Ch 1 → Slides

Three Simple ciphers

(1) Caesar
↳ Simplest of the substitution ciphers.

Ch:	A	B	C	D	E	...	Y	Z
pos:	0	1	2	3	4		24	25

β = Shift Amnt

Enc For every letter in P shift right $\beta \% 26$ position

why

Enc(ch, β)
ch = ch + β

Enc('A', 3) → 'D'

Dec.
For every letter in C shift left $(\beta + 26) \% 26$ position

Dec (ch, β)
ch = ch − β + 26 ... % 26

Enc ('Z', 5) → 'E'
Dec ('E', 5) : (4 − 5 + 26) % 26
= 25 → 'Z'

(2) Matrix - SliDes

ADFGVX

Used by Germans during WWI

1854

Substitute Permute [illegible] WWI 14

Permute Values

Two Keys

Key1: Permute A-Z
0-9

arrange in a 6x6 Matrix
labeled

	A	D	F	G	V	X
A	F	L	1	A	O	Z
D	J	D	W	3	6	U
F	C	I	Y	B	4	P
G	R	5	φ	8	V	E
V	6	K	7	2	M	X
X	S	N	H	0	T	9

Key2: Encrypt

Enc.

(2) MATrix Cipher

ADFGVX

SliDes

③ Public Key Cipher w/out Advanced Math

Bob
- Sends P to Alice
- Encrypts with Alice's public key

Alice
- Decrypts with private key

Alice
- Chooses 4 random integers
  a, b, A, B
- Computes
  $M = ab - 1$
  $e = AM + a$
  $d = BM + b$ → $n = \left\lfloor \frac{ed - 1}{M} \right\rfloor$

Where
Private key: d
Public key: (n, e)

Plaintext, P, is an integer $< n$

Bob
↳ Msg P_b

- Computes

$$C = P_b \cdot e \ \% \ n$$

- Sent C to Alice

Alice uses private key d
to compute

$$P_a = C \cdot d \ \% \ n$$

Claim: $P_a = P_b$

Let $a = 3$
$b = 4$
$A = 5$
$B = 6$

$M = ab - 1 = 11$
$e = AM + a = 58$
$d = BM + b = 70$
$n = \left\lfloor \frac{ed - 1}{m} \right\rfloor = 369$

Bob has (e, n) chooses $P_b = 200$
computes

$$C = (200 \cdot 58) \% 369 = 161$$
$$= (P \cdot e) \% n$$

Alice computes

$P_a = C \cdot d \,\%\, n$

$= (161 \cdot 70) \,\%\, 369$

$= 200 = P_b$

Bob knows
- Algorithm
- n, e
- P_b

Bob can compute C

Alice knows
- Algorithm
- m
- d
- n, e

Alice can compute P_a from C

Eve knows
- Algorithm
- c
- n, e

but not d, which is required to decrypt

Security Req that d is
not easily recoverable
from n, e

Eve knows

$$n = \left\lfloor \frac{ed-1}{m} \right\rfloor$$

e

but does not know m

Just enough number theory

Assume basic facts about integers and operations on integers:

Given integers a, b, c, d

Commutative: $a+b = b+a$, $a*b = b*a$

Associative: $a+(b+c) = (a+b)+c$

$a*(b*c) = (ab)c$

Dist: $a(b+c) = ab+ac$

Well-Ordering Principle

if S is a non-empty set of non-negative integers

Then

$\forall b \in S \ \exists$ a $a \in S$

s.t. $a \leq b$

i.e every non-empty set of non-neg. integers contains a least element

Finite Induction (Burton, p. 2)

Let S be a set of positive integers s.t.

1) $1 \in S$

2) $k \in S \Rightarrow k+1 \in S$

then S is the set of all positive integers.

Follows from the Well ordering Principle. Basis for PMI

Division Algorithm: (w/out proof)

Given integers a, b with $b > 0$
$\exists$ unique integers q, r
Satisfying

$$a = qb + r \quad 0 \le r < b$$

We say
q is the quotient
b is the divisor
r is the remainder

Ex

$$13 = 4 \cdot 3 + 1$$

$$\begin{array}{r} 4 \\ 3 \overline{)13} \\ \underline{12} \\ 1 \end{array}$$

Loosely
Any integer, a, can be 'divided' by a positive integer, b, in such a way that the remainder is smaller than b

Ex1 using D.A.

Square of any odd integer is of the form $8k+1$ where k is an integer

Pf By DA any integer, a, may be written

$a = 4q$
$a = 4q+1$
$a = 4q+2$
$a = 4q+3$

ex. Let $a = 247$

$$\begin{array}{r} 61 \\ 4\overline{)247} \\ \underline{24} \\ 7 \\ \underline{4} \\ 3 \end{array}$$

$a = 4 \cdot 61 + 3$ where $q = 61$

only $4q+1$ and $4q+3$ are odd

$(4q+1)^2 = 16q^2+8q+1 = 8(2q^2+q)+1$
$= 8k+1$

$(4q+3)^2 = 16q^2+24q+9 = 8(2q^2+3q+1)+1$
$= 8k+1$

Ex 2 (go to p7 back)

Two of the equations in Kid Krypto were expressed as DA:

$e = Am + 1$
$d = Bm + b$ | p 13 McAndrew

Def Divisible

Let a, n be integers $a \neq 0$
if $\exists$ an integer c s.t.

$n = ac$

We say a divides n $(a|n)$

equivalently
- a is a factor of n
- n is a multiple of a

Ex $3|15$ b.c $15 = 3 \cdot 5$

$3 \nmid 11$ b.c $\nexists$ c s.t. $11 = 3 \cdot c$

Div. alg properties

a) $a|0$, $1|a$, $a|a$

b) $a|1$ iff $a = \pm 1$

c) if $a|b$ and $c|d$ then $ac|bd$

d) if $a|b$ and $b|c$ then $a|c$

e) $a|b$ and $b|a$ iff $a = \pm b$

f) if $a|b$ and $b \neq 0$ then $|a| \leq |b|$

g) if $a|b$ and $a|c$ then $a|(bx+cy)$ for arbitrary integers x, y

d) Proof

if $a|b$ and $b|c$ then $a|c$

pf

Since $a|b$ and $b|c$ def. of divisibility says

$\exists\, k, m$ s.t.

$b = ak$ and $c = bm$

$\Rightarrow c = akm$

let $q = km$ then $c = aq$

so $a|c$ by def. of divisibility

g) Proof
if $a|b$ and $a|c$ then $a|(bx+cy)$

pf $a|b \Rightarrow b = ak_1$
$a|c \Rightarrow c = ak_2$

So $bx = xak_1$
$cy = yak_2$

$(bx+cy) = (xak_1 + yak_2)$
$= a(xk_1 + yk_2)$

Let $p = xk_1 + yk_2$

then
$(bx+cy) = a \cdot p$

and $a|(bx+cy)$

Def Prime Number

an integer $n > 1$ is prime
if its only divisors are
1 and n

Def. Composite Number

an integer $n > 1$ is composite if it is not prime.

$\Rightarrow \exists\, n = ac, \; a, c$
s.t. $a, c > 1$ and $a, c < n$

Factoring theorem

if n is composite, it must have a factor, c, s.t.

$c \leq \sqrt{n}$

pf by contradiction

Let n be composite
then $n = ac$

Suppose $a > \sqrt{n}$
$c > \sqrt{n}$

$\Rightarrow ac > n$

which contradicts the assumption that $n = ac$
So either $a \leq \sqrt{n}$ or
$c \leq \sqrt{n}$

Def GCD

Let a, b be integers with at least one of them > 0

$\gcd(a,b) = d$, a positive

where d is a positive integer S.T.

1) $d \mid a$ and $d \mid b$

2) if $c \mid a$ and $c \mid b$ $c \le d$

Def Relatively Prime

Two integers a, b are relatively prime if $\gcd(a,b) = 1$

i.e. a, b have no common factor's > 1

$\gcd(2,5) = \gcd(-9,16) = \gcd(2,7) = 1$

#2 mp 5 Another Div alg example

Show $3 \mid a(a^2+2)$ $\forall a \geq 1$

By DA a is of the form $3q$, $3q+1$, $3q+2$

Case 1 $a = 3q$

$a(a^2+2)/3 = 3q((3q)^2+2)/3$

$= q(9q^2+2)$

which is an integer

Case 2 $a = 3q+1$

$(3q+1)((3q+1)^2+2)/3$

$= (3q+1)(9q^2+6q+3)/3$

$= (3q+1)(3q^2+2q+1)$ which is an in.

Case 3 $a = 3q+2$

$(3q+2)((3q+2)^2+2)/3$

$= (3q+2)(9q^2+12q+4+2)/3$

$= (3q+2)(9q^2+12q+6)/3$

$= (3q+2)(3q^2+4q+2)$

which is an integer

Euclid's Alg for gcd

Find gcd(137, 12)

$$\begin{array}{r|l} & 11 \\ 12 & 137 \\ & \underline{12} \\ & 17 \\ & \underline{12} \\ & 5 \end{array} \qquad \begin{array}{r|l} & 2 \\ 5 & 12 \\ & \underline{10} \\ & 2 \end{array} \qquad \begin{array}{r|l} & 2 \\ 2 & 5 \\ & \underline{4} \\ & 1 \end{array} \qquad \begin{array}{r|l} & 2 \\ 1 & 2 \\ & \underline{2} \\ & R=0 \end{array}$$

GCD

At Each Step
1) divisor becomes dividend
2) remainder becomes divisor

GCD is last non-0 remainder

So gcd(137, 12) = 1

gcd(27, 15)

$$\begin{array}{r|l} & 1 \\ 15 & 27 \\ & \underline{15} \\ & 12 \end{array} \qquad \begin{array}{r|l} & 1 \\ 12 & 15 \\ & \underline{12} \\ & 3 \end{array} \qquad \begin{array}{r|l} & 4 \\ 3 & 12 \\ & \underline{12} \\ & R=0 \end{array}$$

GCD

GCD Details

Def //, %

Div Alg

a = qb + r 0 ≤ r < b

① // : quotient when a is divided by b

$a // b = q$

② % : remainder when a is divided by b

$a \% b = r$

Iterative Def gcd(a,b)

1. $q = a//b$
2. $a = b,\ b = r$
3. if $a \% b = 0$
   gcd(a,b) = r
   else goto step ①

Recursive Def gcd(a,b)

```
if a % b == 0
    return b
return gcd(b, a % b)
```

set dividend to divisor
set divisor to remainder

Process can be rep. as a system of linear equations

gcd(12, 137)

$$12\overline{)137}^{\,11} \quad 137 - 12 = 17,\ 17 - 12 = 5$$

$$5\overline{)12}^{\,2} \quad 12 - 10 = 2$$

$$2\overline{)5}^{\,2} \quad 5 - 4 = 1$$

$$1\overline{)2}^{\,2} \quad 2 - 2 = 0$$

$$137 = 11 \cdot 12 + 5$$

$$a = q_1 b + r_1 \qquad 0 \le r_1 < b$$

$$b = q_2 r_1 + r_2 \qquad 0 \le r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3 \qquad 0 \le r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \qquad 0 \le r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n + 0$$

$\gcd(a,b) = r_n$, the last non-0 remainder

GCD theorem

given $a = qb + r$

then $\gcd(a,b) = \gcd(b,r)$

if This is True, then

$$\gcd(a,b) = \gcd(b, r_1)$$
$$= \gcd(r_1, r_2)$$
$$\vdots$$
$$= \gcd(r_{n-1}, r_n)$$
$$= \gcd(r_n, 0)$$
$$= r_n$$ the last non-0 remainder

<u>Ex</u>

$30 = 3 \cdot 9 + 3$

$\gcd(30,9) = \gcd(9,3) = 3$

<u>proof</u>

Let $d = \gcd(a,b)$

then $d|a$, $d|b$

b.c. $a = qb + r$ $\quad d \mid a - qb$

and $d|r$

So d is a common divisor of b and r

but is it the largest

Choose c an arbitrary common divisor of b, r

$\Rightarrow c \mid qb + r$

$\Rightarrow c \mid a$

so c is a common divisor of a, b

$\Rightarrow c \leq d$

b.c. by assumption $d = \gcd(a, b)$

We know

1. $d = \gcd(a, b)$ common divisor of b, r
2. d is a common divisor of b, r
3. c is a common divisor of b, r
4. $c \leq d$

$\Rightarrow d = \gcd(b, r)$

so $\gcd(a, b) = \gcd(b, r)$

which is what we were trying to prove.