1/26

- Shift cipher (only 26 keys)
  enc: $x \longmapsto x+k \bmod 26$
  dec $y \longrightarrow y-k \bmod 26$

- Affine Ciphers
  choose 2 integers α and β and msg x

  $x \longmapsto \alpha x+\beta \pmod{26}$
  $\alpha \neq 0$, α must be relatively prime to 26 (has no divisors in common with 26) ie 1, 3, 5, 7, 9, 11, 15, 17 ...
  no β restrictions

  key is the pair (α, β) 12 x 26 keys possible (312)
  ex: encrypt "Hello" $\alpha=3$ $\beta=12$

  $a = 0 \rightarrow 3(0)+12 = m$

  $t = 19 \rightarrow 3(19)+12 = 57+12 = 69 \bmod 26 = 17 = R$

  $c = 2 \rightarrow 3(2)+12 = 6+12 = 5$

  $k = 10 \rightarrow 32 \bmod 26 = 16 = q$ attack $\longmapsto$ mRRmSq

  decryption:
  cipher text: "0"
  $3x+12 = 14$
  $3x \equiv 2 \bmod 26$
  $3^{-1} \cdot 3^{-1}$
  $x \equiv 18 \bmod 26 \longmapsto S$

  $3 \cdot 9 \equiv 1 \bmod 26$ (9 is inverse of 3 mod 26)
  $3^{-1} \equiv 9 \bmod 26$

  in general if we know
  $3x+12 = y \bmod 26$
  $3x \equiv y-12 \bmod 26$
  $3^{-1} 3x \equiv 3^{-1}(y-12) \bmod 26$
  $x \equiv 9(y-12) \bmod 26$
  $x \equiv 9y-108 \bmod 26$
  $\equiv 9y-4 \bmod 26$

Def.

- A multiplicative inverse for $a \bmod m$ is an integer b, such that

$$a \cdot b \equiv 1 \pmod{m} \qquad b \equiv a^{-1} \bmod m$$

- Theorem:
$a \in \mathbb{Z}$ has a MI $\bmod m$ iff $\gcd(a, m) = 1$ i.e. a, m are r.p

decrypt affine cipher

$$\alpha x + \beta \equiv y \bmod 26$$
$$\alpha x \equiv y - \beta \bmod 26$$
$$\alpha^{-1} \alpha x \equiv \alpha^{-1}(y - \beta) \bmod 26$$
$$x \equiv \alpha^{-1}(y - \beta) \bmod 26$$
$$x \equiv \alpha^{-1} y - \alpha^{-1} \beta \pmod{26}$$

if $\gcd(\alpha, 26) \neq 1$ then decryption isn't possible

V29

2.3 Vigenère Cipher
Key is a "word" any length, vector of integers [0,25]

eg: "code" → (2,14,3,4)

this is how it works

plain 19 7 8 18 8 18 7 14 22 8 19 22 14 17 10 18
+
key (2 14 3 4)..... 2 14 3 4

= 21 21 11 22 10 6 10 18 24 22 22 0 16 5 13 22

V V O W K G S Y W W A Q F N W

key + length secret

2.4 substitution cipher (shift left one) (26! keys)
each letter is replaced by another (possibly the same one)

e.g. A → D
B → Q
C ...
no duplicates!

malicious goals: Read msg, find key, Corrupt messages, identity theft

1) confidentiality: can't read intercepted msg
2) Data integrity: make sure msg wasn't manipulated
3) Authentication: make sure sent from person we know
4) non repudiation: can't claim you didn't send message

Attacks on Cryptosystems:

Kerchoffs Principle: always assume enemy has algorithm you're using for encryption

So the keyspace should be large to prevent brute force attacks in which one decrypts the ciphertext using all possible keys

1) ciphertext only: eve has only the ciphertext
2) Knownplaintext attack: eve has ciphertext and corresponding plaintext.
3) chosen plaintext attack: eve gains access to encryption machine and works out the algorithm (encrypts msgs of her choosing)
4) chosen ciphertext attack: gains access to decryption machine

1/31

Ex: Attacking a shift cipher
$x \to x+k \bmod 26$

hardest (ciphertext only): Brute force 26 keys
Known Plaintext: easy, all shifted by same amount
chose plaintext: encrypt one letter $0 \to 0+k = K$

Ex: $x \to \alpha x+\beta$
ciphertext only → Bruteforce, only 12 α's and 26 β's
Known Plaintext: One can deduce the key by knowing how 2 letters encrypt.
eg: $0(14) \to D(3)$
$F(5) \to S(18)$

$\alpha(14)+\beta \equiv 3 \bmod 26$
$\alpha(5)+\beta \equiv 18 \bmod 26$

$\alpha 9 \equiv -15 \bmod 26$
$\alpha 9 \equiv 11 \bmod 26$

$\alpha 27 \bmod 26 \to \alpha \bmod 26 \equiv 33 \bmod 26$
$\hookrightarrow \alpha \bmod 26 \equiv 7 \bmod 26$

$\beta = 4$

chosen plaintext: choose "ab" ↺ 1
Y_0, Y_1 be ciphertext as #s
$0 \to Y_0$ $\alpha(0)+\beta = Y_0$ $\alpha(1) \equiv Y_1 - \beta$
$1 \to Y_1$ $\beta = Y_0$ $\alpha = Y_1 - Y_0$

Shift / Affine / substitution vulnerable to a frequency analysis of the letters

certain letters more common than other letters

substitution: BF resistant

Vigenere ciphers attacks

if key length is known and text is long then do frequency analysis to make educated guesses for the shift amounts.

n=6 look at: 1, 7, 13...

- Given ciphertext encrypted by a vigenere cipher, how to guess key length?
  2 letters randomly chosen $\frac{1}{26}$ chance they're the same.
- from english text.

Attacking Vigenere cipher (ciphertext only)
Find the key length n

- 2 letters randomly chosen from the alphabet
probability of getting same letter twice $= \frac{1}{26} \approx .038$

- 2 letters from english text at random prob is
$P(A')P(A'') + P(B')P(B'') + \dots + P(z')P(z'')$
$(.082)^2 + (.015)^2 + \dots + (.001)^2$

$= .066$

To find key length (vigenere)
For each $n = 2, 3, \dots$

in the ciphertext, count # of times that

$C_j = C_{j+n}$ (ciphertext letters are the same)

n with the most coincidences is the likely key length (long ciphertext)

Vigenere not secure if key length << message length

---

theory
$a, b \in \mathbb{Z}$ $a \neq 0$

$a \mid b$ if $\exists k \in \mathbb{Z}$ s.t. $b = a \cdot k$

Proposition $a, b, c \in \mathbb{Z}$

1) $\forall a \neq 0$, $a \mid a$ $a \mid 0$ $1 \mid a$
2) if $a \mid b$ and $b \mid c \rightarrow a \mid c$
3) $a \mid b$ and $a \mid c \rightarrow a \mid (sb + tc)$ $s, t \in \mathbb{Z}$

pf2) $a|b$ & $b|c$

$b = ka \quad c = bq \quad k, q \in \mathbb{Z}$

$c = (ka)q$
$c = (kq)a$
$c = la \qquad kq = l \in \mathbb{Z}$
$\therefore a|c$

pf3) $a|b$ & $a|c$

$b = ka \quad c = la \quad , k, l \in \mathbb{Z}$

Then $sb + tc$

$s(ka) + t(la)$
$(sk)a + (tl)a$
$a(sk + tl)$
$\therefore a|(sb+tc)$

Primes #

Def $p \in \mathbb{Z}$, $p > 1$ s.t. $1|p$ and $p|p$

Def $n \in \mathbb{Z}$ $n > 1$ and ¢Prime is called composite

Composite n can always be written as a product $n = ab$ $1 < a, b < n$

variety of prime #'s random 9 digit #, chances it's prime?

Prime # theorem: let $\pi(x)$ = # of primes $\leq x$

Then $$\pi(x) \approx \frac{x}{\ln(x)}$$

in the sense that $\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1$

so the # of primes with 9 or fewer digits given by $\pi(10^9) \approx \frac{10^9}{\ln(10^9)} = \frac{10^9}{9\ln(10)}$

randomly select a #, probability of prime: $\frac{\pi(x)}{x}$

FTOA

Every positive int is a product of primes, unique factorization

Primes only have 1 factor

Uniqueness proof of FTOA requires the following:
euclid's lemma: Let a, b be integers, p is a prime if $p \mid a \cdot b$ then $p \mid a$ or $p \mid b$ (or both)

More generally if $p \mid (a_1 \cdots a_n)$, then p divides a_i for some i

gcds

- Defn: $a, b \in \mathbb{Z}$ (not both 0)

  the gcd is the largest positive integer that divides both a and b

  $\gcd(a,b) = \gcd(|a|, |b|)$

- relatively prime $\gcd(a,b) = 1$

- how to find gcds?
  Use prime factorizations

  fine for small # hard for large #s

- euclidean algorithm:
  Lemma: $a, b, q, r \in \mathbb{Z}$ $a = bq + r$ then
  $\gcd(a,b) = \gcd(b,r)$

Euclidean Algorithm
$a, b, q, r \in \mathbb{Z}$ st

$a = bq + r$ then

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

Euclidean algorithm
$\gcd(12345, 4002)$

$12345 = 3(4002) + 339$

$4002 / 339$

$4002 = 11(339) + 273$

$339 = 273 + 66$

$273 = 4(66) + 9$

$66 = 7(9) + 3$

$\gcd = 3$

- Bezout identity
$d = \gcd(a,b)$
$\exists\ x, y \in \mathbb{Z}$ st
$d = ax + by$

Ex: gcd (405, 2145)
express as lin. comb

$2145 = 5(405) + 120$

$405 = 3(120) + 45$

$120 = 2(45) + 30$

$45 = 1(30) + 15$ gcd

$30 = 15 \cdot 2 + 0$

$120 = 2145 - 5(405)$

$45 = 405 - 3(120)$

$30 = 120 - 2(45)$

$15 = 45 - 30$

$15 = 45 - 30$

$45 - (120 - 2(45))$

$= 3(45) - 120$

$= 3(405 - 3(120)) - 2145 + 5(405)$

$3(405) + 9(120) - 2145 + 5(405)$

$8(405) - 9(120) - 2145$

$-9(2145 - 5(405)) - 2145$

$8(405) + -9(2145) + 45(405) - 2145$

$-10(2145) + 53(405) = 15$

3.3

Congruences $a, b, n \in \mathbb{Z}$ $n \neq 0$

$a \equiv b \mod n$ (a congruent to b mod n)

$n \mid (a-b)$

$a - b = kn \quad k \in \mathbb{Z}$

$a = b + kn$

$a \equiv 0 \mod 2$ a is even

$a \equiv 1 \mod 2$ a is odd

if a is divided by n to give q and r

$a = nq + r$

$a \equiv r \mod n$

$a \equiv b \bmod n$

$n \mid a-b \qquad a = b + nk$ for some k

Proposition

$a, b, c, n \in \mathbb{Z}$ with $n \neq 0$

1) $a \equiv 0 \bmod n \leftrightarrow n \mid a$
2) $a \equiv a \bmod n$
3) $a \equiv b \bmod n \rightarrow b \equiv a \bmod n$
4) $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$

Modular arithmetic: For positive integer n
Let $\mathbb{Z}_n = \{0, \ldots, n-1\}$ we do addition/multiplication mod n with elements of $\mathbb{Z}_n$ we'll end up with an element in $\mathbb{Z}_n$ from 0 to $n-1$

mod 5 ($\mathbb{Z}_5$)

$2+4 \equiv 1 \bmod 5$

$2 \cdot 4 \equiv 3 \bmod 5$

Proposition Let $a, b, c, d \in \mathbb{Z}$ with $n \neq 0$

$a \equiv b \bmod n \qquad c \equiv d \bmod n$

$a + c \equiv b + d \bmod n$

$ac \equiv bd \bmod n$

ex: $89 \cdot 51 + 109 \bmod 21$

$89 \equiv 5 \bmod 21$

$51 \equiv 9 \bmod 21$

$109 \equiv 4 \bmod 21$

$89 \cdot 51 + 109 \equiv 5 \cdot 9 + 4 = 49 \bmod 21 \equiv 7 \bmod 21$

- $88^8 \bmod 79 \equiv 9^8 \bmod 79$

  $9^2 = 81 \equiv (2)^4 \bmod 79 \equiv 16 \bmod 79$

- Ex Find last 2 digits of 97^3

  $97^3 \equiv (-3)^3 \equiv -27 \bmod 100$
  $\equiv 73 \bmod 100$

- Mutiplicative inverse
  $a, b, n \in \mathbb{Z} \quad n \neq 0$
  a MInv for a is an integer b such that
  $ab \equiv 1 \bmod n \quad a^{-1} \equiv b \bmod n$

- a has an inverse b iff $\gcd(a,b) = 1$

- Let p be a prime and $a \not\equiv 0 \bmod p$ then a has an inverse $\bmod p$

- For large numbers do the extended euclidean algorithm for inverses

inverse of
$32 \bmod 101$

$101 = 32 \cdot 3 + 5$ $\qquad$ $5 = 101 - 32 \cdot 3$

$32 = 6 \cdot 5 + 2$ $\qquad$ $2 = 32 - 6 \cdot 5$

$5 = 2 \cdot 2 + 1$ $\qquad$ $1 = 5 - 2 \cdot 2$

$1 = 5 - 2(32 - 6 \cdot 5)$

$= (13)(5) + (-2)(32)$

$= 13(101 - 32 \cdot 3)$

$13(101) + 32(-41)$

$32(-41) \equiv 1 \bmod 41$

$32^{-1} = -41 \equiv 60 \bmod 101$

2/12

Linear congruences have form

$ax \equiv b \bmod n$ $\quad a, b, x, n \in \mathbb{Z}$

Solve for $x \bmod n$

if a^{-1} exists then you can multiply both sides by a^{-1} and solve for x

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

- if $\gcd(a, n) = 1$ then
  $ax \equiv b \bmod n$ has unique solution
  $x \equiv a^{-1} b \bmod n$

ex: solve

$32x \equiv 9 \bmod 101$

$32^{-1} \equiv 60 \bmod 101$

$x \equiv 60 \cdot 9 \bmod 101$

540

$x \equiv 35 \bmod 101$

$\gcd(a, n) > 1 \rightarrow$ 0 or many solutions

- let $d = \gcd(a, n)$

1) if $d \nmid b$ then $ax \equiv b \bmod n$ has no solutions

2) if $d \mid b$ then $ax \equiv b \bmod n$ has exactly d solutions $\bmod n$

ex:

$x \longrightarrow 6x+5 \mod 26$

"C" $\rightarrow$ $y=2$

Solve $6x + 5 \equiv 2 \mod 26$

$6x \equiv 23 \mod 26$

$\gcd(6,26) = 2$

$2 \nmid 23$ so no solutions

ex: "b" $y=1$

$6x+5 = 1$

$6x \equiv 22 \mod 26$

$(6,26) = 2$ $\quad 2 \mid 22$ ✓ so 2 solutions

$x \equiv 8, 21$ are the solutions

One time pad

XOR $0 \oplus 0 = 0$

$1 \oplus 0 = 0$

$1 \oplus 1 = 0$

key length = text length

1 0 1 1 0 1 0 1	text
$\oplus$ 1 1 0 1 0 1 1 1	key
0 1 1 0 0 0 1 0	ciphertext
1 1 0 1 0 1 1 1	key
1 0 1 1 0 1 0 1	text

key length = ciphertext length

Plaintext of n bits can be encrypted into 2^n possible ciphertexts

Conditional probability

For event A let P(A) denote the probability of A happening

For 2 events A + B $A \cap B$ is A and B both happening

Conditional probability of B given A is $P(B|A) = \frac{P(A \cap B)}{P(A)}$

$P(A \cap B) = P(A)\,P(B|A)$

events A B independent if

$P(A \cap B) = P(A) \cdot P(B)$

$P(B|A) = P(B)$

$P(A|B) = P(A)$

ex. 2 6 sided dice

$P(D_1 = 2) = P(D_2 = 6) = \frac{1}{6}$

$P(D_1 = 2 \cap D_2 = 6) = \frac{1}{36}$

So events are independent

$P(D_1 + D_2 \geq 8) = \frac{15}{36} = \frac{5}{12}$

$P(D_1 + D_2 \geq 8 \mid D_1 = 6) = \frac{5}{6}$

$P(D_1 + D_2 \geq 8 \mid D_2 = 2) = \frac{1}{6}$ (6)

$P(D_1 + D_2 \geq 8 \mid D_1 = 1) = 0$

in a crypto system we write
$M = m$ (plaintext)
$C = c$ (ciphertext)
$K = k$ key

if there are N keys and one is chosen randomly then $P(K = k) = \frac{1}{N}$ for each key k

Some plaintexts are more likely than others
eg $P(m = \text{"dog"}) > P(m = \text{"zyx"})$

each ciphertext c has probability
$P(C = c)$

Def: we say a crypto system is perfectly secret if

$$P(M = m \mid C = c) = P(M = m)$$

for all possible m and c

that is knowing $C = c$ doesn't affect the likelihood of $M = m$
so $M = m$ and $C = c$ are independent events

if key is uniformly random, then the OTP has perfect secrecy

Perfect secrecy $\iff$ $M = m$ & $C = c$ are independent

$\iff$ $P(C = c \mid M = m) = P(C = c)$

there are N keys then

$P(C = c) = 1/N$

2/16

Perfect secrecy $P(M=m \mid C=c) = P(M=m) \quad \forall m, c$

Proposition: If a cryptosystem has perfect secrecy, then the # of keys is greater than or equal to the # of possible plaintext

4.5 - indistinguishability and Security

ciphertext indistinguishability

Alice chooses 2 messages m_0, m_1 and gives them to Bob, Bob randomly picks either m_0 or m_1, encrypts it and sends the ciphertext c to Alice

alice guesses whether m_0 or m_1 was encrypted

If there is no strategy where she can guess correctly more than $1/2$ of the time we say the crypto system has ciphertext indistinguishability

OTP has this property

ex: shift cipher doesn't have this property

m_0 = "dog" m_1 = "cat" cipher text c = "VTM"

so we know m_2 was encrypted

Stream Cipher

We want an algorithmic way to generate a stream of bits to use as a key (like OTP)

Alice and Bob will agree on a way to generate the key (no need to transmit the key)

- 5.2 Linear Feedback Shift Registers

Speed vs security tradeoff irl

use recurrence relation mod 2

---

ex: $X_{n+5} \equiv X_n + X_{n+2} \pmod 2$ with IVs

$X_1 \equiv 0,\ X_2 \equiv 1,\ X_3 \equiv 0,\ X_4 \equiv 0,\ X_5 \equiv 1$

$X_1\ X_2 \ldots \quad X_6$

0 1 0 0 1 0 1 1 0 0 1 1 1 1 1 0 0 0 1 1 0 1 1 0 1 0 0

$X_6 \equiv X_1 + X_3 \equiv 0 + 0 \equiv 0 \bmod 2$

$X_7 \equiv X_2 + X_4 \equiv 1 + 0 \equiv 1 \bmod 2$

$X_8 \equiv X_3 + X_5 \equiv 0 + 1 \equiv 1 \bmod 2$

this recurrence relation can be described by $\{1, 0, 1, 0, 0\}$

$$X_{n+5} \equiv 1X_n + 0X_{n+1} + 1X_{n+2} + 0X_{n+3} + 0X_{n+4}$$

10 bits of ~~value~~ data gave a 31 bit key

(relation and initial value)

2/19

Linear Feedback shift Register

Recurrence : $X_{n+k} \equiv C_0 X_n + C_1 X_{n+1} + \cdots + C_{k-1} X_{n+k-1}$

initial bits $x_0, x_1, \ldots, x_{k-1}$

Alice + bob agree on $\{C_0, \ldots, C_{k-1}\}$

and $\{X_0, X_1 \ldots X_{k-1}\}$ 2k bits

independently they can generate a pseudo random stream of bits

very vulnerable to known plaintext attack

Knowing m and $c = m \oplus k$ means you know

$m \oplus c \Rightarrow m \oplus (m \oplus k) = k$

assume we know part of k and we can show how we can find all of k

ex 3 bits we know part of the key is

0 1 0 1 1 1 0 0 1

generated by $X_{n+3} = C_0 X_n + C_1 X_{n+1} + C_2 X_{n+2}$

Solve for C_0, C_1, C_2

0 1 0 1 1 1 0 0 1

$x_0 \equiv 0,\ x_1 \equiv 1,\ x_2 \equiv 0$

$x_3 \equiv c_0 x_0 + c_1 x_1 + c_2 x_2$

$1 \equiv c_0(0) + c_1(1) + c_2(0)$

$1 \equiv c_1$

$$\begin{cases} c_1 \equiv 1 \\ c_0 + c_2 \equiv 1 \\ c_1 + c_2 \equiv 1 \end{cases}$$

$c_1 \equiv 1$ $\quad$ $c_1 + c_2 \equiv 1$ $\quad$ $c_0 + c_2 \equiv 1$

$1 + c_2 \equiv 1$ $\quad$ $c_0 + 0 \equiv 1$

$c_2 \equiv 0$ $\quad$ $c_0 = 1$

Recurrence is

$x_{n+3} \equiv x_n + x_{n+1}$

Block ciphers

encrypt blocks of letters (# of bits) at once. Changing one letter in plaintext changes all letters in the ciphertext block

DES, AES, RSA

- Hill Ciphers

treat letters as integers mod 26 and use matrix multiplication to encrypt blocks of n letters at a time

$n=3$ $n \times n$ matrix entries $\in \mathbb{Z}_{mod 26}$

$$M = \begin{pmatrix} 2 & 7 & 1 \\ 3 & 4 & 3 \\ 1 & 1 & 5 \end{pmatrix}$$

multiply 1×3 vector with a 3×3 matrix via

$$(x \; y \; z) \begin{pmatrix} 2 & 7 & 1 \\ 3 & 4 & 3 \\ 1 & 1 & 5 \end{pmatrix} \equiv (2x+3y+z, \; 7x+4y+z, \; x+3y+5z)$$

3 letters as a 1×3 vector multiply by M to encrypt $\quad cry \to a \cdot (2, 17, 24)$

$a \cdot M \to (1 \; 2 \; 17)$

$cry \Rightarrow BCR \qquad dry \to DJS$

encrypt "Crypto" first do
"cry" then "pto"

Crypto ⇒ BCRXNM

dypto ⇒ DJSXNM

2/21

Hill ciphers

Use $n \times n$ matrix M to encrypt block of n letters (row vector $\vec{v}$ n entries) at a time

encrypt via $\vec{v}M$

decryption of Hill cipher need inverse matrix mod 26

matrix N s.t.

$$NM = MN = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & \ddots \\ & & & & 1 \end{pmatrix} \text{ mod } 26$$

$$M = \begin{pmatrix} 2 & 7 & 1 \\ 3 & 4 & 3 \\ 1 & 1 & 5 \end{pmatrix} \qquad N = \begin{pmatrix} 17 & 18 & 17 \\ 14 & 9 & 23 \\ 25 & 5 & 13 \end{pmatrix}$$

Theorem: $n \times n$ matrix M has a mod m inverse iff $\gcd(\det(M), m) = 1$

For a Hill cipher choose M s.t $\gcd(\det(M), 26) = 1$

$2 \times 2 \quad M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$M^{-1} = \frac{1}{\det(M)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

mod m inverse

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

$M = \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$

$\det M = 8 - 3 = 5$

$5^{-1} \equiv 21 \bmod 26$

$M^{-1} \equiv 5^{-1} \begin{pmatrix} 4 & -1 \\ -3 & 2 \end{pmatrix} \equiv 21 \begin{pmatrix} 4 & -1 \\ -3 & 2 \end{pmatrix} =$

$\begin{pmatrix} 84 & -21 \\ -63 & 42 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 6 & 5 \\ 15 & 16 \end{pmatrix} \bmod 26$

decrypt

6.3 Modes of Operation

Suppose we have a block cipher that encrypts plaintext blocks of a fixed size (eg 64 bit blocks)

what if plaintext is much longer? break it into blocks

$$P = [P_1, \ldots, P_L]$$

let K be the key, E_K / D_K be the encryption decryption functions

different approaches to encrypting P

6.3.1 ECB electronic code book

natural (naive): encrypt each block P_j using E_K. ie $C_j = E_K(P_j)$

for each j

Send $C = [C_1, \ldots C_L]$ to Bob

issue: same plaintext block always encrypts to the same ciphertext

6.3.2 Cipher Block chaining
previous cipher text block affects how the next block gets encrypted

$$C_j = E_k(P_j \oplus C_{j-1})$$

alice sends $[C_1, C_2, \ldots C_L]$ to Bob

decrypt

$$P_j \oplus C_{j-1} = D_k(C_j)$$

$$\Rightarrow \boxed{P_j = D_k(C_j) \oplus C_{j-1}}$$

for C_1 (no C_0 P_0)

could send $E_k(C_1)$ (bad)

Instead choose a random C_0 and sends to Bob $[C_0, C_1, C_2, \ldots, C_L]$

Ex: CBC with Hill cipher
replace $\oplus$ with + (mod 26)

encrypt "hahaha" using $M = \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$

ECB: ha → (7,0)

$(7,0)\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} = (14,7)$ "OH"

"hahaha" → "OHOHOH"

CBC $(C_0 = (0,0))$

- P_1 = "ha" gives C_1 = "OH" (14,7)
- P_2 = "ha" compute $P_2 + C_1 = (7,0) + (14,7) = (21,7$

encrypte $(21,7)\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} = (11,23)$ = "LX"

- P_3 = "ha" $P_3 + C_2 = (7,0) + (11,23) = (18,23)$

$(18,23)\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} = (1,6)$ = "BG"

"hahaha" = "OH LX BG"

"gahaha" → "MGERVB"

2/21

7 - DES data encryption standard

DES 56 bits (outdated)

In practice, Alice + Bob could send DES keys using public key cryptography

DES example of Feistel system

Features of Feistel:
- n rounds to encl/dec process (16 in DES)
- n subkeys (round keys) $K_1, \ldots, K_n$, derived from key K in a predetermined way
- A block being split into halves L_0, R_0
- each round transforms (L_{i-1}, R_{i-1}) into (L_i, R_i)
- function $f(R_{i-1}, K_i)$ must be chosen (by alg.) which outputs half blocks
- One round transforms $(L_{i-1}, R_{i-1}) \longrightarrow$ into $(R_{i-1}, L_{i-1} \oplus f(R_{i-1}, K_i))$

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

How to decrypt $c = L_n R_n$?
encrypt $R_n L_n$ using the reverse key schedule $K_n, K_{n-1}, \ldots, K_1$ to get $R_0 L_0$ and then flip flop

So in total

enc:

$(L_{i-1}, R_{i-1}) \Rightarrow (R_{i-1}, L_{i-1} \oplus f(R_{i-1}, K_i))$

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

and so decryption:

$(R_i, L_i) \rightarrow (L_i, R_i \oplus f(L_i, K_i))$

$\rightarrow (R_{i-1}, L_{i-1} \oplus f(R_{i-1}, K_i) \oplus f(L_{i-1}, K_i))$

$\rightarrow (R_{i-1}, L_{i-1})$

to design feistel system

- choose key schedule $(K_1, \ldots K_n)$ from K
- choose a function $f(R_{i-1}, K_i)$

no mathematical requirements

AES - Advanced Encryption Standard
allows for 128, 192, 256 bits

block cipher that operates on 128 bit blocks

AES has 10, 12, 14 rounds

a block is written as a 4x4 matrix of bytes

each round has
- substitution of bytes
- permutation of entries of the matrix
- multiplication by a matrix of bytes

3.4
Chinese Remainder Theorem
Possible to view a congruence with composite modulus as a system of congruences with smaller moduli

$x \equiv 7 \bmod 99 \quad (9, 11) = 1$

$x = 71 + 99k \quad k \in \mathbb{Z}$
$x = 71 + 9 \cdot 11 k$
$x \equiv 71 \bmod 9 \qquad x \equiv 71 \bmod 11$
$\equiv 8 \bmod 9 \qquad x \equiv 5 \bmod 11$

CRT, this can be reversed
$x \equiv 8 \bmod 9$
$x \equiv 5 \bmod 11 \Rightarrow x \equiv 71 \bmod 99$

ex
$x \equiv 2 \bmod 9 \Rightarrow x \equiv ? \bmod 99$
$x \equiv 7 \bmod 11$

$x \equiv 7 \bmod 11$

$x \equiv 2 \bmod 9$

$x \equiv 29 \bmod 11$

2, 11, 20, 29

$\bmod 11$ ↓

2, 0, 9, 7

Chinese Remainder Theorem

Suppose $\gcd(m, n) = 1$, Given integers a, b $\exists$ one unique solution $x \bmod mn$ to the system

$x \equiv a \bmod m$

$x \equiv b \bmod n$

By extended euclid algorithm $\exists$

$ms + nt = 1$

$ms \equiv 1 \bmod n \quad s \equiv m^{-1} \bmod n$

$nt \equiv 1 \bmod m \quad t \equiv n^{-1} \bmod m$

solution will be given by

$x = bms + ant$

$x \equiv a(t) \bmod m$

$x \equiv a(1) \bmod m$

$x \equiv a \bmod m$

$x \equiv bms \bmod n$

$\equiv b(1) \bmod n$

$x \equiv b \bmod n$

Ex $x \equiv 63 \mod 101$
$x \equiv 10 \mod 32$

do ext euclid algorithm $(101, 32)$
to get
$1 = 101(13) + 32(-41)$
The solution is
$x = 10(101(13)) + 63(32(-41))$
$x = -69526$
$x \equiv 1578 \mod 3232$

Solving $x^2 \equiv 1 \mod n$

if p is prime (odd) then
$x^2 \equiv 1 \mod p$ has only two solutions
1 and $-1 \mod p$

Ex: $x^2 \equiv 1 \mod 77 \leftrightarrow \begin{cases} x^2 \equiv 1 \mod 7 \\ x^2 \equiv 1 \mod 11 \end{cases}$

$x^2 \equiv 1 \mod 7 \rightarrow x \equiv \pm 1 \mod 7$
$x^2 \equiv 1 \mod 11 \rightarrow x \equiv \pm 1 \mod 11$

$(1, 1)$ $x \equiv 1 \mod 77$
$(-1, 1)$ $x \equiv 34 \mod 77$
$(1, -1)$ $x \equiv 43 \mod 77$
$(-1, -1)$ $x \equiv -1 \mod 77$

CRT (general form)

Let $m_1, \dots, m_k \in \mathbb{Z}^+$ with $(m_i, m_j) = 1$ $i \neq j$

given integers $a_1 \dots a_k$ $\exists$ one solution $x \bmod (m_1 \dots m_k)$

to the system

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \vdots \\ x \equiv a_k \bmod m_k \end{cases}$$

3.5 modular exponentiation

$m^e \bmod n$ can be large

ex: $21^{723} \bmod 809$

Repeatedly square 21, reduce mod 809

$21^2 = 441 \pmod{809}$

$21^4 = 321$

$21^8 = 298$

$\vdots$

$21^{512} = 692$

$723 = 512 + 128 + 64 + 16 + 2 + 1$

$21^{723} = 21^{512} \cdot 21^{128} \cdot 21^{64} \cdot 21^{16} \cdot 21^2 \cdot 21^1$

$= 692 \cdot (115)\ (76)\ (23)\ (441)(21) \bmod 809$

$= 94$

3.6 Fermat + Euler's

$m^e \bmod n$ m, e larger than n

$717^{368} \bmod 7$

$717 \equiv 3 \bmod 7$

$717^{368} \equiv 3^{368} \bmod 7$

$3^{368} \equiv 3^{366} \cdot 3^2 \bmod 7$

$(3^6)^{61} 3^2 \bmod 7 = 2$

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

- Fermat Little theorem

If p is Prime and $p \nmid a$ $(a \not\equiv 0 \bmod p)$

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

FLT: if p is prime and $p \nmid a$ then

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

$p \nmid a \iff a \not\equiv 0 \bmod p$

$\iff \gcd(a, p) = 1$

for prime modulus only

eg $2^8 \not\equiv 1 \bmod 9$

$\| \| \|$

4

ex $p = 41$ so $2^{40} \equiv 1 \bmod 41$

Simplify $2^{243} \bmod 41$

$$(2^{40})^6 \cdot 2^3 \bmod 41$$

1

$$\equiv 8 \bmod 41$$

Basic Principle: P be prime and let a, x, y be ints with $P \nmid a$

If $x \equiv y \bmod p-1$ then $a^x \equiv a^y \bmod p$

Pf: if $x \equiv y + (p-1)k$ then

$$a^x \equiv a^{y+(p-1)k} \equiv a^y a^{(p-1)k} \equiv a^y (1)^k \equiv a^y$$

ex: $p = 101$

$502^{502} \bmod 101$

$\equiv -3^{502} \bmod 101$

$-3^2 \cdot -3^{500} \bmod 101$

1

$\equiv 9 \bmod 101$

If $2^{n-1} \not\equiv 1 \bmod n$ then n is composite

$n = 1027$ (don't know if prime/composite)

$2^{1026} \bmod 1027$

$2^{1026} = 2^{1024} \cdot 2^2$

$(471)(4)$

$1884 \bmod 1027$

$\not\equiv 1$ so 1027 composite

2^1

2^2

$\vdots$

$2^{1024} \equiv 471 \bmod 1027$

---

if $\gcd(a, n) \neq 1$ then $a^{n-1} \not\equiv 1 \bmod n$

---

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

$a(a^{n-2}) \equiv 1 \bmod n$

a^{n-2} is the inverse of $a \bmod n$

$\gcd(a, n) = 1$

Euler's phi function

$n \in \mathbb{Z}$ $\phi(n) =$ # of integers a, $1 \leq a \leq n$ where $\gcd(a, n) = 1$

$\phi(10) = 4$

$\phi(6) = 2$

$\phi(7) = 6$

$\phi(p) = p - 1$ when p is prime

$\phi(81) = 81 - \frac{1}{3}81$

$= 81 - 27$

$= 54$

if p is prime and k is a positive integer, then $\phi(p^k) = p^k - p^{k-1}$

- $\phi(n)$ = # of integers with $1 \le a \le n$ and $\gcd(a,n) = 1$

- if p is prime then

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

- if $\gcd(m,n) = 1$ then $\phi(mn) = \phi(m) \cdot \phi(n)$

ex

$$\phi(100) = \phi(4) \cdot \phi(25)$$
$$2 \cdot 20 = 40$$

- if p, q different primes then

$$\phi(pq) = (p-1)(q-1)$$

Can do prime factorization of integer, then do $\phi(n)$

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

$$\phi(n) = \phi(p_1^{k_1}) \phi(p_2^{k_2}) \cdots \phi(p_n^{k_n})$$
$$= \phi(p^{k_1} - p^{k_1-1}) \phi(p_2^{k_2} - p_2^{k_2-1}) \cdots \phi(p_n^{k_n} - p_n^{k_n-1})$$

ex

$$\phi(360) = \phi(6 \cdot 6 \cdot 10)$$
$$= \phi(2 \cdot 3 \cdot 2 \cdot 3 \cdot 2 \cdot 5)$$
$$= \phi(2^3) \cdot \phi(3^2) \cdot \phi(5)$$
$$(8-4) \cdot (9-3) \cdot 4$$
$$= 4 \cdot 6 \cdot 4 = 96$$

Equivalent formula

$$\phi(n) = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

product over all distinct prime factors of n

so

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

$\frac{1}{2}$ $\frac{2}{3}$ $\frac{4}{5}$

$$= 96$$

Eulers theorem if $\gcd(a,n) = 1$ then

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

---

ex $n = 77$ $\phi(n) = \phi(7) \cdot \phi(11)$

$6 \cdot 10 = 60$

$2^{60} \equiv 1 \bmod 77$

$3^{60} \equiv 1$

$4^{60} \equiv 1$

ex simplify

$3^{484} \bmod 77$

$(3^{60})^8 \cdot 3^4 \bmod 77$

$\equiv 81 \bmod 77$

$\equiv 4 \bmod 77$

Basic Principle

Let $a, n, x, y \in \mathbb{Z}$ with $n \geq 1$ and $\gcd(a, n) = 1$

If $x \equiv y \bmod \phi(n)$ then

$$a^x \equiv a^y \bmod n$$

---

ex: last 2 digits of 7^{83}

So $7^{83} \bmod 100$

$\phi(100) = 40$

$83 \equiv 3 \bmod 40$

$7^{83} \equiv 7^3 \bmod 100$

$\equiv 343 \bmod 100$

$\equiv 43 \bmod 100$

---

ex: $241^{90} \bmod 115$

$241 \equiv 11 \bmod 115$

$241^{90} = 11^{90} \bmod 115$

$\phi(115) = \phi(5 \cdot 23)$

$4 \cdot 22 = 88$

$90 \equiv 2 \bmod 88$

$241^{90} \equiv 11^{90} = 11^2 \equiv 121 \bmod 115 \equiv 6 \bmod 115$

RSA Algorithm

In a symmetric private key cryptosystem ($K_e = K_d$) the keys are known to both Alice and Bob.

But how to agree on a key if miles apart?

Public key cryptography

Bob makes his own enc/dec keys

makes his encryption keys public

keeps his decryption key private to decrypt messages he receives

must not be feasible for eve to calculate the decryption key from the encryption key

9.1 RSA for real

How Bob sets up RSA

1) Bob chooses 2 large secret primes P, Q and computes $n = PQ$ and $\phi(n) = (P-1)(Q-1)$

2) Bob chooses an integer e with $\gcd(e, \phi(n)) = 1$

3) Bob computes d with $ed \equiv 1 \bmod \phi(n)$ via the extended euclidean algorithm

4) Bob makes n and e, Public information keeps $P, Q, d, \phi(n)$ private

---

RSA assume the plaintext is an integer m

RSA Encryption

1) Alice looks up Bobs n and e

2) Alice encrypts m by computing
$c \equiv m^e \bmod n$ (modular exponentiation)

3) sends c to Bob

RSA decryption

1) Bob gets c from Alice

2) Bob decrypts by
$m \equiv c^d \bmod n$

Why work? Eulers.

Recall $ed \equiv 1 \bmod \phi(n)$

So $c^d \equiv (m^e)^d \equiv m' \equiv m \bmod n$ (reduce mod $\phi(n)$)

- Everyone has access to n, e so everyone can send
- Only Bob can decrypte the ciphertexts to him

Why secure?
For eve to decrypt Bobs message she needs d.

She knows n, e why can't eve calculate d? she doesn't know $\phi(n)$ ie, it's hard to calculate factors of n (the two primes)

P, Q large so eve can't factor n ($n = PQ$) so she can't compute $\phi(n)$

Turns out factoring integers is hard (600 digits)

3/13

RSA $n = pq$

Security relies on Eve cannot factor n or compute $\phi(n)$

if $n = pq$
then $\phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1$

so $n - \phi(n) + 1 = p + q$

so if one knows n and $\phi(n)$ then one knows pq and $p+q$
This is enough to solve for $p+q$

if $n = pq$ is a product of two distinct primes then the roots of

$$X^2 - (n - \phi(n) + 1)X + n = 0$$

are $X = p, q$

pf: $x^2 - (n - \phi(n) + 1) + n = 0$
$x^2 - (p+q)X + pq = 0$
$(X-p)(X-q) = 0$

ex: $n = 119579$
and $\phi(n) = 118776$
then p, q are the roots of

$$X^2 - (n - \phi(n) + 1)X + n = 0$$

$$X^2 - 804X + 119579 = 0$$

$$X = \frac{804 \pm \sqrt{(804)^2 - 4(119579)}}{2} = \frac{804 \pm 410}{2} = 607, 197$$

9.2 - Attacks on RSA

Certain implementation mistakes lead to loss of security

$n = pq$ has m digits. if Eve knows the first $m/4$ digits / the last three Eve can effiently factor n

if d is too small say $d < \frac{1}{3} n^{1/4}$ then d can be calculated quickly

Timing attacks - measure time it takes to calculate, predict d

Short plaintext attack
if Eve knows the plaintext is small

Alice wants to send Bob a 56 bit DES key via RSA $m \approx 10^{17}$, but n has hundreds of digits, c would likely be the same order of magnitude as n

Say eve knows c, n, e and $m \approx 10^{17}$

Brute force encrypting takes too long

Eve makes 2 lists
1) $cx^{-e} \pmod n$ $\forall x, 1 \leq x \leq 10^9$
2) $y^e \bmod n$ $\forall y, 1 \leq y \leq 10^9$

2×10^9 encryptions
$(x^{-1})^e$ is just inverse

eve looks for m such that

$cx^{-e} \equiv y^e \bmod n$

$\Rightarrow c \equiv x^e y^e \bmod n$

$c \equiv (xy)^e$

$m \equiv c^d \equiv (xy)^{ed} \equiv xy \bmod n$

$m \equiv xy \bmod n$

must be true m is a product of 2 integers $\leq 10^9$

easy prevent: Alice can adjoin random digits at the start of m to make it longer

when Bob decrypts, discard junk at the beginning

9.3 - Primality: Testing (checking if # is prime)

9.4 - factoring

$x^2 \equiv y^2 \bmod n$

Basic Principle:
Let n be an integer and suppose there are integers x, y st $x^2 \equiv y^2 \bmod n$ but $x \not\equiv \pm y \bmod n$ then n is composite
Moreover $\gcd(x-y, n)$ is a nontrivial factor of n (not 1 or n)

How it works

$x^2 \equiv y^2 \bmod n$

$x^2 - y^2 \equiv 0 \bmod n$

$n \mid (x-y)(x+y)$

and $x \not\equiv \pm y \bmod n$ implies $n \nmid (x+y)$ and $n \nmid (x-y)$

factors are split between $x-y$ and $x+y$

3/15

$x^2 \equiv y^2 \bmod n$ factoring

If $x^2 \equiv y^2 \bmod n$ and $x \not\equiv \pm y \bmod n$ then $\gcd(x-y, n)$ is nontrivial factor of n

Ex: factor $n = 55$

$8^2 \equiv 64 \equiv 9 \equiv 3^2 \bmod 55$

so $8^2 \equiv 3^2 \bmod 55$

$\gcd(8-3, 55) = 5$

Ex. Sps we have

$411^2 \equiv 3091^2 \bmod 6901$

$\gcd(3091-411, 6901) = \gcd(2680, 6901) = 67$

How to find $x^2 \equiv y^2 \bmod n$ - no reliable way

consider: $x^2 \equiv 1 \bmod n$ $x \not\equiv \pm 1 \bmod n$

n is composite so $\gcd(x-1, n)$ is a nontrivial factor

ex: $10^2 \equiv 1 \mod 33$

$\gcd(10-1, 33) = 3$

Ex: one can show $4^6 \equiv 1 \mod 91$

$(4^3)^2 \equiv 1 \mod 91$

$\gcd(63, 91) = 7$

ex: $16^{44} \equiv 1 \mod 391$

$(16^{22})^2 \equiv 1 \mod 391$

$16^{22} \equiv 1 \mod 391$

$(16^{11})^2 \equiv 1$

$16^{11} \equiv 254 \mod 391$

$(254)^2 \equiv 1 \mod 391$

$\gcd(253, 391) = 23$

ex: $26^{88} \equiv 1 \mod (1513)$

$88 = 2^3 \cdot 11$

$26^{11} \equiv 967 \mod 1513$

$26^{22} \equiv 967^2 \equiv 55 \mod 1513$

$26^{44} \equiv 55^2 \equiv 1512 \mod 1513 \quad (-1)$

$26^{88} \equiv (-1)^2 \equiv 1 \mod 1513$

failed to find x st $x^2 \equiv 1 \mod 1513$ and $x \not\equiv \pm 1 \mod 1513$

$r = n-1$

$a^r \equiv 1 \bmod n$ factoring method: sps we have the congruence of the form $a^r \equiv 1 \bmod n$ and $r \in$ even

$r = 2^k m$ where $m \in$ odd

Let $b_0 \equiv a^m \bmod n$ successively define

$$b_{v+1} \equiv b_v^2 \qquad 0 \le v \le k-1$$

- if $b_0 \equiv \pm 1$ then we failed to factor n
- if $b_v = -1$ for some v then we failed to factor n
- if $b_{v+1} \equiv 1$ for some v and $b_v \neq \pm 1$ then $\gcd(b_v - 1, n)$ is a nontrivial factor of n

Primality testing: Fermat Primality test: $n > 1$ random integer with $1 < a < n-1$

- If $a^{n-1} \not\equiv 1 \bmod n$ then n is composite
- If $a^{n-1} \equiv 1 \bmod n$ then n is probably prime

MR Primality Test: do Fermat test, if $a^{n-1} \equiv 1 \bmod n$ try $a^r \equiv 1 \bmod n$ factorization, if it gives a factor then n is composite, if it doesn't then n is probably prime

$n = 341$

$2^{340} \equiv 1 \mod 341$ $\quad 340 = 4 \cdot 85$

$2^{85} \equiv 32 \mod 341$

$32^2 \equiv 1 \mod 341$

So $\gcd(31, 341)$ is a nontrivial fact- so 341 is composite.

Primality testing

1) Fermat primality test

if $a^{n-1} \not\equiv 1 \bmod n$ then n is composite

if $a^{n-1} \equiv 1$ then n is probably prime

2) $a^r \equiv 1 \bmod n$ Factoring

Combining 1 + 2 gives Miller Rabin primality test:

- if $a^{n-1} \equiv 1 \bmod n$ try $a^r \equiv 1$ Factoring.
if it yields a factor then n is composite
otherwise it's probably prime

In MR first write $n-1 = 2^k m$ m odd
For a base a define

$b_0 \equiv a^m \bmod n$

$b_1 \equiv b_0^2 \equiv a^{2m} \bmod n$

$b_2 \equiv b_1^2 \equiv a^{4m} \bmod n$

$\vdots$

$b_k \equiv b_{k-1}^2 \equiv a^{2^k m}$

b_k

If $b_0 \equiv \pm 1 \bmod n$, then n is probably prime

- If $b_0 \equiv 1 \bmod n$ and $b_1 \equiv \pm 1$ then n is composite and $\gcd(b_1 - 1, n)$ is a factor
- If $b_2 \equiv \pm 1 \bmod n$ and $b_1 \equiv 1$ then n is composite $\gcd(b_1 - 1, n)$ is a factor

do this until b_{k-1}
if $b_{k-1} \not\equiv -1$ then composite,
otherwise probably prime

Ex $n = 561$

$2^{560} \equiv 1 \bmod n$

$560 = 2^4 \cdot 35$

$b_0 = 2^{35} \equiv 263 \bmod 561$

$b_1 = 2^{70} \equiv 166 \bmod 561$

$b_2 = 2^{140} \equiv 67 \bmod 561 \leftarrow \neq 1$

$b_3 = 2^{280} \equiv 1 \bmod 561 \leftarrow 1$

nontrivial $\leftarrow 67^2 \equiv 1 \bmod 561$

$\gcd(66, 561) = 33$

Def n

if n composite and $a^{n-1} \equiv 1 \bmod n$

then n is a pseudo prime for base a

If n composite and MR says n is probably prime then n is a strong pseudo prime

strong pseudo prime implies pseudoprime

ex: 561 is a pseudo prime for

base 2 $2^{560} \equiv 1$ not strong

ex: $2^{340} \equiv 1 \bmod 341$ ← pseudo

$3^{340} \equiv 56$ ← not pseudo

3/27

Find 300 digit prime?

- prime # theorem $\frac{1}{\ln 10^{300}} \approx \frac{1}{690}$
- for odd $\approx \frac{1}{345}$

Pick 300 digit odd #, test N+2, N+4...
for primality, doing MR keep going until you find a very likely prime.
< 400 MR tests

Not all primes of a similar size are equally good for cryptography

Prime factorization of p-1 can play a role

PF: $p-1 : 2^1 \cdot 3^1 \cdots 19^1$
$q-1 : 2^1 \cdot 3^1 \cdot$ big prime #

If $p \mid n$ and $p-1$ has only small divisors then there's an algorithm to factor n

Idea: if $p-1$ only has small factors then $B!$ will be a multiple of $p-1$ when B is of moderate size

Say $B! = (p-1)k$ for some k

let $b \equiv 2^{B!} \pmod{n}$

Mod p we know

$$b \equiv 2^{B!} \bmod p$$

$$b \equiv 2^{(p-1)k} \bmod p$$

(Fermats) $b \equiv 1 \bmod p$ this implies $p \mid b-1$, find p by computing $\gcd(b-1, n)$

Pollards $p-1$ factoring algorithm

choose $a > 1$

choose bound B

compute $b = a^{B!} \bmod n$

$b_1 = a \bmod n$

$b_2 = b_1^2 \bmod n$

$b_3 = b_2^3 \bmod n \quad [a^6]$

$b_4 = b_3^4 \bmod n \quad [a^{24}]$

$\vdots$

$b_k = b_{k-1}^k \bmod n \quad [a^{k!}]$

Let $d = \gcd(b-1, n)$ if $1 \le d \le n$ then we have found a nontrivial fac. of n

---

$n = 600000001$

$? = \ldots$

$n = pq$

$p-1 = 6 \times 10^8 = 2^9 \cdot 3 \cdot 5^8$

$B = 35 \quad a = 2$

$\gcd(2^{35}-1, n) = 60000000$

How can we choose prime p s.t. $p-1$ has at least one large factor

Idea: choose any prime q with ≥ 150 digits and choose a random 150 digit even integer k

$$kq+1$$

Test for primality, if not prime, increment K and try again until you find

a prime $p = kq+1$ so q is (large) is a factor of $p-1$

Primitive roots

$3^1 \equiv 3 \bmod 7$
$3^2 \quad 2 \bmod 7$
$3^3 \quad 6$
$3^4 \quad 4$
$3^5 \quad 5$
$3^6 \quad 1$

Period 6

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

2
4
1
⋮

We say the order of 3 mod 7 is 6 $\quad ord_7(3) = 6$

order of 2 mod 7 is 3 $\quad ord_7(2) = 3$

Suppose $p \in$ Prime and $a \not\equiv 0 \bmod p$
consider

Powers of a : $a^k \bmod p$

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

1) always find 1 in the sequence

2) sequence repeats

Def
smallest positive integer m s.t $a^m \equiv 1 \bmod p$ is called the order of $a \bmod p$ $\operatorname{ord}_p(a) = m$

Def integer a is called a primitive root for a prime p if $\operatorname{ord}_p(a) = p-1$

important: for a primitive root we see all nonzero #s mod p in terms of powers

$a^1, a^2, \ldots$

3 is a primitive root of 7

$p = 13$ $a = 3$

$3^1 \equiv 3 \bmod 13$
$3^2 \equiv 9 \bmod 13$
$3 \equiv 1 \bmod 13$

3
9
⋮
1

$a = 2$

$2^1 : 2$
$2^2 : 4$
$\vdots\ 8$
$\vdots\ 3$
$\vdots\ 6$
$\vdots\ 12$
$\vdots\ 11$
9
5
10
7
$2^{12}\ 1$

$\operatorname{ord}_{13}(2) = 12$ so 2 is a PR of 13

Non obvious facts

$p \in$ Prime

- For any $a \not\equiv 0 \bmod p$ $\quad ord_p(a) \mid (p-1)$
- Primitive roots for p exist in fact exactly $\phi(p-1)$ primitive roots of p

---

ex $p = 13$ $\quad \phi(12) = 4$ so 4 PR for 13

2, 6, 7, 11

Basic Property

PR a

$a^x \equiv a^y \pmod p$

$\iff x \equiv y \bmod (p-1)$

CH10 discrete logs

Fix prime p, α, β that are nonzero mod p finding x s.t.

$\beta \equiv \alpha^x \bmod p$ is the discrete log of β

$x = L_\alpha(\beta)$ discrete log of β with respect to α $\pmod p$

Ex: $\alpha = 2 \quad p = 13 \quad L_2(3) = ?$

$2^x \equiv 3 \pmod{13}$

$16 \equiv 3$

$2^4 \equiv 3 \quad x = 4 \quad L_2(3) = 4$

$2^4, 2^{16},$

discrete log is unique mod n, take the smallest

4/3

Discrete log:

- Prime p, α, β find x s.t.

$$a^x \equiv \beta \bmod p$$

$$x = L_\alpha(\beta)$$

ex: $p = 13$ $L_3(2) = ?$

$$3^x \equiv 2 \bmod 13$$

$3^1 \to 3$
$3^2 \to 9$
$3^3 \to 1$ } loop

3 is not a primitive root

Discrete log problem: primitive root α for prime p:

given a PR α for p and an int $\beta \leq p-1$ find unique $0 \leq x \leq p-2$ s.t. $\alpha^x \equiv \beta \bmod p$

Like factoring, discrete log is hard for large primes

Def:
A function $f(x)$ is a one way function if $f(x)$ is easy to compute but given y, it's computationally infeasible to find x s.t. $f(x) = y$

- $f(x) = \alpha^x \bmod p$ is a OWF
- $f(P,Q) = PQ$ is a OWF

10.4 Diffie Hellman key exchange

Alice Bob establish a private key over public channels

Send using RSA is a solution

output a key K s.t. Alice + Bob can compute but no one else can compute it

Diffie-Hellman key exchange

1) large prime p and PR α for p are chosen (public)

2) Alice chooses secret random int $1 \leq x \leq p-2$
Bob " " $1 \leq y \leq p-2$

3) Alice computes $A \equiv \alpha^x \pmod{p}$ and sends to Bob

4) Bob computes $B \equiv \alpha^y \pmod{p}$ and sends to Alice

5) Alice computes $k = B^x \bmod p$
Bob computes $k = A^y \bmod p$

they both get k because

$$B^x \equiv (\alpha^y)^x \equiv \alpha^{xy} \bmod p$$

$$A^y \equiv (\alpha^x)^y \equiv \alpha^{xy} \bmod p$$

p should be large!!

ex: $p = 101 \quad \alpha = 7$

- Alice chooses 28

$$A \equiv 7^{28} \equiv 97 \pmod{101}$$

- Bob chooses 71

$$B \equiv 7^{71} \equiv 18 \pmod{101}$$

In private:

- Alice computes

$$18^{28} \equiv 58 \mod 101$$

- Bob computes

$$97^{71} \equiv 58 \mod 101$$

Then both x or y she can compute it she knows

$$A \equiv \alpha^x \mod p$$

$97 \equiv 7^x \mod 101$ and $18 \equiv 7^y \mod 101$ (discrete log problem)

Generally p is prime, α is a PR for p

$A \equiv \alpha^x \bmod p$ $\quad$ $B \equiv \alpha^y \bmod p$

$K = \alpha^{xy} \bmod p$

4/5

10.5

Elgamal public key crypto system

Security relies on difficulty of solving discrete logs

In order to receive encrypted messages Bob sets up:

EL GAMAL SETUP

1) Bob chooses a large prime p a primitive root α for p (public)

2) Bob chooses secret integer b and computes

$$\beta \equiv \alpha^b \bmod p$$

3) Bob posts (p, α, β)

EL GAMAL Encryption:

Alice wants to send bob message m $0 \leq m < p$

1) get Bobs public (p, α, β)

2) she chooses secret random integer k and computes

$$r \equiv \alpha^k \bmod p \text{ and } t \equiv \beta^k m \bmod p$$

3) she sends Bob (r, t)

EL gamal decryption

Bob doesn't know k

but Bob can compute β^k as

$$r^b \equiv (\alpha^k)^b \equiv (\alpha^b)^k \equiv \beta^k \bmod p$$

then

$$t \equiv \beta^k m \equiv r^b \bmod p \quad \text{implies}$$

$$m \equiv (r^b)^{-1} t \equiv r^{-b} t \bmod p$$

- to decrypt (r, t) bob computes

$$m \equiv r^{-b} t \bmod p$$

- If eve gets b, then eve can decrypt as Bob does

eve knows that $\beta \equiv \alpha^b \bmod p$ solving b-b is direct by problem

---

If eve has k then Eve can compute

$$\beta^k \bmod p$$

Since $t \equiv \beta^m \bmod p$ then eve computes:

$m \equiv (\beta^k)^{-1} t \bmod p$

To find k, Eve solves

$$r \equiv a^k \bmod p \text{ for } k$$

10.2 Computing discrete logs

given α & p s.t. $\alpha^x \equiv \beta \pmod p$ how can we solve for x $p \in$ Prime, alpha is a p-imitive ...t.

Name brute force attack compute $\alpha^k \bmod p$ for $k = 0, 1, 2 \ldots$ until we get β

will require p mults/reductions, not feasible when p has hundreds of digits

10.2.2
Baby step - grant step
improved over brute force

First choose an integer $N > \sqrt{p-1}$

make 2 lists

1) $\alpha^j \bmod p$ for all $0 \leq j < N$
2) $\beta \alpha^{-Nk}$ for all $0 \leq k < N$

Look for a match between the two lists

find

$$\alpha^j \equiv \beta \alpha^{-Nk} \bmod p$$

$$\alpha^{j+Nk} \equiv \beta \bmod p$$

$$L_\alpha(\beta) = j + Nk$$

definitely be a match

do around $\sqrt{p-1}$ computations

ex:

$\alpha = 7 \quad p = 23 \quad$ Solve $7^x \equiv 2 \bmod 23$

$\sqrt{22} \approx$ Take $N = 5$

$7^0 \equiv 1$

$7^1 \equiv 7$

$7^2 \equiv 3$

$7^3 \equiv 21$

$7^4 \equiv (9)$

$2 \cdot 7^{-5k}$

$2(7^{-5})^0 = 1$

$2(7^{-5})^1 = 15$

$2 \cdot (7^{-5})^2 = (9)$

$7^4 \equiv 9 \equiv 2 \cdot (7^{-5})^2$

$7^{14} \equiv 2 \bmod 23$

$L_7(2) = 14$

we have a DLP

$$\alpha^x \equiv \beta \pmod{p}$$

x is in PR of p

There is a method to determine the value of $x \bmod 2$

Lemma: if α is a PR of prime p then

$$\alpha^{\frac{p-1}{2}} \equiv -1 \bmod p$$

$$b = \alpha^{\frac{p-1}{2}}$$

$$b^2 = \alpha^{p-1} \equiv 1 \bmod p \quad \text{if } p \text{ is prime}$$

But $b = \alpha^{\frac{p-1}{2}} \neq 1$ because α is a PR and its order is $p-1$ and $\frac{p-1}{2} < p-1$

$\therefore b = \alpha^{\frac{p-1}{2}} \equiv -1 \bmod p$

Back to $\beta \equiv \alpha^x \bmod p$

$$\beta^{\frac{p-1}{2}} \equiv (\alpha^{\frac{p-1}{2}})^x \bmod p$$

$$\beta^{\frac{p-1}{2}} \equiv -1^x \bmod p$$

Method for a DLP $\beta \equiv \alpha^x \bmod p$, compute $\beta^{\frac{p-1}{2}} \bmod p$ if

- $\beta^{\frac{p-1}{2}} \bmod p \equiv 1$, x is even
- $\beta^{\frac{p-1}{2}} \bmod p \equiv -1$, x is odd

$6 \equiv 10^x \bmod 17$

$6^{\frac{p-1}{2}} \equiv 6^8 \bmod 17$

$6^2 \equiv 2 \bmod 17$

$6^8 \equiv 16 \equiv -1 \bmod p$ so x is odd

$x = 5$

2.1 Pohlig-Hellman algorithm

generalization

for $\beta \equiv \alpha^x \bmod p$ if q is a small prime divisor of $p-1$ then we can determine the value of $x \bmod q$ as follows

write $x = x_0 + qt \quad 0 \le x_0 < q \quad t \in \mathbb{Z}$

$\beta = \alpha^{x_0 + qt} = \alpha^{x_0} \alpha^{qt} \bmod p$

Raise both sides to $p-1/q$ power $(\in \mathbb{Z})$

$\beta^{p-1/q} \alpha^{x_0 \frac{(p-1)}{q}(p-1)t} \equiv \alpha^{x_0 (\frac{p-1}{q})}$

$\beta^{\frac{p-1}{q}} \equiv (\alpha^{\frac{p-1}{q}})^{x_0} \bmod p \quad 0 \le x_0 < q$

$\delta \equiv \gamma^{x_0} \bmod p$

assuming q is small, BF try all possible x_0's until we find the solution

ex: $p = 131 \quad \alpha = 2$ (PR)

$$2^x \equiv 3 \mod 131$$

$p - 1 = 130 = 2 \cdot 5 \cdot 13$

And $x \mod 2, 5, 13$

mod 2) $3^{\frac{p-1}{2}} = 3^{65} \equiv 3^{64} \cdot 3 \equiv 1 \mod 131$

x is even $\quad x \equiv 0 \mod 2$

mod 5)

$x \equiv x_0 + 5t \quad 0 \le x_0 \le 5$

$26 = \frac{p-1}{5} \quad 2^{x_0 + 5t} \equiv 3 \mod 131$

$(2^{x_0 + 5t})^{26} \equiv 3^{26}$

$2^{26x_0} \cdot 2^{130t}$

1 (Fermat)

$(2^{26})^{x_0} \equiv 3^{26} \mod 131$

$53^{x_0} \equiv 58$

$x_0 = 0, 1, 2, 3, 4$

$x_0 = 2$

$53^2 \equiv 58 \mod 131$

$x \equiv 2 \mod 5$

mod 13 $x = x_0 + 13t$

$$2^{x_0+13t} \equiv 3 \bmod 131$$

$$\frac{p-1}{13} = 10$$

$$2^{10x_0} \equiv 3^{10} \bmod 131$$

$$107^{x_0} \equiv 99 \bmod 131$$

$x_0 = 0, \ldots 12$

$x_0 = 7$

$x \equiv 7 \bmod 131$

- $x \equiv 0 \bmod 2$
- $x \equiv 2 \bmod 5$
- $x \equiv 5 \bmod 13$

$\Rightarrow x \equiv 2 \bmod 10$, $x \equiv 5 \bmod 13$ $\Rightarrow x \equiv 72 \bmod 130$

$$2^{72} \equiv 3 \bmod 131$$

if q is a ~~prime~~ divisor of $p-1$
find $(x \bmod q)$ requires q BTorces

works for any divisor d of $p-1$

if p is a prime s.t. $p-1$ only has small prime factors then discrete logs can be computed for p using these ideas

Pohlig Hellman Algorithm $\alpha^x \equiv \beta \bmod p$

assume that $p-1 = q_1^{r_1} q_2^{r_2} \cdots q_m^{r_m}$ prime factorization
if we can compute the value of $x \bmod q_i^{r_i}$ for i
then use CRT to get

$$x \pmod{\underbrace{q_1^{r_1} \cdots q_m^{r_m}}_{p-1}}$$

based on case $r_i = 1$

consider case where $q^2 \mid p-1$
we want $x \pmod{q^2}$

$$x = x_0 + x_1 q + t q^2$$

$0 \le x_0, x_1 < q$ and t is an integer so
$x \equiv x_0 \bmod q$ and $x \equiv x_0 + x_1 q \bmod q^2$

$$\beta \equiv \alpha^{x_1} \pmod{p}$$

$$\beta \equiv \alpha^{x_0 + q x_1 + t q^2} \pmod{p}$$

assume we know x_0

$$\beta \alpha^{-x_0} \equiv \alpha^{x_1 q + t q^2} \bmod p$$

raise both sides to $\frac{p-1}{q^2}$

$$\beta^{\frac{p-1}{q^2}} \alpha^{-x_0 \left(\frac{p-1}{q^2}\right)} \equiv \alpha^{x_1 \left(\frac{p-1}{q}\right) + t(p-1)}$$

compute

BF check $x_1 = 0, 1, 2, 3, \ldots q-1$ until congruent

one can do this to find $x \bmod q^r$
assuming $q^r \mid p-1$ done when you find

$$x \bmod q$$
$$x \bmod q^2$$
$$\vdots$$
$$x \bmod q^r$$

ex $p = 600000001$ a prime that is vulnerable

$p-1 = 6 \times 10^8 = 2^9 \cdot 3 \cdot 5^8$

To solve $\alpha^x \equiv \beta \bmod p$

Find $x \bmod 2^9 \quad \leq 2 \cdot 9$

$x \bmod 3 \quad \leq 3$

$x \bmod 5^8 \quad \leq 8 \cdot 5$

10.3 Bit commitment

Alice wants to send Bob a bit

- Bob can't determine it's value until alice reveals it to him
- once alice sends the bit, she can't change it

A solution:

1) Alice Bob agree on a large prime p with $p \equiv 3 \bmod 4$ and primitive root α for p

2) Alice chooses a random integer $x < p-1$ with the property that the second to last bit x_1 of x is b $\quad x = x_n \ldots x_1 x_0$ (with $x_1 = b$)

3) Alice computes $\beta \equiv \alpha^x \bmod p$ and sends to Bob

4) when the time comes alice reveals x to Bob so Bob confirms its $\alpha^x \bmod p = \beta$

Bob can't determine x without Alice help because he has to solve

$$\alpha^x \equiv \beta \bmod p$$

- Since α is a PR ~~and~~ the solution x to DLP is unique $(\bmod p-1)$ So Alice can't change her answer

1) 2nd to last bit
   $x \bmod 2$ easy need $x \bmod 4$
2) why $p \equiv 3 \bmod 4$
   if $p \equiv 1 \bmod 4$ then $4 \mid p-1$ so
   $x \pmod 4$

if $p \equiv 3 \bmod 4$, we can't do last

Hash functions

- Applications in msg authenticity / integrity pw security, digital signature

- hash function, takes message m arbitrary length produces a smaller message

no unhashing messages

~~no~~ messages > # of outputs (not 1 to 1)
multiple messages → same output

∃ pairs of messages m, m' st $h(m) = h(m')$

decent hash function should satisfy:
1) Fast - given m, find $h(m)$ quickly
2) Pre image resistance, can't invert a hash ie given $h(m)$ can't find m
3) Strong Collision resistance, computationally infeasible to find m, m' st $h(m) = h(m')$

3') Weak collision resistant: given m, computationally infeasible to find m' s.t. $m \neq m'$ and get $h(m) = h(m')$

if h is not preimage resistant then it is probably easy to produce collisions

Given any m let $y = H(m)$ Since h is not Pre image resistant we can find an m' s.t $h(m') = y$, giving a collision $h(m) = h(m') = y$

Bad hash function
large integer n, $h(m) = m \bmod n$

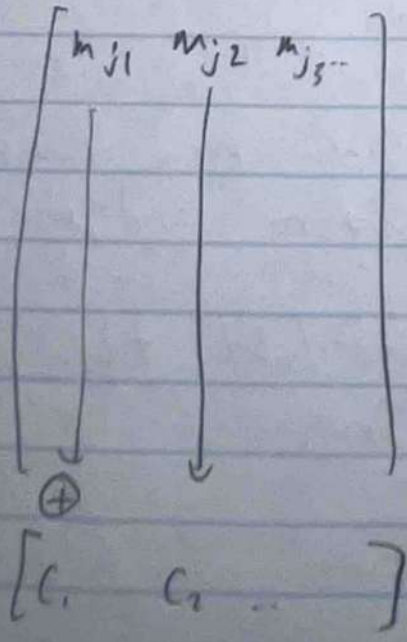
Satisfies 1

11.2 Simple Hash functions
integer n = # of bits in digest

message M, divide it into blocks each
$M = M_1 \| M_2 \| \dots \| M_l$

$h(m) = M_1 \oplus M_2 \oplus \dots \oplus M_l$

$M_j = [m_{j,1}, \dots, m_{j,n}]$



one way to modify it is bit rotation n-bit block
B let Rot(B) be a right shift by 1

$\hat{h}(m) = M_1 \oplus Rot(M_2) \oplus Rot^2(M_3) \oplus \ldots$

4/15

11.3 Merkle Damgard Construction MDC

This construction builds a compression function $f(H, M)$ f takes 2 bit strings H and M as inputs and outputs a bitstring

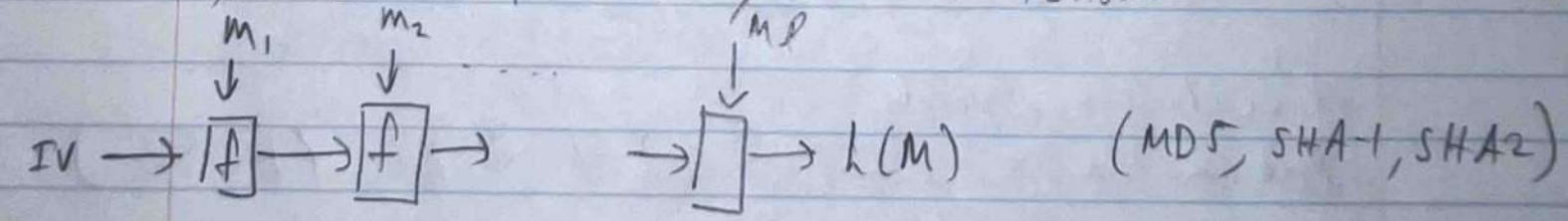
$H' = f(H, M)$ of same length as H
M can be a different length
H and H' can be 256 when $M = 512$

Given such a function f we'll build a hash function as follows.

1) given a message M, to be hashed break it into blocks of 512 bits each $M = M_1 \| M_2 \cdots \| M_l$

2) choose a 256 bit initial value IV,

3) iteratively apply f as follows



(MD5, SHA-1, SHA2)

MDC is subject to a length extension attacks:
SPs eve knows $h(M)$ but not M There eve can compute $h(M \| M')$ for any block M' of eve's choosing

because $h(M \| M') = f(h(M), M')$

12 - Hash functions and Applications

12.1 - Birthday Attack

If there are 23 people in a room, there's a 50% that 2 people have the same birthday

if 40 People : 89%.
if 77 People : 99.98%

For 23 people
- 1st person has bday
- 2nd has diff bday with prob $\frac{364}{365} = 1 - \frac{1}{365}$
- 3rd person has $\frac{363}{365}$ $(1 - \frac{2}{365})$
- 23rd person has diff bday $(1 - \frac{22}{365})$

$$\text{no\_match} = (1 - \tfrac{1}{365})(1 - \tfrac{2}{365}) \cdots (1 - \tfrac{22}{365})$$

$$P_{\text{match}} = 1 - \text{no\_match} = .507$$

if we have r people

$$\text{Prob(match)} = 1 - (1 - \tfrac{1}{365})(1 - \tfrac{2}{365}) \cdots (1 - \tfrac{r-1}{365})$$

more generally N objects, r people each chooses an object with replacement

$$P(\text{2 people chose the same thing}) = 1 - (1 - \tfrac{1}{N}) \cdots (1 - \tfrac{r-1}{N})$$

N is large r is close to N Probability can be obtained $\approx 1 - e^{-\frac{r^2}{2N}}$

$1 - e^{\frac{(-23)^2}{2 \cdot 365}} = .5155$

Q: how large must r be to get prob $= \frac{1}{2}$

$$\frac{1}{2} = 1 - e^{\frac{-r^2}{N}}$$

$$\ln e^{\frac{-r^2}{N}} = \ln \frac{1}{2}$$

$$-\frac{r^2}{N} = \ln\left(\frac{1}{2}\right)$$

$$r^2 = 2\ln(2)\, N$$

$$r = \sqrt{2\ln(2)} \cdot \sqrt{N}$$

4/17

Say we want to find a collisions for an n-bit hash function h there are $N = 2^n$ possible hashes compute $h(x)$ for randomly chosen x's

How many to compute until prob(collision) $\geq \frac{1}{2}$

$1.177 \cdot 2^{n/2}$ different x's

prob(collide) $= 1 - e^{-50}$

≈ 1

Could be done if $n = 60$ but 256 is so big

Modification of Bday Problem

r people in room 1

r people in room 2

each person chooses one of N objects, person room 1 chooses the same object as person in room 2

$1 - e^{-\frac{r^2}{N}}$

To get $\frac{1}{2}$ $\frac{1}{2} = 1 - e^{-\frac{r^2}{N}}$

$$r = \sqrt{\ln 2}\sqrt{N} = .833\sqrt{N}$$

12.1.1

Birthday attack on discrete logs

α is a PR for a prime p

we want x st $\alpha^x \equiv \beta \bmod p$

2 lists of length r where $r \approx \sqrt{p}$

1) Compute $\alpha^k \bmod p$ for r randomly chosen values of k

2) Compute $\beta\alpha^{-l} \bmod p$ for r randomly chosen values of l

Look for match in two lists

$$\alpha^k \equiv \beta\alpha^{-l} \bmod p.$$

$$\alpha^{l+k} \equiv \beta \bmod p$$

$$x = k + l$$

12.2 - Multi collisions

issue with MDC is: if it is feasible to find collisions, then you can find multicollisions. several messages with same hash $x, \ldots, x$

Given a certain value H_0, we can always find 2 blocks M and M' such that $f(H_0, M) = f(H_0, M')$
we can build multi-collisions as follows

Starting with $H_0 = IV$ And blocks M M' as above s.t. $f(IV, M_1) = f(IV, M_1')$

$f(IV, M_1) = h(M_1)$ $\quad$ $f(IV, M_1') = h(M_1')$

$H_1 = h(M_1) = h(M_1')$

Next find M_2 and M_2' s.t
$f(H_1, M_2) = f(H_1, M_2')$

It follows the following 4 messages are the same

$M_1 \| M_2$
$M_1' \| M_2$
$M_1 \| M_2'$ $\quad$ where $h(M_2) = H_2$
$M_1' \| M_2'$

Next find M_3, M_3' with
$f(H_2, M_3) = f(H_2, M_3')$
so 8 messages

$M_1 \| M_2 \| M_3$

$\vdots$

$M_1' \| M_2' \| M_3'$

After finding K collisions of the form
$f(H, M) = f(H, M')$
we have a multi collision with 2^K messages

12.5 MAC
when Alice sends Bob a message
two concerns are
1) is the message really from Alice
2) Has the message been changed during transmission

To address these, Alice sends some kind of appendix, she sends (m, MAC) to Bob

Bad attempt: Alice/Bob choose hash function h and she sends (m, h(m)), Bob independently computes h(m) and verifies
- detects accidental transmission error, won't detect malicious tampering eve changes m to m' and sends Bob h(m') and sends (m', h(m')) to Bob

no authentication

so to authenticate do Diffie Hellman to exchange keys for authentication

Assume k is a shared secret between Alice/Bob when Alice sends m to Bob also send $h(k \| m)$ and send $(m, h(k \| m))$ to Bob

if h is built from MDC then it is vulnerable to length extension attack

SPS one observes Alice send $(m, h(k \| m))$ to Bob, If m' is any additional block of one's choosing then one can compute

$h(k \| m \| m') = f(h(k \| m), m')$ so one can send

$(m \| m', h(k \| m \| m'))$ like it came from Alice

- HMAC

Form inner/outer padding strings

ipad = 0x36 ... 36

opad = 0x5c ... 5c

$k_1 = k \oplus$ ipad

$k_2 = k \oplus$ opad

$HMAC(m, k) = h(k_2 \| h(k_1 \| m))$ alice sends $(m, HMAC(m, k))$ to Bob

12.6 PW Protocols
Alice wants to log into server, sends credentials to Veronica (verifier)
makes username: I pw: P, tells veronica

4/22 Hashing + PWs

Alice sets a account by choosing username I and PW P and sends to veronica (verifier)

Bad: Storing them as plaintext (bad idea), eve gets the file, it's joever

Better attempt; Veronica chooses hash function h, when alice creates her account Veronica stores (I, h(P)) and discards P

- when alice logs in veronica checks to make sure h(P) is correct
- Bad because someone could login with h(P') and I not a problem if h collision resistant
- Eve obtains file, she knows hash of everyones pw but due to preimage resist shouldn't be able to construct actual pw
- Eve can do dictionary attack, hash every word in the dictionary, see if hashes match anything in the file

you can salt to protect against a dictionary attack. when alice creates an account, veronica assigns her a random bitstring s called salt Veronica stores $(I, s, h(s||p))$

- Veronica computes $h(s||p)$ everytime alice logs in
- If eve obtains the file she can only attack one user at a time doing dictionary attack with the user's salt but not all users at once

hash pws because its a one way function

---

13) Digital signatures

how can we be sure that someone was actually behind a message and how do we prevent them from denying a sent message

MAC provide authentication but not non-repudiation.

13.1 - RSA digital signatures
"RSA backwards"
Alice sets up RSA as usual
$n = pq$, $\gcd(e_A, \phi(n)) = 1$ $e_A d_A = 1 \bmod (\phi(n))$

to sign a message Alice uses d_A (only she knows)
Signature is $S \equiv m^{d_A}$ She can send the pair (m, S) to anyone and everyone can verify the message came from Alice by "encrypting her signature using the public info (n, e_A)

compute $S^{E_A}(m \bmod n)$ and check that matches m

$$m \equiv m^{d_A e_A} = m$$

$$(m')^{d_A} \equiv s' \quad (s')^{E_A} \equiv m'$$

4/24

El Gamal signature scheme

Alice sets up El gamal

- She chooses a large prime p and $\in PR$ α for p
- She chooses a secret integer a s.t. $1 \leq a \leq p-2$ and calculates $\beta = \alpha^a \bmod p$
- She post (p, α, β) publicly

---

to sign a message she does the following

1) chooses a random integer k, $1 \leq k \leq p-2$ and $\gcd(k, p-1) = 1$
2) computes $r \equiv \alpha^k \bmod p$. $0 < r < p$
3) computes $s \equiv k^{-1}(m - ar) \pmod{p-1}$

The signed message is the triple (w, r, s)

Bob can verify it

1) get Alices public (p, α, β)

2) compute $v_1 \equiv \beta^r r^s \pmod p$ and $v_2 \equiv \alpha^m \bmod p$

3) the signature is valid, iff $v_1 \equiv v_2 \bmod p$

$$v_1 \equiv \beta^r r^s \equiv (\alpha^a)^r \cdot (\alpha^k)^s = \alpha^{ar+ks} \pmod p$$

So $v_1 \equiv v_2 \bmod p \iff \alpha^{ar+ks} \equiv \alpha^m \bmod p$

$$\iff ar + ks \equiv m \bmod p-1$$

$$s \equiv k^{-1}(m - ar) \bmod (p-1)$$

---

if eve has a she can sign it like Alice

$(ks \equiv m - ar)$

Sps eve doesn't know a but wants to forge Alices signature on m she has $p \alpha \beta$ wants to produce (r, s) s.t. $\beta^r r^s \equiv \alpha^m \bmod p$

She can pick a r and try to solve for s

$r^s \equiv \beta^{-r} \alpha^m \bmod p$ is a DLP

Picking a known s is worse

Some Differences with RSA
- many valid signatures for a given m
- Message is not easily recovered from the signatures (r, s)

in RSA:
$S = m^d \bmod p$
$S^e \equiv m \bmod p$

important Alice chooses different k each time, if she reuses k, eve can solve for a
(r will be the same)

13.3 hash and signing
Previous schemes Sig(m) at least as long as msg m
so transmit twice as much and public key methods are slow

Rather than signing m, she can hash the message and then sign the hash instead

Alice sends $(m, Sig(h(m)))$ $h(x)$ is known

if Fred finds 2 messages s.t. $h(m) = h(m')$ then he can get alice to sign m and has consequently obtained $Sig(h(m')) = Sig(h(m))$

13.4
B-day attack on signature
SPS $h(m)$ only has 50 bit output
Fred drafts good doc m, bad doc m'
- expect $h(m) != h(m')$

In each doc Fred finds 30 places where he can change commas, spaces words etc

So he can make 2^{30} versions of each doc

Prob Some version of m has same has as Some version of m'

$$\approx 1 - e^{\frac{-r^2}{N}}$$
$$= 1 - e^{-\frac{2^{10}}{2^{50}}}$$
$$1 - e^{-2^{10}} = 1 - e^{-1024} \approx 1$$

4/24 ch 21 - Elliptic Curves

IR elliptic curve

defn: elliptic curve: graph of equation of the form
$E: y^2 = x^3 + ax^2 + bx + c$

where a, b, c are given real #'s

Curve in x, y - plane where (x, y) holds true

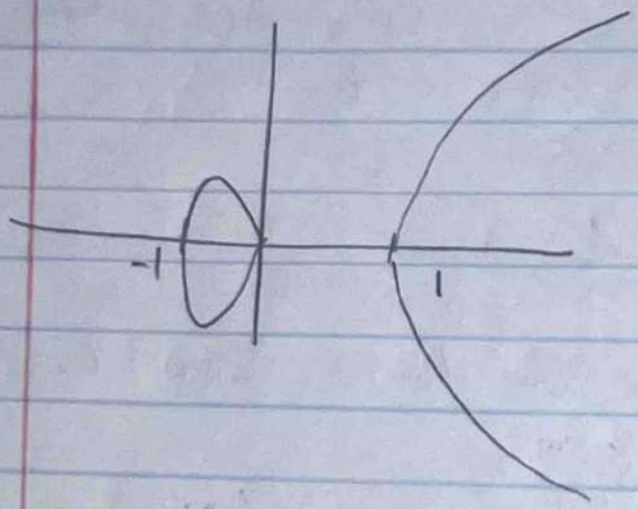
Elliptic curves come in 2 forms depending on the roots of the RHS

- 3 real roots ex:

$y^2 = x^3 - x$

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

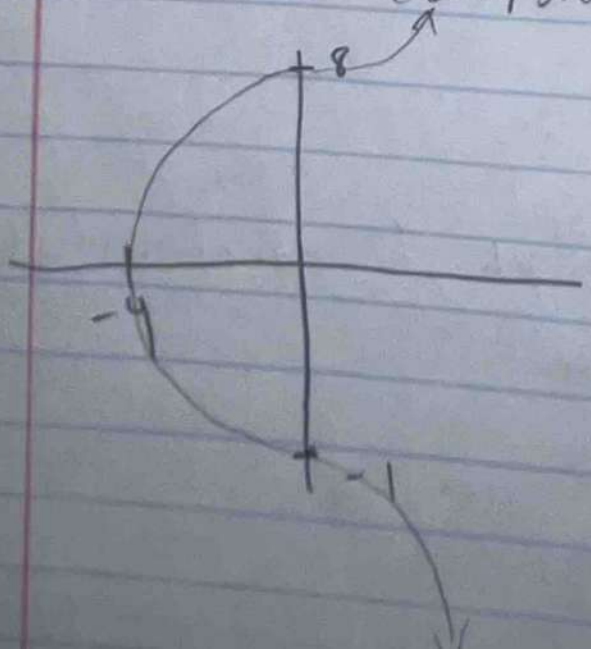
elliptic curve looks like



- 1 real root, 1 real 2 complex

$y^2 = x^3 + 64$

has one component



"point at infinity" ∞ in the y direction

can use change of variables on

$y^2 = x^3 + ax^2 + bx + c \rightarrow y^2 = \tilde{x}^3 + b\tilde{x} + c$

$\left[x = \tilde{x} - \frac{a}{3}\right]$

often sufficient to study curves of the form

$y^2 = x^3 + bx + c$

Addition on a elliptic curve

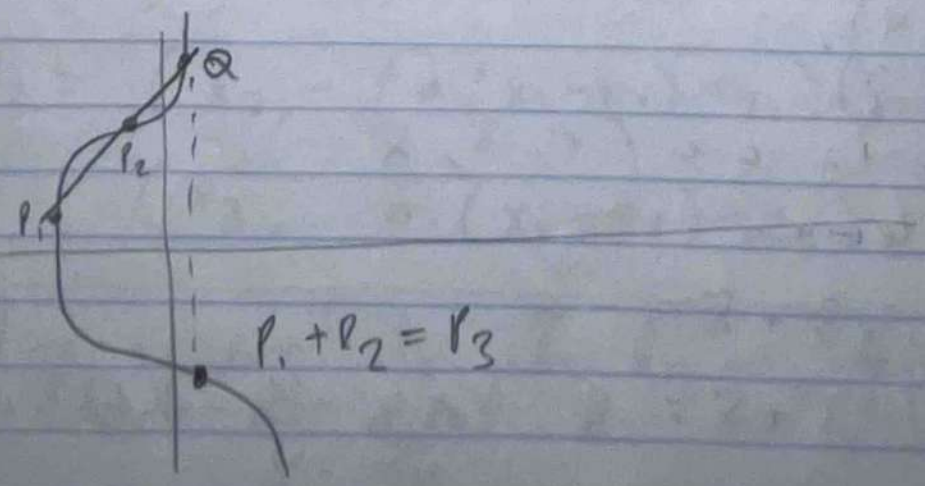
way to "add" 2 points on an elliptic curve E

P_1 P_2 on curve · draw a line through P_1, P_2 (L)

· L intersects E at a third point (Q)

· Reflect Q through the x-axis to get P_3

· $P_1 + P_2 = P_3$



$x^3 + ax^2 + bx + c$

$(x-r_1)(x-r_2)(x-r_3) = x^3 - (r_1+r_2+r_3)x^2 + (r_1r_2 + r_1r_3 + r_2r_3)x - r_1r_2r_3$

Lemma: if $P(x) = x^3 + ax^2 + bx + c$ and 3 real roots r_1, r_2, r_3 then

$r_1 + r_2 + r_3 = -a$

ex:

$P_1 = (1,2)$ $P_2 = (3,4)$ both live on

$y^2 = x^3 - 7x + 10$

slope $= \frac{4-2}{3-1} = 1$

eqn = $y - 2 = (1)(x-1)$

$y = x + 1$

to get Q: plug one into the other

$(x+1)^2 = x^3 - 7x + 10$

$x^2 + 2x + 1 = x^3 - 7x + 10$

$0 = x^3 - x^2 - 9x + 9$

$P_1 = (1,2)$

$P_2 = (3,4)$

$Q = (\tilde{x}, \tilde{y})$

So roots are $1, 3, \tilde{x}$

From lemma

$1 + 3 + \tilde{x} = -a$

$1 + 3 + \tilde{x} = 1$ $\tilde{x} = -3$ Q is $(-3, -2)$

$\tilde{y} = -2$

$P_1 + P_2 = (-3, 2)$

5/1

addition law for $y^2 = x^3 + bx + c$ for $P_1 = (x_1, y_1)$
$P_2 = (x_2, y_2)$

$$m = \frac{y_2 - y_1}{x_2 - x_1} \qquad y - y_1 = m(x - x_1)$$

$$y = m(x - x_1) + y_1$$

$$(m(x - x_1) + y_1)^2 = x^3 + bx + c$$

$$m^2 (x - x_1)^2 + 2m(x - x) y_1 + y_1^2 = x^3 + bx + c$$

$$0 = x^3 - m^2 x^2 + \underline{\text{Constant terms}}$$

3 roots one x_1, x_2, x_3
(P_1) (P_2) Unknown

$$-(-m^2) = m^2 = x_1 + x_2 + x_3$$

$$x_3 = m^2 - x_1 - x_2$$

3-d point of intersect

$$Q = (x_3, m(x_3 - x_1) + y_1)$$

$$P_1 + P_2 = (x_3, -(m(x_3 - x_1) + y_1))$$

$$(x_3, m(x_1 - x_3) - y_1)$$

adding a point to itself we have to find the target at point P

ex $P=(1,2)$ $y^2 = x^3 - 7x + 10$

implicit differentiation

$$2y\frac{dy}{dx} = 3x^2 - 7$$

$$\frac{dy}{dx} = \frac{3x^2-7}{2y} \quad @\ P(1,2) = \frac{3-7}{4} = -1$$

So $L: \quad y - 2 = -1(x-1)$

$$y = -x + 3$$

$$(x+3)^2 = x^3 - 7x + 10$$

$$0 = x^3 - x^2 - x + 1$$

Since C is tangent at $P(x=1, y=2)$ then $x=1$ is a double root

$$1 + 1 + x_3 = -(-1)$$

$$x_3 = -1$$

$$Q = (-1, 4)$$

$$P_1 + P_1 = (-1, -4)$$

---

in general $P_1 = (x_1, y_1)$ and $P_1 + P_1$

$$y^2 = x^3 + bx + c$$

$$m = \frac{dy}{dx} = \frac{3x^2+b}{2y} = \frac{3(x_1)^2+b}{2(y_1)}$$

Addition Law: $P_1=(x_1,y_1)$ $P_2=(x_2,y_2)$ be points on $E: y^2=x^3+bx+c$

then $P_1+P_2=P_3=(x_3,y_3)$ where

$x_3 = m^2 - x_1 - x_2$

$y_3 = m(x_1 - x_3) - y_1$

where

$$m = \begin{cases} \frac{y_2-y_1}{x_2-x_1} & \text{if } P_1 \neq P_2 \\ \frac{3x_1^2+b}{2y} & \text{if } P_1 = P_2 \end{cases}$$

if slope is ∞ $\left(\frac{1}{0}\right)$ then we define

$P_1+P_2=\infty$

$P+\infty=P$

Properties Points P, Q, R on curve E

- $P+Q=Q+P$
- $(P+Q)+R=P+(Q+R)$
- $P+\infty=P$
- $(x,y)+(x,-y)=\infty$ additive inverse

$-P=(x,-y)$

$P-Q=P+(-Q)$

5/3

P on elliptic curve positive int k

$kP = \underbrace{P + \cdots + P}_{k \text{ terms}}$

$kP \longmapsto a^k \bmod p$

to compute $100P$ we do repeated doubling

$2P = P + P$
$4P = 2P + 2P$
$8P = 4P + 4P$
$16P = 8P + 8P$
$32P = 16P + 16P$
$64P = 32P + 32P$

$100P = 64P + 32P + 4P$

21.2 elliptic curves mod p
p a prime $b, c \in \mathbb{Z}$
$E: y^2 \equiv x^3 + bx + c \bmod p$

Point on E is pair (x, y) of int mod p that satisfies the congruence

$0 \le x, y \le p$ a finite set of points (not a curve)
we include ∞
plug in each possible x see if possible sol y

Let $p > 2$ be a prime
$y^2 \equiv 0$ only has $y \equiv 0 \bmod p$

$a \not\equiv 0 \bmod p$ then $y^2 \equiv a \bmod p$ either has
no sols or 2 sols $b \equiv -b \bmod p$

$y^2 \equiv a \bmod p$ has sols for half of possible a's
with $1 \le a \le p-1$

---

ex: all points on curve
$E: y^2 \equiv x^3 + 3x + 4 \bmod 7$
sequence mod 7
$0^2 = 0$ $3^2 = 2$
$1^2 = 1$ $4^2 = 2$
$2^2 = 4$ $5^2 = 4$
$6^2 = 1$

$y^2 \equiv a \bmod 7$ has sol iff $a = 0, 1, 2, 4 \bmod 7$
BF on x
$x = 0 \to y^2 = 0 + 0 + 4 \iff y = 2, 5$ $(0,2)$ $(0,5)$
$x = 1 \to 1 + 3 + 4 \equiv 1$ $y = 1, 6$ $(1,1)$ $(1,6)$
$x = 2 \to 8 + 6 + 4 \equiv 4$ $y = 2, 5$ $(2,2)$ $(2,5)$
$x = 3 \to$ no sol
$x = 4 \to$ no sol
$x = 5 \to \equiv 4 \to$ $y = 2, 5$ $(5,2)$ $(5,5)$
$x = 6 \to \equiv 0 \to$ $(6,0)$

$E((0,2), (0,5), (1,1), (1,6), (2,2), (2,5), (5,2), (5,5), (6,0), \infty)$

(Hasse's theorem)
if E is an elliptic curve mod p and let N be the # of points on E then

$$|N - (p+1)| < 2\sqrt{p}$$

ex: $p = 101$

$$|N - 102| < 2\sqrt{101}$$
$$|N - 102| \leq 20$$
$$82 \leq N \leq 122$$

Add law on curve mod p
$P_1 = (x_1, y_1)$ $P_2 = (x_2, y_2)$ be points on
$E: y^2 \equiv x^3 + bx + c \bmod p$

then
$P_1 + P_2 = P_3 = (x_3, y_3)$ where

$x_3 \equiv m^2 - x_1 - x_2 \pmod p$ $y_3 \equiv m(x_1 - x_3) - y_1 \pmod p$

and $m = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} \pmod p & \text{if } P_1 \neq P_2 \\ (3x_1^2 + b)(2y)^{-1} \pmod p & \text{if } P_1 = P_2 \end{cases}$

add (1,1) and (5,2) in

$y^2 \equiv x^3 + 5x + 4 \mod 7$

$m \equiv (2-1)(5-1)^{-1} \equiv 4^{-1} \equiv 2 \mod 7$

$x_3 = m^2 - x_1 - x_2 \equiv 4 - 1 - 5 \equiv -2 \equiv 5$

$y_3 \equiv m(1-5) - 1$

$\equiv -8 - 1 = -9 \equiv -2 \mod 7$

$y_3 = 5$

$P_1 + P_2 = (5,5)$

5/6 Ex:

$E: y^2 \equiv x^3 + 5x + 3 \pmod{8009}$

$P = (1,3)$ and $-P = (1,-3)$ are on E

Find another point on E by computing $2P = P + P$

$m = (3 \cdot 1^2 + 5)(2 \cdot 3)^{-1} \mod 8009$

$8 \quad 6^{-1} \mod 8009$

$8 \quad 6^{-1} \mod 8009$

$8(1335) \mod 8009$

$\equiv 2671$

1335

$6 \overline{)8010}$

6

20

18

21

18

30

$x_3 = m^2 - x_1 - x_2$

$2671^2 - 1 - 1 \equiv 6229 \mod 8009$

$y_3 = 2671(1 - 6229) - 3 \equiv 7711 \mod 8009$

$2(1,3) \to (6229, 7711)$

21.5 - Elliptic curve cryptosystems based on the discrete log problem (Diff-Helman, El Gamal)

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

this is an abelian group under multiplication mod p

every elt has an inverse in the set

$V(p) \longleftrightarrow E$

nonzero # mod p $\longleftrightarrow$ Points on elliptic curve

mult. mod p $\longleftrightarrow$ Elliptic curve addition

1: Mult. identity $\longleftrightarrow$ elliptic infinity

mult inverse $\longleftrightarrow$ additive inverse $-(x,y) = (x,-y)$

Exponentiation $g^k \bmod p \leftrightarrow$ repeated addition $k \cdot P = P+P+\ldots P$

p-1 # of elts in $V(p)$ $\longleftrightarrow$ # of points on curve in $E = n$

fermat's: $g^{p-1} \bmod p \equiv 1 \longleftrightarrow$ Lagrange's theorem $nP = \infty$ $\forall P$ on E

DLP: $g^k \equiv h \bmod p$ solve for $k \longleftrightarrow$ given points P, Q on curve; solve $kP = Q$ for k

Elliptic curve DLP:
with smaller key sizes, get comparable levels of security

---

intle past m was int, now will be P on E

Elliptic Diffie Hellman key exchange

① Alice and Bob publicly agree on elliptic curve E and P and base point G on E (α in DH)

② Alice chooses random int a
Bob chooses random int b
Alice computes $A = aG$ and sends it to Bob
Bob computes $B = bG$ and sends it to Alice

④ Alice computes $K = aB$
Bob computes $K = bA$

$K = aB = a(bG) = b(aG) = bA$

⑤ K is the shared secret

Elgamal Encryption

1) Bob setup: chooses point on E and G on E
2) secret integer b and computes $B = bG$ (public) so
3) (E, G, B) is public

Encryption

1) Alice encodes her message as a point M on E
2) she chooses secret k and computes $R = kG$ and $T = M + kB$
3) she sends (R, T) to Bob

Decryption Bob receives (R, T) and computes

$$M = T - bR$$

$$T - bR = (M + kB) - b(kG)$$
$$M + k(bG) - b(kG)$$
$$= M + \infty$$
$$= M$$

5/8:

How to encode int m as a point on elliptic curve

$E:\ y^2 \equiv x^3 + bx + c \mod p$

$m < p$ otherwise break into blocks

have $m = x$ on point E

$M = (m, y)$ may not exist

$y^2 \equiv m^3 + bm + c$ may not have sol'n for y

$\frac{1}{2}$ Prob we can solve for y

Fix write m in binary and some 6 extra bits at end

$\widetilde{m} \equiv (m \text{ in binary}) \| b_1 b_2 b_3 b_4 b_5 b_6$

$\exists$ 64 such #s

Find point $\widetilde{m}$ on E of form $M = (\widetilde{m}, y)$ for some y

Prob not on E $\left(\frac{1}{2}\right)^{64} \approx 0$

receiver gets M, discard last 6 bits

More on ECDLP

For DLP we have α as a PR means smallest $k \geq 0$ such that $\alpha^k \equiv 1 \bmod p$ is $k = p-1$

How to choose Base point G for ECDH and EC Elgamal?

order of point G, on an elliptic curve is the smallest int m s.t. $mG = \infty$

If m is the order of G then there are m different possibilities for the value G

if $mG \Rightarrow \infty$
then
$(m+1)G \Rightarrow G$
$(m+2)G \Rightarrow 2G$

if m is very small, one can BF an ECDLP

Theorem: if elliptic curve has exactly n points on it and m is the order of point G on E, then $m | n$

$m \leq n$ and best case $m = n$ if possible

Attacks on ECDLP

Say G has order m and we want to solve

$$kG = Q \quad \text{for } k$$

1) BF: Try $k = 0 \dots m-1$
and evaluate kG until we get Q

To stop, have m large enough so this isn't feasible

BSGS: choose N

$$N = \sqrt{m}$$

make lists:

(I) Compute $k \cdot G$ for $k = 0 \dots N-1$

(II) Compute $Q - lNG$ for $l = 0 \dots N-1$

there will be a match in the 2 lists

$$kG + lNG = Q$$

$$\underbrace{(k + lN)}\, G = Q$$

discrete log

amount of work / storage $\Rightarrow$ proportional to $\sqrt{m}$

choose m large enough such that this isn't feasible

③ Pohlig-Hellman: if q is a prime divisor of n we can determine the value of $k \bmod q$

for the ECDLP: $kG = Q$

if we can find $k \bmod q$ or $\lceil \bmod q' \rceil$ $\forall$ prime divisors of n, then we can do CRT to solve for k

if n has all small divisors then the ECDLP can be solved via Pohlig Hellman

to thwart: make sure n has at least 1 large prime factor

Recall: m/n n # of points on E

if n has all small Prime factors then any ECDLP in E can be solved