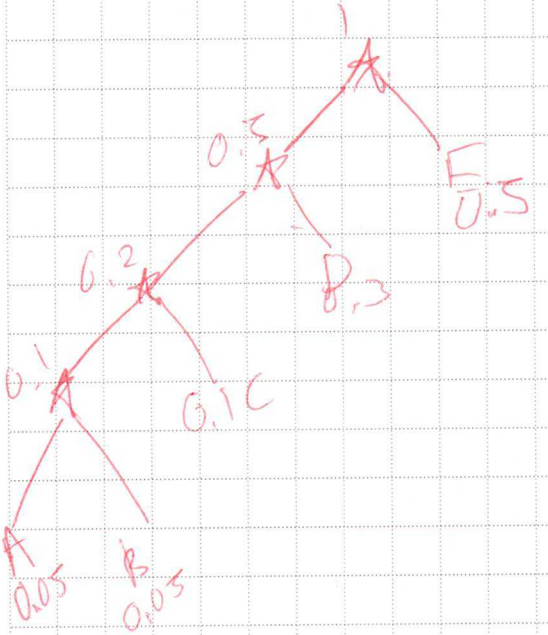
- write 0 for left move & 1 for right move

x_i x_0

Example

	A	B	C	D	E
p	.05	.05	.1	.3	.5

C is Huffman code:



$H(p) = 1.78$

L s.t.

$L(C) \leq 1.8$

A ~> 0000

B ~> 0001

C ~> 001

D ~> 01

E ~> 1

→ Shannon's info. theoretical approach to crypto

Q What is the (averaged) uncertainty about the key that remains after CA has seen n ciphertext symbols?

Shannon's Approach

"Everything is a random variable (in particular all sets are equipped with probability distributions)

cryptosystem

P, $P(x) = \text{Prob}(P = x)$

TÜL

4/5/2022

Shannon's Approach to Crypto

So $f(x): A \to B$ $\quad G(y): B \to A$

Strength Analysis- Motivation: How safe is it for to use $f(x)$ & $g(x)$.

Consider $\exists_{(a,b)} CA_{(a',b')} = (a,b) = k \in K$

Everything is a random variable

So if $\text{lets} \in P$ all lets have a probability distribution.

CRYPTO SYSTEMS

Plain Text P is a probability set denoted as

$\text{Prob}_P(x) = P(x)$ otherwise $\text{Prob}(P=x)$

$K \rightsquigarrow \text{Prob}_K$ $\quad C \rightsquigarrow \text{Prob}_C$

assume the following.

(1) P, K are independent defender

If we have probability distribution $\text{Prob}_{P \times K}$

and $\text{Prob}_{P \times K}(x, K) = \text{Prob}_P(x) \cdot \text{Prob}_K(x)$

So they're not related

(2) C is determined by P & K

(3) P is determined C & K

We Consider

$P_n \; x_1, x_2, \ldots x_N, x \in P$

$C_n \; y_1 \ldots y_n$

(continued)

Discovery of Shannon

4/5/2022

Definition: The Numerical Value

Bad notation:

$$E_n = H(P_N) + H(K) - H(C_n)$$

$$H(Prob_{P^n}) \quad H(Prob_K) \quad H(Prob_{C^n})$$

This is called

Key Equivocation Ambiguity

Remark: people think on E_N as the average uncertainty about the Key that remains after CA saw n of n symbols from C

More remarks:

(i) $n \to 0$: $H(K)$ - max uncertainty about Key.

$$E_0 = H(K)$$

(ii) By intuition:

Lemma $\lim_{n \to \infty} E_N \to 0$ can be proved □

(iii) In general it is difficult to compute $H(K)$ so E_N is also not so easy to compute E_N.

If suppose X, P_X Y, P_Y P_X & P_Y are indepent

i.e $P_{X \times Y}^{(x,y)} = P_X^{(x)} \times P_Y^{(y)}$

RSA Specifics

Key Computation

the modulus

1.) Choose two (large) primes compute $n = pq$

Modern computing looks for $N \geq \sim 2{,}000$ bits so factorization is out of range for most computers

(p) & (q) are 600 digits long

2.) Compute $\lambda = (p-1)(q-1)$ ← the totient

3.) Choose e s.t. $\gcd(e, \lambda) = 1$

Public Key is (n, e) encryption

4.) Compute the inverse of $e \bmod \lambda$

i.e. $de = 1 \bmod \lambda \rightarrow (n, d)$ secret decrypt Key

---

To encrypt a message m, compute $(m^e) \bmod n$

$(m^e) \bmod n = y$ ⇝ encrypted msg.

To decrypt an encrypted message y compute $(y^d) \bmod n$ ⇝ gives m back

---

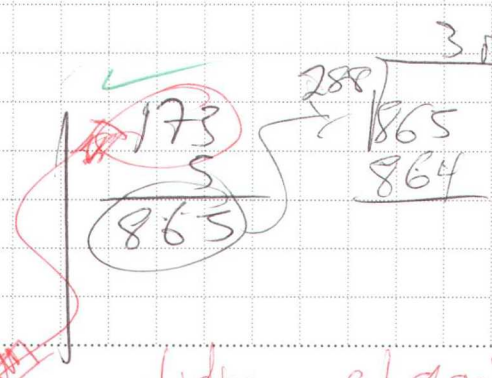
Ex: $p = 17$ $q = 19$ $17 * 19 = 323 = n$

$\lambda = (p-1)(q-1) = 16 * 18 = 288$

$e = 5$ $\gcd(5, 288) = 1$ ✓

Public Key $(323, 5)$

Decrypt secret $(323, 173)$

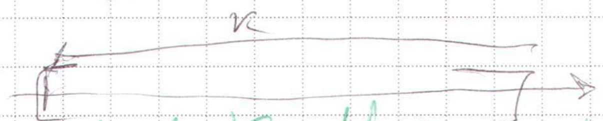


↑ Euclidean algorithm

Message $m = 200$

Encrypt $(200^5) \bmod 323 = 98 \rightarrow$ encrypt msg

Decrypt $(98)^{173} \bmod 323 = 200$



# of R that's inherited $\approx \frac{n}{\ln(n)}$

density is $\sim \log_n$

Trick: ← Binary ← base 2 10101101

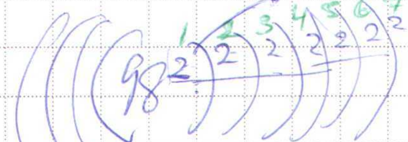
$2^7\ 2^6\ 2^5\ 2^4\ 2^3\ 2^2\ 2^1\ 2^0$

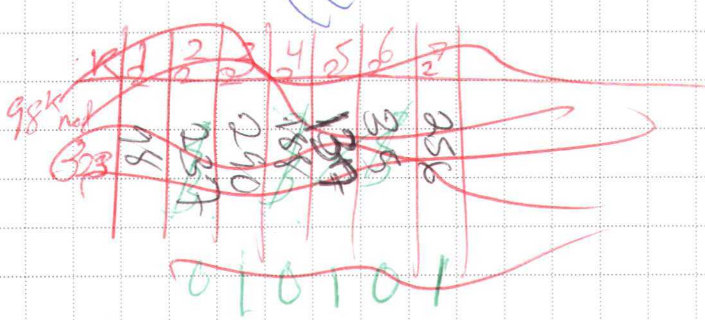
$173 = 128 + 32 + 8 + 4 + 1$

$\quad\ \ 2^7 \quad 2^5 \quad 2^3 \quad 2^2 \quad 2^0$

So $(98)^{173} =$

$98^{128} + 98^{32} + 98^{8} + 98^{4} + 98^{1}$





$98^k \bmod 323$

k	0	1	2	3	4	5	6	7
2^k	98	237	240	120	188	137	35	256
	1	0	1	1	0	1	0	1

$256 + 137 + 120 + 240 + 98 =$

Fermat's Little Theorem

If p is prime $a^p \equiv a \bmod p$ for $\forall a$

a	0	1	2	3	4	5	6
$a \bmod 7$	0	1	2	3	4	5	6

Proof: If $a \not\equiv 0$

$a \not\equiv 0$, then a is a UNIT (i.e. $\gcd(a,p)=1$)

$\exists\, b$ s.t. $ba \equiv 1 \bmod p$

$a^0 \equiv a \ (\circ b) \iff a^{p-1} \equiv 1 \bmod p$ □

Example

x	1	2	3	4	5	6
$a \circ x \bmod p$	3	2	2	5	1	4

we want to show

$3^6 \equiv 1 \bmod 7$

$3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4 = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$

$(3 \cdot 1)(3 \cdot 2)(3 \cdot 3) \ldots (3 \cdot 6) = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 6 \bmod 7$

$3^6 = 1 \bmod 7$ □

Putting it all together

Claim: RSA is correct, i.e. $(\text{decrypt})(\text{encrypt})(m) = m$

Proof: We are asking if $(m^e \bmod n)^d \bmod n = m$

LHS: $m^{de} \bmod n = m^{1+k\lambda}$

$= m \cdot (m^\lambda)^k \bmod n$

$= m \cdot (m^{(p-1)(q-1)})^k \bmod n \overset{?}{=} m$

Recall $de \equiv 1 \bmod \lambda$

$de = 1 + k\lambda$ $\exists k$

Continue →

Continued

Instead of checking LHS = RHS mod q

we'll check LHS = RHS mod p and LHS = RHS mod f } C.R.T.

If $m \equiv 0 \bmod p$

$m \equiv 0 \bmod \Rightarrow m^{p-1} \equiv 1 \bmod p$

$LHS = M\left((m^{p-1})^{q-1}\right)^k \equiv m \bmod p$

m^{p-1} : 1

Same for the RHS / f

Back to Shannon & Crypto

$y_1 \dots y_n$

$P_n = X \cdot X_2$

C_n

K

~~determine~~ detention $E_n = H(P_n) + H(K) - H(C_n)$

is called key ambiguity (equivocation)

Remark: we then on E_n is the average uncertainty about the key that remains after CA has seen n symbols of cipher text

Remark: we assume uniform prob

(i) $n = 0$, $E_0 = H(K) = \log(|K|)$

(ii) $E_n \xrightarrow[n \to \infty]{} 0$

~~Assumption~~ Definition

If P_X, P_Y are independent

$P(x,y) = P_X(x) \cdot P_Y(y)$

Then $H(P_{X+Y}) \geq H(P_X) + H(P_Y)$

Reasonable assumption

$H(P) = n \cdot H(P)$

Note: suppose $P = C$, $\#(P) = N$

$H(C_n) \leq \log(\#(C_n))$

$= n \cdot \log(\#(C))$

$\mathcal{E}_N = H(K) + H(P_N) - H(C_N)$

$\geq \log(\#(W_N)) W \cdot H(P) - n\log(N)$

Notation Tendency $\rightsquigarrow R = \log(N) - H(P)$

Compute

$\geq \log(\#(C_n)) n \cdot H(P) - n\log(N)$

determinism $= \log(\#(K)) - nR$

In Particular if $\mathcal{E}_N = 0 \Rightarrow n \geq \frac{\log(\#(K))}{R}$

"Normal security"

Remark: People think on U as the length n st beyond it the system is not safe anymore.

Examples: Biased random plain text on two symbols (Permutation Cipher on $\mathbb{Z}_2$)

$P = \{0, 1\}, \quad P(0) = p, \quad P(1) = q = 1 - p$

$K = \{id, \tau\}$ ($\tau(0) = 1$, $\tau(1) = 0$), $\quad P(id) = 1/2$, $\quad P(\tau) = 1/2$

$C = P$ — on the level of set

Goal: compute $E_n = H(C^n) - H(k) - H(c)$

$H(C^n) = ?$

Suppose $y_1 \dots y_n$ is a string with m 1's and $n-m$ 0's
→ the probability of getting a sequence

$$\frac{p^m \cdot q^{n-m}}{2} + \frac{p^{n-m} \cdot q^m}{2}$$

$$H(C^n) = -\sum_{y \in \{0,1\}^n} P_r(y) \cdot \log(P_r(y)) \rightarrow = \sum^{n} \binom{n}{m} \frac{p^m q^{n-m} + p^{n-m} q^m}{2} \log(\dots)$$

$$H(K) = \log(2)$$

$$H(P_N) = n \cdot H(1-p, p)$$

$$\geq -n\left(p\log(p) + q\cdot\log(q)\right)$$

Numerics

$p = .25, \quad q = 0.75$

E_0	$= .1$
E_1	$= .813$
E_2	$= 0.6681$
E_3	$= 0.385$
E_{10}	$= 0.163$
E_{20}	$= -0.03$
E_{50}	$= .0003$

Remark

$$U = \frac{\log(\#(K))}{R}$$

$$= \frac{1}{R} = 5.3$$

Shannon key Equivocation

$$\varepsilon_n \geq \log(\#(K)) - n$$

$$R = \log(K) - H(P)$$

$$\varepsilon_N = 0 \Rightarrow n \geq U = \frac{\log(\#K))}{R}$$

$$\varepsilon_n \quad \underbrace{\#(\log(K))}_{U}$$

Perfect Secrecy

def: The system has perfect secrecy if (PS) $\Leftrightarrow$ P & C are independent

Fact: If the system had (PS) then

$$\#(K) \overset{\#P}{\geq} \#\text{Possible}$$

Remark:

(1) Condition is not enough to give (PS)

(2) Suppose

$$K = \text{Perm}(P) \Longleftrightarrow K = P!$$

then we have (PS)

HW - Find Example

$\#(P) = 4$, $\#(K) = 4$, K

$C = P$, with induced distribution, s.t.

s.t. your system has no (PS)

Take $K_1 \in K$, take $x_1 \in P$

Consider $e_{K_1}(x_n) = y_1$

$K_n \longrightarrow x_1 \neq x_2$

$\exists K_2$ s.t. $e_{K_2}(x_2) = y_1$

$\text{prob}(x_2, y_1) = 0$

$\neq$ Does not equal

$P(x_2) \cdot P(y_1)$

$\neq 0 \qquad \neq e$

note: $K_2 \neq K_1$

$x_1 = d_{K_1}(y_n) = d_{K_2}(y_1) = x_2$

Continued this way

$P_{possible} \hookrightarrow K$

$x_1 \longmapsto K_1$
$x_2 \longmapsto K_2$

Stream cipher: one time pad

Take message $x_1, x_2, \ldots$ and (pseudo-random) set of keys

$K_1, K_2, \ldots$

and produce

$y_1, y_2, \ldots$

Eg. The Vigenère system is a stream cipher or ~~transpose~~ affine cipher

$P = C = \mathbb{Z}_N$ $K = \mathbb{Z}_N$ take key at random

$y_i = x_i + k_i$

uniformly at random

$\mathbb{Z}_N^N$, K. we denote is huge

Claim: The one-time pad gives perfect secrecy

Random # Generator

Goal: Get sequence $K_1, \ldots K_n \in \mathbb{Z}_n$ behave as if they have some information at random

multiplicative affine RNG

Affine

Take $N \geq 2$, $a, b \in \mathbb{Z}_N$

$a \in (\mathbb{Z}_N)^*$ and $K_b \in \mathbb{Z}_N$

↑ seed

and we set $K_i \in \mathbb{Z}_N$

$K_i = a K_{i-1} + b$, $i = 1, \ldots$

4/19/2022

Perfect Secrecy

$k \in K$ $\quad e_k - P_n \longrightarrow C_n$

(P_n, C_n, K)

Def: we say that (☆) has perfect secrecy if the random variable P_n & C_n are independent variables i.e.

$$\text{Prob}(\vec{x} = \vec{a}, \vec{y} = \vec{b}) = \text{Prob}(\vec{x} = \vec{a}) \cdot \text{Prob}(\vec{y} = \vec{b})$$

Fact: If $(*)$ has perfect secrecy

then $\#((P_n)_{possible}) \leq \#(K_n)$

Example $N=4$, $Z_N = \{0, 1, 2, 3\}$ ($N-1$)

① $P = Z_4 = C$, $K = \{k_1, I_{01}, I_{02}, I_{12}\}$

P has a probability S.t. $P_{possible} = P$

K has a uniform distribution

(P, C, K)

we do not have perfect secrecy

$Prob(x=0, y=3) = 0$

$Pr > 0$

---

② Shift Cipher $e_k(x) = x+k$

$P = C = K = Z_N$

P: any distribution; K: uniform

Claim (P, C, K) has perfect secrecy

$Prob(x=a, y=b) \overset{\text{assumption}}{=} Prob(x=a, k=b-a)$

$= Prob(x=a) \cdot \frac{1}{N}$

$= Prob(x=a) \cdot Prob(y=b)$

TOL

TO DO

(3) Consider

$$P_n = (\mathbb{Z}_N)^n = C_n = K_n$$

(uniform)

Claim (P_n, C_n, K) has perfect secrecy

(4) $P_2 = (\mathbb{Z}_N)^2 = C_2$

Any msg of $> 0 \in \mathbb{Z}$ possible prob.

$K = \mathbb{Z}_N$

$e_K(x_1, x_2) = (x_1 + K, x_2 + K)$

(P_2, C_2, K) has no PS

Stream Cipher & Onetime Pad

Recall

P, C, K

$x_1 \; x_2 \ldots x_n$

$k_1 \; k_2 \ldots$

$y_1 \; y_2 \ldots y_n$

Stream

P_n, C_n, K_n

$e_K(\vec{x}) = e_{k_1}(x_n) \ldots e_{k_n}(x_n)$

Eg. $P = C = \mathbb{Z}_N^* K$

↑ Vigenère cipher $P_n = (\mathbb{Z}_N)^n = C_n = K_n$

TO DO

Linear Congruential Generator. (Affine)

"Random # Generator"

$n \geq 2$, $a, b \in \mathbb{Z}_n$

$a \in (\mathbb{Z}_n)^*$ $k_0 \in \mathbb{Z}_n$ (seed)

Next, construct

$k_0 = a k_0 + b \ldots$

$k_i = a \cdot k_{i-1} + b$

Def: If k_n is equipped with uniform dist.

Maximum Period sequence

Fact: If $n = p_1^{e_1} \cdots p_k^{e_k}$ — $a \in (\mathbb{Z}_n)^*$, $b \in \mathbb{Z}_n$

then $\forall k_0$, $k_1 = a k_0 + b$, has period n

TO DO

iff

① & ② & ③

$gcd(N, b) = 1 \wedge \forall\, i = 1, \ldots$

$P_i \nmid a - 1$

$4 \mid N$ then $4 \mid a - 1$

Example $N = 8 = 2^3$

$a = 5, \; b = 1$

0 1 6 7 4 5 2 3

One Time pad - theoretical Perfect Secrecy

$P = Z_N = C = K$

$n \in \mathbb{N}$

$x_1 \; x_2 \; \cdots \; x_n \in Z_N$

$+ \quad + \quad + \quad +$

$k_1 \; k_2 \; k_n \in Z_N$

$\| \quad \| \quad \| \quad \|$

$y_1 \; y_2 \; y_n$

$K_i = aK_{i-1} + b$

LCG - Zhrun $a=3$ $b=$

k_0	k_1	k_2	k_3	k_4	k_5	
0	5	20	13	18	7	(repeat)
1	8	3	14	21	16	" "
2	11	12	15	24	23	" "
3	2	22	19	10	9	" "
4	17 (repeats)					

$N = p_1^{e_1} \cdots p_r^{e_r}$ For $N = 2^3 = 8$

① $aK_1 + b = K_2$

$\gcd(N, b)$ —— So N & B are coprime

② $\forall i \quad p_i \mid (a-1)$

③ If $4 \mid N \Rightarrow 4 \mid (a-1)$

Charles wants to break N

N, a, b

$K_0, K_1, \ldots K_{N-1}$

Continued

TO DO

$K_i, K_{i-1}, \ldots\ldots, K_{i-N} = d_i$

$d_i = K_i - K_{i-1}$ ← difference

$K_i = aK_{i-1} + b$

$K_{i-1} = aK_{i-2} + b$

$d_i = a(K_{i-1} - K_{i-2}) = ad_{i-1}$

if invertible $d_{i-1} \in (\mathbb{Z}_N)^*$

$a = d_i \cdot d_{i-1}^{-1}$

$K_i = a^i K_0 + (a^{i-1} + \ldots + a^2 + a + 1)b$

if $i = 0$ → $= 0$

Induction Proof

Let $i = 0$

$\vdots$

$\vdots$

$\cdot\, aK_0 + (a^{-1} \cdots\cdots)$

$d_i = K_i - K_{i-1} = a^{i-1}((a-1)K_0 + b)$

Which shows

$a - 1 \equiv 0 \bmod p$

$\therefore \gcd((a-1)K_0 + b, N) = \gcd(b, N) = 1$

this proves $b \in (\mathbb{Z}_N)^*$

$\forall i$ $d_i \in (\mathbb{Z}_N)^*$

invertible $\star$ invertible = invertible

Evelia ~~Cellus~~ functrast

Rivest, Shamir, Adleman (35) - RSA

TO DO

$A \to B$ $\quad N = p \cdot q$ $\quad e \cdot d \equiv 1 \mod K$

$d_e \equiv 1 \mod (p-1)(q-1)$

B ($N = p \cdot q$) $\xrightarrow{\text{Public Key}}$ A (N, e)

$x \longmapsto x^e$

$x \longmapsto \mathcal{E}(x) = x^e \mod N$

$\mathcal{D}\, x^{ed} = x \pmod N$

$\mathcal{E}(x) = x^e$

A $\longrightarrow$ B

$B^w = p^w$

e_j $\quad (p-1)(q-1) = k$

RSA: $x \longrightarrow x$ (f, then $g = f^{-1}$) — large — bij - nice formula

Ex ① $\mathbb{Z}_N$, $N = p \cdot q$, $e \in \left(\mathbb{Z}_k\right)^*$ $\quad K = (p-1)(q-1)$

$\log(x) \simeq \#\left(\mathbb{Z}_N\right)^*$

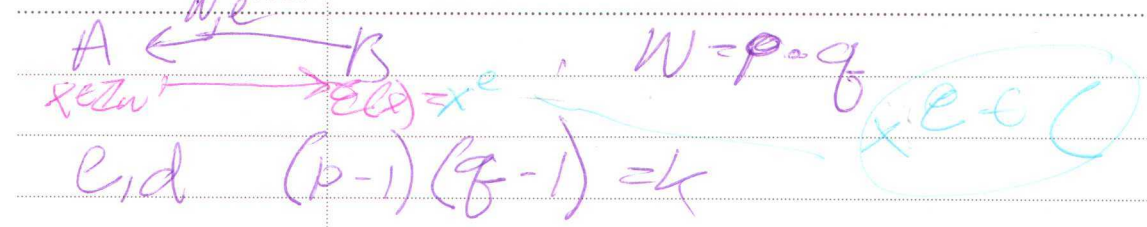
Ex ② $\mathbb{Z}_N \longrightarrow \mathbb{Z}_N$

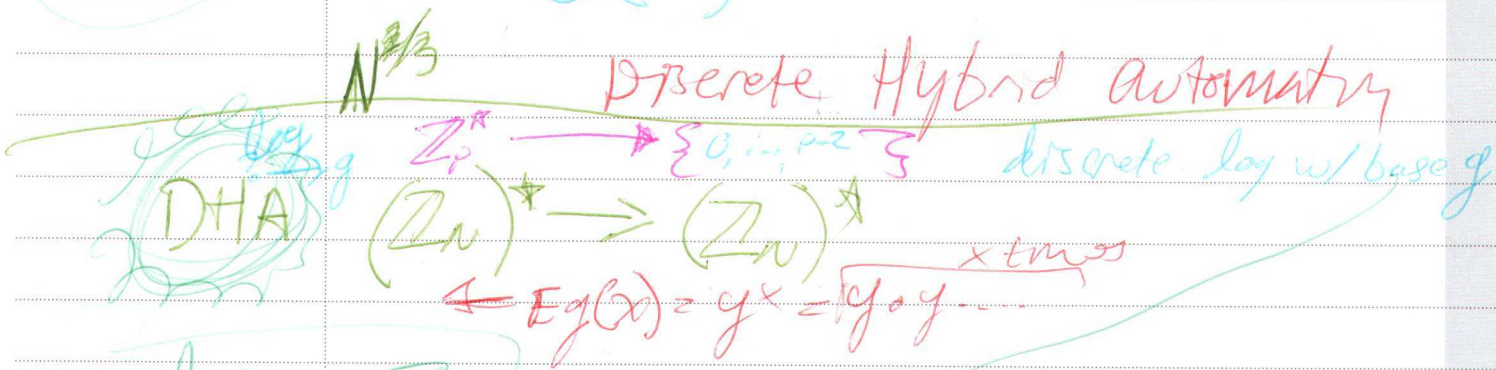
$x \longmapsto x^e$

this means there is a $d =$

so $\mathcal{D}(\mathcal{E}(x)) = x \mod N$

TO DO





$\log_g : Z_p^* \to Z_p$

generator g

$a \longrightarrow \log_g(a) = ? \; x$

$Z_p^* = \{1, \dots, p-1\} \Rightarrow \exists g$ s.t. $\forall y \in (Z_p)^*, \exists! x$ s.t. $g^x = y$

$N = 3 \cdot 17 = 51$

$\ell = (p-1)(q-1) = 2 \cdot 16 = 32$

find soln to $d_k = 1 \bmod 32$

choose $e = 3 \cdot d = 11$

let $m = 2$ (then) $\cdot E(m) = 2^3 \bmod N = 8$

$D_K \; 8^{11} = \left(\left(8^2\right)^2 \cdot 8\right) \cdot 8 \bmod 51$

$8^2 = 64 = 13$

$13^2 = 169 \equiv 16$

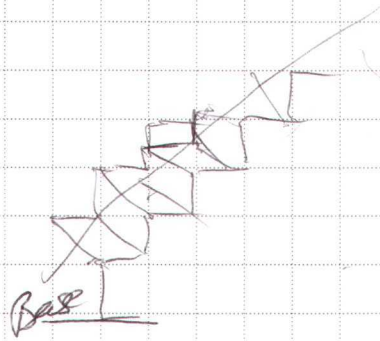
$16 \cdot 8 = 128 \equiv 26$

$26^2 = 676 =$

$$(x^e)^d \equiv x \pmod{n}$$

FLT - Fermat's Little Theorem

p $a \in \mathbb{N}$, $a^p \equiv a \pmod{p}$



proof by induction

Base $a = 0$ ✓

Induction $(a+1)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i + 1^p$

$(a+1)^2 = a^2 + 2(a) + 1$

$\binom{2}{1}$

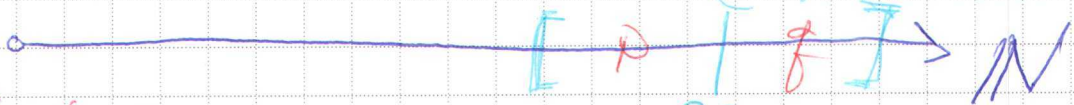
mod p

$a^p + 0 + 1 = a + 1$ ∎

---

consider p, q very large Primes

prime Number Theorem $\#(x/\log(x))$



x very large

$e = (p-1)(q-1)$

k

almost every element is prime

$\mathbb{Z}_N \approx$ for $N \gg\gg$

$\frac{N}{\log(N)} \approx N$

B Choose a base a at random,
$1 \leq a \leq p-1$ & let $p-1 = m \cdot 2^k$
where m is odd

Compute the sequence
$x_0, x_1, \ldots x_k$
$x_k = a^{m \cdot 2^k} \bmod p$