The Time Pad

Slides on perfect Secrecy

(1) Encode a Message as a Sequence of bits

(2) Randomly generate a key
- Sequence of bits
- As long as the PT.

(3) XOR PT with K

Ex PT: 00101101
K: 11001000
CT: 11100101
K: 11001000
PT: 00101101

enc $CT = PT \oplus K$ →

dec $(PT \oplus K) \oplus K$ →

$PT \oplus (K \oplus K)$ →

$PT \oplus 0 = PT$

Why $0 \oplus 0 \rightarrow 0$

$1 \oplus 0 \rightarrow 1$

Considerations

(1) key must be random
(2) key must be as long as PT
(if shorter it becomes Vigenere)
(3) key must not be reused
(4) key Dist. problem

Gen Random Seq

- Coin flips
- Count geiger counter clicks
  - even
  - odd
- Linear Congruential Generator
- Blum Blum Shub pseudo random bit generator

lastT

no pos. integers a, b, c satisfy

$c^n = a^n + b^n$ if $n > 2$

Fermat's Little theorem

Let p be prime and a an integer s.t. $p \nmid a$

Then $a^{p-1} \equiv 1 \mod p$

Ex 1 $p = 5$

$a = 3$

$3^4 \equiv 81 \equiv 1 \mod 5$

So 3 is the MI of $3^3 \mod 5$

b.c. $3 \cdot 3^3 = 3^4 \equiv 1 \mod 5$

Ex 2

Show $5^{38} \equiv 4 \mod 11$

by Fermat 11 is prime $11 \nmid 5$

$5^{10} \equiv 1 \mod 11$

$5^{38} = (5^{10})^3 \cdot 5^8$

$\equiv 5^8 \mod 11$

$\equiv (5^2)^4 \mod 11$

but $5^2 \equiv 3 \mod 11$

so $(5^2)^4 \equiv 3^4 \mod 11$

$\equiv 81 \mod 11$

$\equiv 4 \mod 11$

Proof of Fermat

Consider the first $p-1$ multiples of a

$Q_1 = \{a, 2a, 3a, \ldots, (p-1)a\}$

Claim

(1) none are congruent mod p

(2) none are congruent to 0

(1) Suppose

$ra \equiv sa \mod p \quad 1 \le r < s \le p-1$

$\gcd(a,p) = 1$ by assumption

$r \equiv s \mod p$

$r - s = kp$ and $p \mid r-s$

Not possible b.c. $r-s < p$

(A) Suppose $r > s$

$r - s \le p-1 < p$

(B) Suppose $r < s$

$r - s \ge 1$

But since $s \le p-1$

(A) none are divisible by p
(B) none are cong. to one another mod p

Without a/c mod p there are only $p-1$ residues, $\therefore$ q must be cong mod p TO $1 \ldots p-1$.

(2) Suppose

$$ra \equiv 0 \bmod p \qquad 1 \le r \le p-1$$

NOT possible b.c.
$p \nmid a$ by supposition
$p \nmid r$ b.c. $r < p$

(1) and (2) imply that $a, 2a, \ldots, (p-1)a$ are congruent TO $1, 2, \ldots, (p-1) = Q_2$
Taken in some order

Since if $a \equiv b$ and $c \equiv d \bmod p$
$ac \equiv bd \bmod p$

We can multiply the elements of Q_1 and Q_2 TO obtain

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \bmod p$$

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \bmod p$$

but $p \nmid (p-1)!$

so

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

Ex

Show $10^{37} \equiv 12 \mod 13$

By Fermat

$10^{12} \equiv 1 \mod 13$

$10^{37} = 10^{12} \cdot 10^{12} \cdot 10^{3}$

$10^{37} \equiv 10^{3} \equiv 12 \mod 13$

Fermat Corollary

If p is prime

$a^p \equiv a \mod p$ $\forall$ all integers a

not those in which $p \mid a$

Case 1 $p \mid a$

$a \equiv 0 \mod p$

$a^p \equiv 0^p \equiv 0 \mod p$

$a^p \equiv a \mod p$

Case 2 $p \nmid a$

$a^{p-1} \equiv 1 \mod p$ by Fermat

$a^p \equiv a \mod p$

Ex Show that 117 is composite

Find a s.t.

$a^{117} \not\equiv a \pmod{117}$

p is not prime by the following

Let $a = 2$

$2^{117} = 2^{7 \cdot 16 + 5} = (2^7)^{16} \cdot 2^5$

$2^7 = 128 \equiv 11 \pmod{117}$

$2^{117} \equiv (11)^{16} \cdot 2^5 \equiv (121)^8 \cdot 2^5 \pmod{117}$

$\equiv 4^8 \cdot 2^5 \pmod{117}$

$\equiv 2^{16} \cdot 2^5 \pmod{117}$

$\equiv 2^{21} \pmod{117}$

$\equiv (2^7)^3 \pmod{117}$

$\equiv 11^3 \pmod{117}$

$\equiv 121 \cdot 11 \pmod{117}$

$\equiv 4 \cdot 11 \pmod{117}$

$\equiv 44 \pmod{117}$

but

$44 \not\equiv 2 \pmod{117}$, so 117 is not prime

Def

ϕ Euler Totient function
denoted $\phi(N)$

$\phi(N)$ = number of integers $< n$
that are relatively prime to n

Ex $\phi(30) = 8$

$\{1, 7, 11, 13, 17, 19, 23, 29\}$

$\phi(1) = 1$, $\phi(2) = 1$, $\phi(4) = 2$

$\phi(5)$ ... $= 1$ b.c. $\gcd(1,2) = 1$
There are no others

$\phi(15)$ ...

Properties of ϕ

① $\phi(1) = 1$ b.c. $\gcd(1,1) = 1$

② $\phi(n) = n-1$ iff n is prime

Ⓐ if n is prime then $\phi(n) = n-1$
pf. if n is prime then
every integer $< n$ is
relatively to n

$\Rightarrow$

(B) if $\phi(n) = n-1$ then n is prime

prove contrapositive

if n is NOT prime then $\phi(n) \neq n-1$

n is comp. Then n has a divisor d s.t. $1 < d < n$

Do there at least 2 integers among $1, 2, 3, \ldots, n-1$ that not relatively prime to n

Do

if n is comp. $\phi(n) \neq n-1$

and

if $\phi(n) = n-1$ then n is prime

x	y	$x \Rightarrow y$	$\sim x$	$\sim y$	$\sim y \Rightarrow \sim x$
0	0	1	1	1	1
0	1	1	1	0	1
1	0	0	0	1	0
1	1	1	0	0	1

Theorem
ϕ Counter
if p is prime and $k>0$

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right)$$

Ex $p=2$, $k=3$

$\phi(2^3) = 2^3 - 2^2$ 1 3 5 7 ϕ

1 2 3 4 5 6 7

pf
$\gcd(n, p^k) = 1$
only if $p \nmid n$

Notice there are p^{k-1} integers between 1 and p^k divisible by p.

$p, 2p, 3p, \ldots, p^{k-1}p$

i.e. all multiples of p

The rests the integers in the are relatively prime to p^k.

$1, \ldots, p, \ldots, 2p \ldots p^k$

so $\phi(p^k) = p^k - p^{k-1}$

none $p^1, p^2, p^3 \ldots p^{k-1}$ are in this set

Ex $\phi(16)$

$\phi(2^4)$

remove mults. of 2

1 ~~2~~ 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~

$16 - 8 = 8$

$\phi(2^4) = 2^4 - 2^3 = 8$

We know how to find $\phi(n)$ for primes n

Find $\phi(n)$ for composite n

Lemma necessary to prove next theorem.

Given integers a, b, c

$\gcd(a, bc) = 1$ iff $\gcd(a, b) = 1$
$\gcd(a, c) = 1$

i.e. given a composite $a = bc$ and a one rel. prime to b and c, a is rel. prime to bc.

QED

(proof Burton, p. 130

Leads TO

Multiplicative Function Th.

if m, n are positive integers with $\gcd(m,n) = 1$

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

Proof: Burton p. 131
a very long proof

Ex $\phi(35) = 5 \cdot 7$

$\gcd(5,7) = 1$

$\phi(35) = \phi(5 \cdot 7) = \phi(5) \cdot \phi(7)$

$= \phi(5) = 4$ prop. of ϕ
$\phi(7) = 6$

$\phi(35) = 24$

$\phi(5)$

1, 2, 3, 4 (4)

$\phi(7)$

1, 2, 3, 4, 5, 6 (6)

$\phi(35) = 24$

1 2 3 4 6 8 9 11 12 13 14
17 18 19 22 23 24
26 27 29 31 32 33 34

$\phi(5)\,\phi(7) = 24$

Can be made canonical

Th. If $n > 1$ is an integer with prime factorization

$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ then

$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$

Pull $p_1^{k_1}$ from Term 1

$p_2^{k_2}$ from Term 2

$\vdots$

ϕ (since $n = p_1^{k_1} \cdots p_r^{k_r}$

ϕ knowing $(p_1^{k_1} - p_1^{k_1-1}) = p_1^{k_1}\left(1 - \frac{1}{p_1}\right)$

$(p_2^{k_2} - p_2^{k_2-1}) = p_2^{k_2}\left(1 - \frac{1}{p_2}\right)$

$\vdots$

$= 1 - \frac{1}{p_1}$

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

Ex: $\phi(360)$

$360 = 2^3 \cdot 3^2 \cdot 5$

$\phi(360) = 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$

$= 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 96$

Proof by PMI

Base Case $r=1$

$$\phi(p) = p - p^{-1} = p\left(1 - \frac{1}{p}\right) = p-1$$

which is also what ϕ counter tells us.

Assume T for $r=1$

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_i^{k_i} - p_i^{k_i-1})$$

True that

$$\gcd(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}, p_{i+1}^{k_{i+1}}) = 1$$

so by mult. funct.

$$\phi(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}, p_{i+1}^{k_{i+1}}) =$$

$$\phi = \phi(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}) \cdot \phi(p_{i+1}^{k_{i+1}})$$ get the P. Ih

By hyp.

$$\phi(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_i^{k_i} - p_i^{k_i-1})$$

$$\phi = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_i^{k_i} - p_i^{k_i-1}) \cdot (p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1})$$

which is what we want to show

Euler

Recall Fermat

Let p be a prime $p \nmid a$

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

Euler's theorem

For any integer a, n with $\gcd(a,n) = 1$, $n \geq 1$

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

Notice n does not have to be prime.

If n were prime we'd

Euler becomes Fermat

$a^{n-1} \equiv 1 \bmod n$

So Euler is a generalization of Fermat.

Proof is very similar to the proof of Fermat

Ex

$n = 15 = 3 \cdot 5$

$\phi(15) = \phi(3) \cdot \phi(5)$

$= 3\left(1 - \frac{1}{3}\right) \cdot 5\left(1 - \frac{1}{5}\right)$

$= 3-1 \cdot 5-1 = 8$

{1 2 4 7 8 11 13 14} rel prime to 15

Let $a = 4$

By Euler

$4^{\phi(15)} \equiv 1 \mod 15$

$4^8 \equiv 1 \mod 15$

$4^8 = (4^2)^4 \equiv 1 \mod 15$

$1 \equiv 1 \mod 15$

Ex

Find the last two digits in 3^{256}

Eq question

Find smallest $n \geq 1$ s.t.

$$13^{256} \equiv n \bmod 100$$

Euler

$n \geq 1$ $\gcd(a, n) = 1$

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

let $n = 100$

$$\phi(100) = \phi(2^2) \cdot \phi(5^2)$$

$$= 2^2\left(1 - \frac{1}{2}\right) \cdot 5^2\left(1 - \frac{1}{5}\right)$$

$$= (4 - 2) \cdot (25 - 5)$$

$$= 2 \cdot 20 = 40$$

So

$$3^{40} \equiv 1 \bmod 100$$

$$3^{256} = (3^{40})^6 \cdot 3^{16}$$

$$\equiv 3^{16} \bmod 100$$

$3^{16} \equiv (3^4)^4 \equiv (81)^4 \pmod{100}$

But $81 \equiv -19 \pmod{100}$

So

$3^{16} \equiv (81)^4 \equiv (-19)^4 \equiv (361)^2$

notice $361 \equiv 61 \pmod{100}$

So $\equiv (61)^2 \pmod{100}$

$\equiv 21 \pmod{100}$

So last two digits of $3^{256} = 21$

Ex Find $27^{100} \pmod{64}$

By Euler

$\gcd(27, 64) = 1$

so $27^{\phi(64)} \equiv 1 \pmod{64}$

$\phi(64) = \phi(2^6) = 2^6\left(1 - \frac{1}{2}\right)$

$= 32$

$27^{32} \equiv 1 \pmod{64}$

$$27^{100} = (27^{32})^3 \cdot 27^4$$

$$27^{100} \equiv 27^4 \pmod{64}$$

Notice

$$27^2 \equiv 25 \pmod{64}$$

$$\begin{array}{r} 11 \\ 64 \overline{)729} \\ \underline{64} \\ 89 \\ \underline{64} \\ 25 \end{array}$$

$$27^{100} \equiv (25)^2 \bmod 64$$

$$\equiv 49 \bmod 64$$

Inverses

Use Euler to find MI

if $n \geq 1$ and $\gcd(a,n) = 1$

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

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

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

Ex Find $9^{-1} \pmod{14}$

$\phi(14) = \phi(2)\,\phi(7)$

$= 2\left(1-\frac{1}{2}\right) \cdot 7\left(1-\frac{1}{7}\right)$

$= 1 \cdot 6 = 6$

So $9^{-1} \equiv 9^{6-1} \bmod 14$

$\equiv 9^5 \bmod 14$

$\equiv (3^2)^5 \bmod 14$

$\equiv (3^3)^3 \cdot 3 \bmod 14$

$\equiv (13)^3 \cdot 3 \bmod 14$

$\equiv 13^2 \cdot 39 \bmod 14$

$169 - 1 = 12 \cdot 14$

$\equiv 13^2 \cdot 11 \bmod 14$

Notice $14 \cdot 12 = 168$

so $13^2 \equiv 1 \bmod 14$ $\quad 1 \cdot 69 \equiv 1$

$\equiv 11 \bmod 14$

$9^{-1} \equiv 11 \bmod 14$

$11 \cdot 9 = 99 \equiv 1 \bmod 14$

$14 \overline{)99}$ R 1

Closer to home

Find $11^{-1} \bmod 26$

$26 = 2 \cdot 13$

$\phi(26) = \phi(2)\,\phi(13)$

$= 2\left(1-\frac{1}{2}\right) 13\left(1-\frac{1}{13}\right)$

$= 1 \cdot 12 = 12$

by Euler INV.

$11^{12-1} \equiv 11^{-1} \bmod 26$

$11^{11} \equiv 11^{-1} \bmod 26$

Now $11^3 = 1331 \equiv 5 \bmod 26$

$11^{11} \equiv (11^3)^3 \cdot 11^2$

$\equiv 5^3 \cdot 11^2 \bmod 26$

$\equiv 125 \cdot 17 \bmod 26$

$\equiv 21 \cdot 17 \bmod 26$

$\equiv 19 \bmod 26$

$26 \overline{)125}$ 4
104
21

$11 \cdot 19 \equiv 1 \bmod 26$

Euler I) $\gcd(a,n)=1 \quad a^{\phi(n)} \equiv 1 \bmod n$

Euler inv: $a^{\phi(n)-1} \equiv a^{-1} \bmod n$

Chinese Remainder Th.

(pf) Burton, p78

Let $n_1, n_2, \ldots n_r$ be positive integers s.t. $\gcd(n_i, n_j) = 1$ for $i \neq j$

Then the system of linear congruences

$$x \equiv a_1 \bmod n_1$$
$$\equiv a_2 \bmod n_2$$
$$\vdots$$
$$\equiv a_r \bmod n_r$$

has a solution which is unique mod $n_1 n_2 \ldots n_r$

To find Solution

Let $n = n_1 \cdot n_2 \cdot \ldots \cdot n_r$

For each $k = 1, 2, 3, \ldots, r$

Let

$$N_k = \frac{n}{n_k} = n_1 \cdot n_2 \cdots n_{k-1} \cdot n_{k+1} \cdots n_r$$

Choose $x_1, x_2, \ldots, x_r$

s.t. $N_k x_k \equiv 1 \bmod n_k$

Then

$$x = a_1 N_1 x_1 + \cdots + a_r N_r x_r \mod n$$

Ex (Sun Tsu)

Find a number that leaves remainders 2, 3, 2 when divided by 3, 5, 7

i.e. find x s.t.

$$\begin{aligned} x &\equiv 2 \mod 3 \\ &\equiv 3 \mod 5 \\ &\equiv 2 \mod 7 \end{aligned}$$

$n = 3 \cdot 5 \cdot 7$

$N_1 = \frac{105}{3} = 35$

$N_2 = \frac{105}{5} = 21$

$N_3 = \frac{105}{7} = 15$

$35 \cdot x_1 \equiv 1 \mod 3$

$21 x_2 \equiv 1 \mod 5$

$15 x_3 \equiv 1 \mod 7$

Find

$35^{-1} \mod 3$
$21^{-1} \mod 3$
$15^{-1} \mod 3$

$x_k \equiv N_k^{-1} \mod n_k$

Use Euler

$a^{\phi(n)-1} \equiv a^{-1} \mod n$

$\gcd(35,3) = 1 \quad \phi(3) = 2$

$35^{-1} \equiv 35^{2-1} \mod 3$

$\equiv 2$

$\gcd(21,5) = 1 \quad \phi(5) = 4$

$21^{-1} \equiv 21^{3} \mod 5$

$\equiv 1 \cdot 1 \cdot 1 \mod 5$

$21^{-1} \equiv 1 \mod 5$

$\gcd(15,7) = 1 \quad \phi(7) = 6$

$15^{-1} \equiv 15^{5} \mod 7$

$\equiv 1^{5} \mod 7$

$\equiv 1 \mod 7$

$X \equiv (a_1 n_1 x_1 + a_2 n_2 x_2 + a_3 n_3 x_3) \pmod{105}$

$\equiv (2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1) \mod 105$

$\equiv (140 + 63 + 30) \mod 105$

$\equiv 23 \mod 105$

Try

$23 \equiv 2 \mod 3$

$23 - 2 = 21 = 7 \cdot 3$ ✓

$23 \equiv 3 \mod 5$

$23 - 3 = 20 = 4 \cdot 5$ ✓

$23 \equiv 2 \mod 7$

$23 - 2 = 21 = 3 \cdot 7$ ✓