Extended Euclid (proof Trapp & Washington, ?)

Let a, b be integers with at least 1 of a, b non-zero

Then ∃ integers s, t

Such that

$$as + bt = \gcd(a,b)$$

In particular, if a, b are relatively prime

$$as + bT = 1$$

Ex $\gcd(172, 20) = 4$

So, $172S + 20T = 4$

But how to find S, T

① find gcd(172, 20)
② run Euclid in reverse

$$20\overline{)172}^{\,8} \quad \begin{array}{r}16\\ \hline 12\end{array} \qquad 12\overline{)20}^{\,1} \quad \begin{array}{r}12\\ \hline 8\end{array} \qquad 8\overline{)12}^{\,1} \quad \begin{array}{r}8\\ \hline 4\end{array}\ \text{gcd} \qquad 4\overline{)8}^{\,2} \quad \begin{array}{r}8\\ \hline R=0\end{array}$$

Express using DA form

$$172 = 8 \cdot 20 + 12$$
$$20 = 1 \cdot 12 + 8$$
$$12 = 1 \cdot 8 + 4$$
$$8 = 2 \cdot 4$$

next page

$$172 = 8 \cdot 20 + 12$$
$$20 = 1 \cdot 12 + 8$$
$$12 = 1 \cdot 8 + 4$$
$$8 = 2 \cdot 4$$

Reverse Euclid

$$4 = 12 - 8$$
$$= 12 - (20 - 1 \cdot 12)$$
$$= 12 - (20 - 12)$$
$$= 2 \cdot 12 - 20$$
$$= 2(172 - 8 \cdot 20) - 20$$

$$= 2 \cdot 172 - 17 \cdot 20$$

$$4 = 172S + 20T$$

So $S = 2$
$T = -17$

$$172 \cdot 2 + (20 \cdot (-17)) = 4$$
$$344 - 340 = 4$$

Ex. $S = 45$
$T = 39$

$$45S + 39T = \gcd(45, 39)$$

$$\begin{array}{r} 1 \\ 39\overline{)45} \\ \underline{39} \\ 6 \end{array} \qquad \begin{array}{r} 6 \\ 6\overline{)39} \\ \underline{36} \\ 3 \end{array} \qquad \begin{array}{r} 2 \\ 3\overline{)6} \\ \underline{6} \\ 0 \end{array}$$

gcd

$$\gcd(45,39) = 3$$

So $45S + 39T = 3$

$$45 = 1 \cdot 39 + 6$$
$$39 = 6 \cdot 6 + 3 \qquad \gcd(45,39) = 3$$

$$3 = 39 - 6 \cdot 6$$
$$= 39 - 6(45 - 39)$$
$$= -6 \cdot 45 + 7 \cdot 39$$

$S = -6$
$T = 7$

Ex

$\gcd(482, 1180)$

$$\begin{array}{r} 2 \\ 482 \overline{)\,1180} \\ 964 \\ \hline 216 \end{array} \qquad 1180 = 2 \cdot 482 + 216$$

$$\begin{array}{r} 2 \\ 216 \overline{)\,482} \\ 432 \\ \hline 50 \end{array} \qquad 482 = 2 \cdot 216 + 50$$

$$\begin{array}{r} 4 \\ 50 \overline{)\,216} \\ 200 \\ \hline 16 \end{array} \qquad 216 = 4 \cdot 50 + 16$$

$$\begin{array}{r} 3 \\ 16 \overline{)\,50} \\ 48 \\ \hline 2 \end{array} \qquad 50 = 3 \cdot 16 + 2$$

$$\begin{array}{r} 8 \\ 2 \overline{)\,16} \\ 16 \end{array}$$

$\gcd(482, 1180) = 2$

$482S + 1180T = 2$

$12 = 1 \cdot 10 + 2$

$2 = 12 - 1 \cdot 10$

$2 = 50 - 3 \cdot 16$

$= 50 - 3(216 - 4 \cdot 50)$

$= 13 \cdot 50 - 3 \cdot 216$

$= -3 \cdot 216 + 13 \cdot 50$

$[illegible] - 13(482 - 2 \cdot 216)$

$[illegible] - 13 \cdot 482$

$= -13 \cdot 482 + [illegible] \cdot 216$

$= -13 \cdot 482 +$

$$2 = 50 - 3\cdot 16$$
$$= 50 - 3(216 - 4\cdot 50)$$
$$= 13\cdot 50 - 3\cdot 216$$
$$= 13(482 - 2\cdot 216) - 3\cdot 216$$
$$= 13\cdot 482 - 26\cdot 216 - 3\cdot 216$$
$$= 13\cdot 482 - 29\cdot 216$$
$$= 13\cdot 482 - 29(1180 - 2\cdot 482)$$
$$= 13\cdot 482 - 29\cdot 1180 + 58\cdot 482$$
$$= 71\cdot 482 - 29\cdot 1180$$

$S = 71$

$T = -29$

lucky we have Done

$\text{xgcd}(482, 1180) = (2, 71, -29)$

Fundamental theorem of arithmetic in four parts

① Euclid's lemma

if $a | bc$ with a, b relatively prime, then $a | c$

Ex $a = 3$ $b = 5$ $c = 6$

$\gcd(a, b) = 1$

$3 | 5 \cdot 6$ and $3 | 6$

Pf.

$\gcd(a, b) = as + bt$

Since a, b are relatively prime

$1 = as + bt$

$c = cas + cbt$

$= acs + bct$

$a | bc$ by assumption

$a | acs$ b.c $a | a$

$\Rightarrow a | (acs + bct)$

$a | c(as + bt)$

either $a | c$ or $a | (as + bt)$

but $(as + bt) = 1$

so $a | c$ as claimed

② Prime Divisor theorem

if p is prime and $p | ab$

then $p | a$ or $p | b$

Case 1

assume $p | a$

We're finished

Case 2

assume $p \nmid a$

Notice

p, a are relatively prime

$p | ab$

by Euclid's lemma $p | b$

so $p | a$ (case 1)

or $p | b$ (case 2)

There are no more cases

③ Prime Div. theorem Corollary

if p is prime and $p \mid a_1 a_2 \ldots a_k$

then $p \mid a_k$ for some k $1 \le k \le n$

This is just an extension of prime division Theorem and can be proved by PMI (Burton, p. 41)

④ Corollary 2

if $p_1, q_1, q_2, \ldots, q_n$ are all prime

and $p \mid q_1 \ldots q_n$

Then $p = q_k$ for some k $1 \le k \le n$

pf. by Corollary 1, $p \mid q_k$

for some k $1 \le k \le n$

But q_k is prime as is p

Since $p > 1$ b.c. p is prime

$p \mid p = q_k$

Fundamental Th of arithmetic

(A) Every positive integer, n, can be represented as itself or as a product of primes

(B) This representation is unique apart from the order of the factors

(A) proof

n is either or prime
if n is prime $n = n \cdot 1$
we are finished

(B) if n is composite $\exists$ an integer, d, s.t. $d | n$ and $1 < d < n$
among all such integers there exists a least, p_1, by the well ordering Principle.

p_1 is not composite
if it were it would have a divisor q with $1 < q < p_1$

But since $q | p_1$ and $p_1 | n$

$q | n$ which would contradict our choice of p_1 as the smallest possible divisor of n.
So p_1 is prime

Now we can write

$$n = p_1 n_1$$

where p_1 is prime and
$1 < n_1 < n$

if n_1 is prime
⇒ we have a prime factorizati

if not, repeat the arg. to produce

$n = p_1 p_2 n_2$ where

$n_1 = p_2 n_2$ and $1 < n_2 < n_1$

after a finite number of steps

$$n = p_1 n_1$$
$$n_1 = p_2 n_2$$
$$\vdots$$
$$n_{k-1} = p_k \cdot 1$$

So $n = p_1 p_2 \cdots p_k$

a prime factorization

(B) The factorization is unique

pf by contradiction

Suppose n can be written as a product of primes in two ways

$n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$ $r < s$

with p_i, q_j prime $\forall i, j$

So that

$p_1 \leq p_2 \leq \ldots p_r$

$q_1 \leq q_2 \leq \ldots \leq q_s$

Since $p_1 | n$, $p_1 | q_1 q_2 \ldots q_s$

Recall Corollary 2

if $p, q_1, q_2, \ldots, q_n$ are all prime

and $p | q_1 q_2 \ldots q_n$

$p = q_k$ for some $1 \leq k \leq n$

By Corollary 2, since all q_j are prime $p_1 = q_k$ for some k

Since q_1 is smallest in the seq and $p_1 = q_k$

$p_1 \geq q_k$

We can make the same arg for q_1

namely $q_1 = p_k$ and $q_1 \geq p_1$

$\Rightarrow q_1 = p_1$

Cancel these to obtain

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

Since $r < s$

We arrive at

$$1 = q_{r+1} q_{r+2} \cdots q_s$$

But each q_j is prime and so > 1

So $r < s$ is false, $r = s$

and

$p_1 = q_1$

$p_2 = q_2$

$\vdots$

$p_r = q_s$

contradicting that the two factorizations are different

they are identical $\Rightarrow$ each factorization is unique

Corollary

any positive integer > 1 can be written uniquely in canonical form

$$n = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$$

each k_i $(1 \le i \le n)$ is a positive integer and each p_i is prime with

$$p_1 < p_2 < \cdots p_n$$

Ex

$$4725 = 3^3 \cdot 5^2 \cdot 7$$
$$17360 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$$

Prove this one

Euclid's Theorom

There are an infinite number of primes

Pf By Contradiction

Let $P_1 = 2$, $P_2 = 3$, $P_3 = 5 \ldots$ be the primes in ascending order

Suppose there is a last prime, P_n

Let
$$P = P_1 P_2 \dots P_n + 1$$

Since $P > 1$ it may be written as a product of primes

$$P = P_a P_b P_c \dots P_r$$

$\Rightarrow$ P is divisible by some prime, P_j

Since $P_1, P_2, \dots P_n$ are the only primes P_j is among them

So $P_j \mid P_1 P_2 \dots P_n$ and $P_j = P_k$

Recall Prop 9 of division algorithm

if $a \mid b$ and $a \mid c$

$a \mid bx + cy$ for arbitrary integers x, y

Let $x = 1$
$y = -1$
$a = P_j$, $b = P$, $c = P_1 P_2 \dots P_n$

We know $P_j \mid P$ and $P_j \mid P_1 P_2 \dots P_n$

by the property

Since $a \mid bx + cy$

$$p_j \mid \underbrace{P}_{b} \cdot 1 + \underbrace{(p_1 p_2 \dots p_n)}_{c} (-1)$$

$$p_j \mid P - (p_1 p_2 \dots p_n)$$

but $P = p_1 p_2 \dots p_n + 1$

So $p_j \mid 1$

but $p_j > 1$ by assumption

=> no finite list of primes is complete

=> # of primes is infinite

Congruence (Def)

Let n be a positive integer

Two integers a, b are said to be congruent modulo n

Written $a \equiv b \pmod n$

if $a - b = kn$ for some inte[ger] k

Ex $3 \equiv 24 \pmod 7$ b.c $3 - 24 = (-3) \cdot 7$

$-3 \equiv 11 \pmod 7$ b.c $-3 - 11 = (-2) \cdot 7$

$17 \equiv 17 \pmod{13}$ b.c $17 - 17 = 0 \cdot 13$

hw/ Factoids (for homework)

(A) any two integers are congruent mod 1

pf/ let a, b be integers

Suppose
$a \not\equiv b \bmod 1$
there is no k s.t.

$a - b = k \cdot 1$ or $a + (-b) = k \cdot 1$
Since arith. is closed under addition this can't be

So $a \equiv b \bmod 1$

hw 1 (B) any two integers are cong if both are even or both are odd

Let a, b be even integers

$a = q \cdot 2$ and $b = k \cdot 2$

Then $a - b = q2 - k2$

$= 2 \cdot (q - k)$

Let $n = q - k$

$a \equiv b \mod n$

Let a, b be odd integers

So $a = q+1$, $b = k+1$

where q, k are even

$a - b = (q+1) - (k+1)$

Let $q = 2r$

$k = 2s$

$a - b = (2r+1) - (2s+1)$

$= 2r - 2s$

$= 2(r-s)$

$a \equiv b \mod (r-s)$

Relationship TO Div. alg.

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

$a - r = qb$

$a \equiv r \mod b$

Ex $\quad 11 = 1 \cdot 7 + 4$

$11 \equiv 4 \mod 7$

in C $11 \% 7 = 4$
the remainder when 11 is divided by 7

Notice there are b possibilities for r
$0, 1, \ldots, b-1$

i.e when a is divided by b the possible remainders are $0, 1, \ldots, b-1$

so
every integer a is congruent mod b to exactly one of
$0, 1, 2, \ldots, b-1$

$P = \{0, 1, \ldots, b-1\}$
↳ set of least non-negative residues mod b

Use Root Set to Define
Complete Set.

Complete Set
a Collection of integers is said
to form a complete set
$P = \{a_1, a_2, a_3, \dots, a_b\}$

is said to form a complete
set of residues mod b
if the elements of P are
congruent mod b to $0, 1, \dots, b-1$
Taken in some order.

Ex
$-12, -4, 11, 13, 22, 52, 91$ are
a complete set of residues
mod 7
i.e.

$-12 \equiv 2 \bmod 7$
$-4 \equiv 3 \bmod 7$
$11 \equiv 4 \bmod 7$
$13 \equiv 6 \bmod 7$
$22 \equiv 1 \bmod 7$
$82 \equiv 5 \bmod 7$
$91 \equiv 0 \bmod 7$

is not necessarily unique

2

iff a, p leave same remainder when divided by b, a and p are congruent.

if (a ≡ p mod b, a and b leave the same remainders when divided by b.

Theorem
Congruence and the division algorithm
(Burton, p.65)

For arbitrary integers a, b

$a \equiv p \mod b$

iff a and p leave the same remainder when divided by b

Ex $11 \equiv 4 \mod 7$

$$7 \overline{\big)\, 11}^{\,1} \quad 7 \cdot 1 = 7, \quad 11 - 7 = 4 \qquad\qquad 7 \overline{\big)\, 4}^{\,0} \quad 7 \cdot 0 = 0, \quad 4 - 0 = 4$$

Same remainder ⇒ cong.

$11 - 4 = 1 \cdot 7$

Congruence properties

a) $a \equiv a \mod n$

b) if $a \equiv b \mod n$ then $b \equiv a \mod n$

c) if $a \equiv b \mod n$ and $b \equiv c \mod n$ then $a \equiv c \mod n$

Closure prop.

e) if $a \equiv b \mod n$ and $c \equiv d \mod n$
$a + c \equiv b + d \mod n$ and
$ac \equiv bd \mod n$

notice d is missing

d) if $a \equiv b \mod n$ then
$a + c \equiv b + c \mod n$ and
$ac \equiv bc \mod n$

d) if $a \equiv b \mod n$
$a^k \equiv b^k \mod n$ for any positive integer k

proof of c

if $a \equiv b \mod n$ and $b \equiv c \mod n$
$a \equiv c \mod n$

pf

$a \equiv b \mod n$ then

$$a - b = k_1 n$$

$b \equiv c \mod n$ then

$$b - c = k_2 n$$

So

$$a - b = k_1 n$$
$$+ \quad b - c = k_2 n$$

$$a - c = k_1 n + k_2 n$$
$$= n(k_1 + k_2)$$

Let $k = k_1 + k_2$

$$a - c = kn$$

and $a \equiv c \mod n$

Proof of 1 closure property

c) if $a \equiv b \mod n$
$c \equiv d \mod n$

$ac \equiv bd \mod n$

Proof

$$a - b = k_1 n$$
$$c - d = k_2 n$$

$$a = b + k_1 n$$
$$c = d + k_2 n$$

$$ac = (b + k_1 n)(d + k_2 n)$$

$$= bd + \underline{d k_1 n + b k_2 n + k_1 k_2 n^2}$$

$$ac - bd = n(d k_1 + b k_2 + k_1 k_2 n)$$

Let $k = d k_1 + b k_2 + k_1 k_2 n$

$$ac - bd = k n$$

and $ac \equiv bd \mod n$

Now we can solve equations

$x+7 \equiv 3 \mod 17$

$x \equiv -4 \mod 17$

We want x to be positive

Addition theorem

x, y, n, p are integers, $n > 0$

$x \equiv y \mod n \Rightarrow$

$x \equiv y + pn \mod n$

pf

$x - y = kn$

$x - y - pn = kn - pn$

$x - y - pn = n(k-p)$, let $q = k - p$

$x - y \equiv pn \mod n$ Def

$x \equiv y + pn \mod n$

$x \equiv -4 \mod 17 \Rightarrow$

$x \equiv -4 + 17 \equiv 13 \mod 17$

notice Div. was missing from closure

Closure under division

Let a, b, c, n be integers with $n \neq 0$ and with $\gcd(a,n)=1$

if $ab \equiv ac \mod n$

then $b \equiv c \mod n$

(if a, n are relatively prime we can divide both sides by a)

<u>pf</u>

Since $\gcd(a,n)=1$ $\exists$ integers

s, t s.t.

$as+nt=1$ by extended Eucli

$(b-c)(as+nt)=b-c$

$bas-cas+bnt-cnt=b-c$

$s(ab-ac)+nt(b-c)=b-c$

but $ab-ac=kn$ by def.

so

$skn+nt(b-c)=b-c$

$n(sk+t(b-c))=b-c$

$n(sk+bt-ct)=b-c$

Let $sk+bt-ct=q$, an integer

then

$$b - c = nq$$

and $b \equiv c \mod n$

which is what we were trying to prove

$\underline{Ex}$

$$2x + 7 \equiv 3 \mod 17$$

$$2x \equiv -4 \mod 17$$

$$\gcd(2, 17) = 1$$

$$x \equiv -2 \mod 17$$

$$x \equiv 15 \mod 17$$

$$5x + 6 \equiv 13 \mod 11$$

$$5x \equiv 7 \mod 11$$

$$5x \equiv 7 + 3 \cdot 11 \mod 11 \qquad \text{readdith}$$

$$\equiv 40 \mod 11$$

$$\gcd(5, 11) = 1$$

$$x \equiv 8 \mod 11$$

$40 + 6 \equiv 13 \mod 11$

$46 \equiv 13 \mod 11$

$2 \equiv 2 \mod$

Def **Multiplicative Inverse**

The MI of an integer a

is that integer p S.T. $ap = 1$

p is written a^{-1}

So

$$a a^{-1} = 1$$

Recall

Given $5x + 6 \equiv 13 \mod 11$

$$5x \equiv 7 \mod 11$$

$\gcd(5, 11) = 1$

Dividing by 5 is same a multiplying $5^{-1} \mod 11$

$$5^{-1}(5x) = 7 \cdot 5^{-1} \mod 11$$

$$9 = 5^{-1} x = 7 \cdot 5^{-1} \mod 11$$

as it happens $5^{-1} \equiv 9 \mod 11$

(b.c. $5 \times 9 = 45 \equiv 1 \mod 11$)

$$5x \cdot 9 \equiv 7 \cdot 9 \mod 11$$

$$x \equiv 63 \mod 11$$

but $63 \equiv 8 \mod 11$

so $x \equiv 8 \mod 11$

How To Find MI (Troppe & WA p 73)

Th. Suppose $\gcd(a,n)=1$

Let S, T be integers
We know from extended Euclid
That $\exists$ integers a, n S.T $as+nT=1$

Then S is the MI of a mod n

Proof

$$as + nT = 1$$

$$as - 1 = nT$$

$$as \equiv 1 \bmod nT$$

So S is the MI of a mod n

Ex $11111x \equiv 4 \bmod 12345$

① Show $\gcd(11111, 12345) = 1$

$$12345 = 1 \cdot 11111 + 1234$$
$$11111 = 9 \cdot 1234 + 5$$
$$1234 = 5 \cdot 246 + 4$$
$$5 = 1 \cdot 4 + 1$$
$$4 = 4 \cdot 1 + 0$$

$\gcd(11111, 12345) = 1$

So

$$11111 \cdot S + 12345 \cdot T = 1$$

S is MI of 11111 mod 12345

$$\begin{aligned}
1 &= 5 - 4 \\
&= 5 - (1234 - 5 \cdot 246) \\
&= 247 \cdot 5 - 1234 \\
&= 247(11111 - 9 \cdot 1234) - 1234 \\
&= 247 \cdot 11111 - 2224 \cdot 1234 \\
&= 247 \cdot 11111 - 2224(12345 - 11111) \\
&= 2471 \cdot 11111 - 2224 \cdot 12345
\end{aligned}$$

$S = 2471$
$T = -2224$

So $2471 = 11111^{-1} \bmod 12345$

$11111x$ [illegible] $= 1234$

Suppose $11111x = 4 \bmod 12345$

$$\begin{aligned}
x &= 4 \cdot 2471 \bmod 12345 \\
&= 9884 \bmod 12345
\end{aligned}$$

Affine from Caesar Cipher

Caesar

0	1	2	3	. . .	25
A	B	C	D	. . .	Z

β = shift Amt

E('A', 3)
Shift right 3 spaces

⟶ 'D'

For clarity, suppose mapping to pos is done outside of one

$$E(x, \beta) = (x + \beta) \bmod 26$$

$$y = x + \beta \bmod 26$$

Decrypt is inverse

$$x = y - \beta \bmod 26$$

Use addition theorem to make x positive

$$x = y - \beta + 26 \bmod 26$$

To Sum

$$E(C, \beta) = (C+\beta) \bmod 26$$

$$D(C, \beta) = (C-\beta+26) \bmod 26$$

C in range $[0..25]$
β in range $[1..25]$

Key Space = 25

<u>Affine Cipher</u>

Caesar cipher required <u>additive</u>
Affine requires <u>mult. inv.</u>

$$E_{\alpha,\beta}(x) = (\alpha x+\beta) \bmod 26$$

alpha in range $[1..26]$

if $\alpha = 1$, Affine becomes Caesar.

$$\begin{tikzcd} X \arrow[r, bend left, "E_{\alpha,\beta}(x)"] & Y \arrow[l, bend left, "D_{\alpha,\beta}(Y)"] \end{tikzcd}$$

Let

$$y \equiv \alpha x + \beta \pmod{26}$$

solve for x to find inverse

$$\alpha x = y - \beta \pmod{26}$$

Let $\gcd(\alpha, 26) = 1$

$$\alpha^{-1}\alpha x = \alpha^{-1}(y - \beta) \pmod{26}$$

$$x = \alpha^{-1} y - \alpha^{-1}\beta \pmod{26}$$

So

$$E_{\alpha,\beta}(x) = \alpha x + \beta \mod 26$$

$$D_{\alpha,\beta}(x) = \alpha^{-1} x + (-\alpha^{-1})\beta \mod 26$$

Ex x in range $[0..25)$

α " " $[1..25]$

$\beta \in \{$ all odd integers in range $[1..25]$ except 13 $\}$

Notice

D is just E with

$\alpha = \alpha^{-1}$

$\beta = -\alpha^{-1}\beta$

Ex

'G' Pos('G') = 6

$\alpha = 11$
$\beta = 5$

$E_{11,5}(6) = (66 + 5) \bmod 26$
$= 19 \longrightarrow$ 'T'

To Decrypt we need

$\alpha^{-1} \bmod 26$

in Sage
11.inverse_mod(26) or
inverse_mod(11,26)

notice $11 \cdot 19 \% 26 = 1$

$E_{19,-19 \cdot 5}(19) = (19 \cdot 19 - 95) \% 26$

or using Addition theorem and
modular reduction

$E_{19,-19 \cdot 5}(19) =$

$E_{19,7 \cdot 5}(19)$

$E_{19,9}(19) = (19 \cdot 19 + 9) \% 26$

$= 6 \to$ 'G'

Key Space

α = 12 possibilities
β = 26 possibilities

$12 \cdot 26 = 312$

But $\alpha = 1$, $\beta = 0$ no shift

Key space : 311

Transposition is an enormous improvement.

But still vulnerable to freq analysis.

Polyalphabetic Cipher.
Blaise Vigneue | 16th century
envoy to Vatican

Caesar ; Affine mono alphabetic
→ shift along a single alphabet

Vigneue Polyalphabetic Cipher.

Step 1
generate a string of chars: key
"THIS WASAKEY

PT:	M	E	E	T	M	E	AT	TEN	TODA
Key:	T	H	I	S	W	A	SA	KEY	THIS

Pos('H') = 7
Pos('E') = 4
11

Pos('I') = 8
Pos('E') = 4
12

ch(11) = 'L'

ch(12) = 'M'

You get the idea

Key is a vector, Our Example

[19, 7, 8, 18, 22, 0, 18, 0, 10, 4, 24]

Caesar is a Vignere like this
[β] → KeySpace = 26

Vignere[β_1, β_2, ..., β_N]
where there are 26 possibil
for each β_k

KeySpace Vignere: 26^N
where N = key length

Thought to be unbreakable

Charles Babbage was one of the first to break it.

Tech

Why → Same letter can be encrypted multiple ways

~~Still if you can find the key length susceptible to frequency analysis~~

Vignere Sq. Geeks for Geeks

Key: AYUSH
PT GEEKS

Enc

Row G, Col A → Cell G Row is PT
Row E, Col Y → Cell C

⋮

Dec

Row A, Cell G → Col G Row is key
Row Y, Cell C → Col E

Attacks

(1) known PT
have some CT and corresponding PT

Let P_j be jth char in PT
Let K_j be corresponding key.

$$C_j = P_j + K_j \mod 26$$

$$C_j - P_j = \underline{\underline{K_j}} \mod 26$$

↳ a character of the key

(2) chosen PT

Eve chooses PT and is given CT

choose 0

$$(0 + K_j) \mod 26 = K_j$$

↳ a character of the key

(3) CT only is hard

Technique
- find key length
- freq analysis w/in subsets.

Project - Break Vigenere

- Kasiski attack (Kahn, pp207 ff
- Scientific American
  1/14/1917

- Trappe & WA