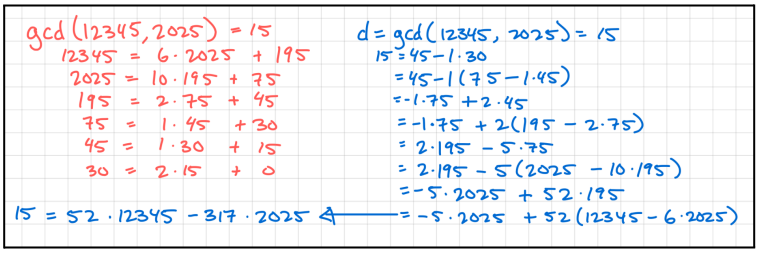
Substitution Cipher: Characters replaced with another character
Attacks: short words, letter frequency, common 2-letter/3-letter
Vigenere Cipher: Keyword encrypts according to tabula recta. Repeat keywords as needed. Weakness: Short keywords
→ **Kasiski Examination:** Repeated groups of ciphertext may reveal key length. Line up characters and count, expect the actual key to be reflective of the English alphabet freq. A/E/I Peaks, RST Peaks
→ **Distinction:** substitution cipher letter freq follow English Alphabet
Friedman's Coincidence Index:

$I_e = 0.0656 \qquad I_r = (\frac{1}{26})^2 \approx 0.0385 \qquad I_c = \sum_{i=1}^{26} \frac{N_i(N_i-1)}{N(N-1)}$

$k \approx \frac{I_E - I_r}{I_c - I_r} = \frac{0.0656 - 0.0385}{I_c - 0.0385}$

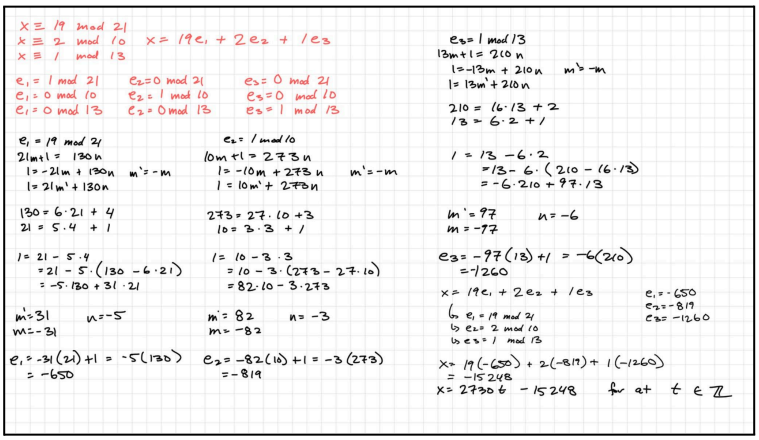
Kerckhoff's Principle: A good crypto-system should be secure even when the adversary knows the algorithm. Security should rely on key
Cryptography: Data communications and storage in a secure format
Cryptanalysis: The science of analyzing and breaking ciphers.
b | a: read as "b divides a" → "b is a factor of a" // "a is divisible by b"
Fundamental Theorem of Arithmetic: Every positive integer $n > 1$ can be written as a unique product of primes(p's repeat). $n = p_1 p_2 \dots p_r$

→ **Euclid's Lemma:** An integer $p \geq 2$ is prime if and only if whenever a and b are integers s.t. p divides ab, then p divides a or p divides b.
Unit: An element $\alpha \in Z/mZ$ is called a unit if there is some $b \in Z/mZ$ such that $ab \equiv 1 \bmod m$
Euclidean Algorithm: Used to compute the gcd of large numbers
→ **Bezout's Lemma(in blue):** Let a, b be positive integers. Then gcd(a, b) is the smallest possible integer than can be written in the form of $ma + nb$, where m,n are integers. If d=gcd(a,b) then d | a and d | b, so d | ma + nb for all integers m, n.



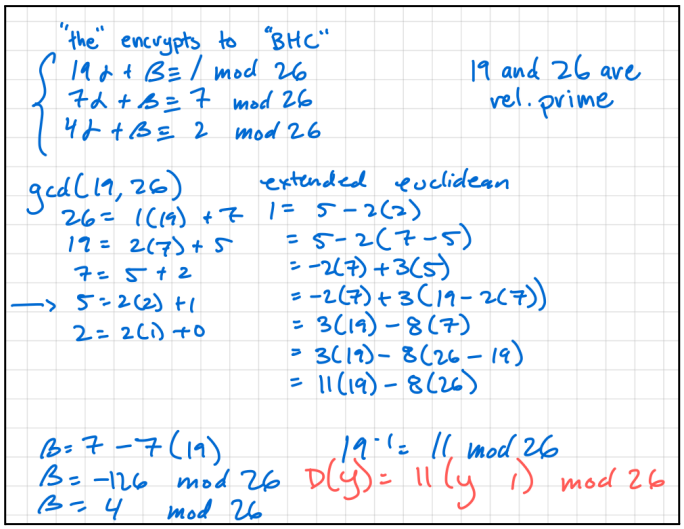
Chinese Remainder Theorem: Suppose $n_1, n_2, \dots, n_k$ are integers which are pairwise relatively prime(any two of them are relatively prime). Then for any integers $a_1, a_2, \dots, a_k$ then $x \equiv a_i \bmod n_i \; for \; 1 \leq i \leq k$

1. Check the set contains pairwise relatively prime numbers
2. Create identity matrix for all values, e, we are trying to solve for
3. Use the Euclidean algorithm to get the total fo the bigger mod
4. Use the Extended Euclidean Algorithm to get m, n factors
5. Plug in m, and n to get the e values
6. Add all e-values to get a value for x.
7. There are multiple solutions for multiple of congruence

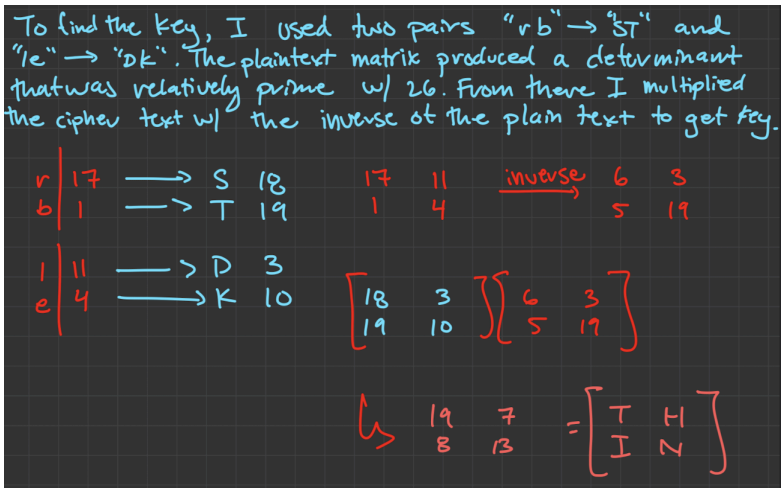


Relatively Prime: Two integers are relatively prime if their greatest common divisor is 1, i.e. they share no common factors other than 1

Euler Totient Function
$\phi(n) = \#\ of\ positive\ integers \leq n\ that\ are\ relatively\ prime\ to\ n$
$\phi(4) = 2 = [1, 3] \quad \phi(5) = 4 = [1, 2, 3, 4] \quad \phi(p) = p - 1\ if\ p\ is\ prime$
Affine Cipher
Encryption: Choose two integers $\alpha, \beta\ with\ gcd(\alpha, \beta) = 1$. The encryption function is defined as $x \Rightarrow \alpha x + \beta \bmod 26$
Decryption: To decrypt, we need multiplicative inverse
Keys: a → ϕ(26)=12 keys, b → 26 possible keys. 312 Total



Hill Cipher(really weak, creating linear system of equations)
Encryption: Matrix multiplication on a block of plaintext by an invertible matrix(determinant is relatively prime to 26)
Decryption: Calculate the inverse of the n x n encryption matrix.
2x2 matrix inverse => (1 / det) * [[d -b][-c a]] mod 26
Key: Invertible n x n matrix(or a keyword that tells us how to generate it)



Playfair Cipher(British field cipher)
Structure: Start with a keyword. Remove duplicates + combine i/j. Write keyword into the 5x5 square and follow with rest of the letters alphabetically
Encryption: Form digraphs from plain text. If a digraph is a repeated letter, split it into two groups by inserting "x" between the repeated letters. If needed add an "a" at the end to form the final digraph.
Decryption: Reverse the encryption rules

Digraphs fall into three possible cases:

1. Both letters in the digraph are in the same row of the 5 × 5 grid
   - ⟶ replace each letter in the digraph by the letter to the right of it (wrapping around, if necessary)
   - E.g., `to` encrypts to `UP`
2. Both letters in the digraph are in the same column
   - ↓ replace each letter by the letter below it (wrapping, if necessary)
   - E.g., `ge` encrypts to `OG`
3. Letters in digraph are not in same row or same column
   - ☐ create the rectangle in the grid that the two letters form
   - to encrypt first letter, look along its row until you get to the end of the rectangle, replace with that letter
   - to encrypt second letter, do the same
   - E.g., `me` encrypts to `GD`

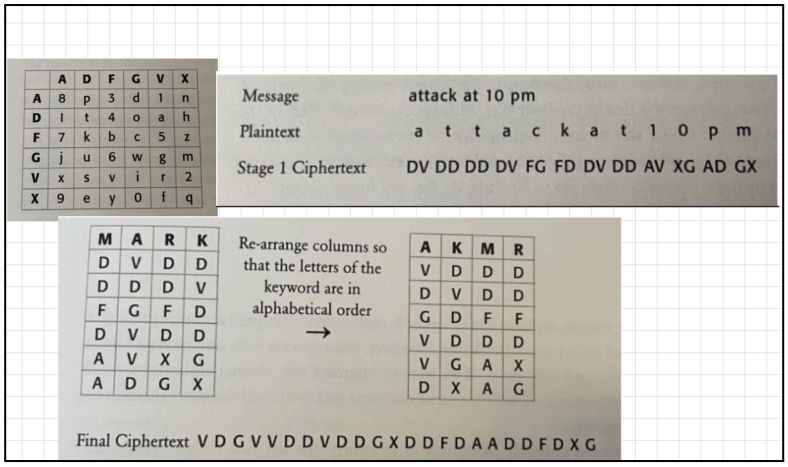
ADFGVX Cipher

Structure: Decide on a keyword and number. Fill in a 6x6 grid alternating letters and numbers according to the chosen keyword and number marking each row and column with the acronym ADFGVX.

Stage 1 Encryption: Read the row and column labels for each plaintext

Stage 2 Encryption: Choose a keyword. Write the letters of the keyword as the top row of a fresh grid. Write the first stage cipher text in the grid in a series of rows. Rearrange the columns by alphabetizing the letters of the keyword. Read off the final ciphertext by reading down the columns.

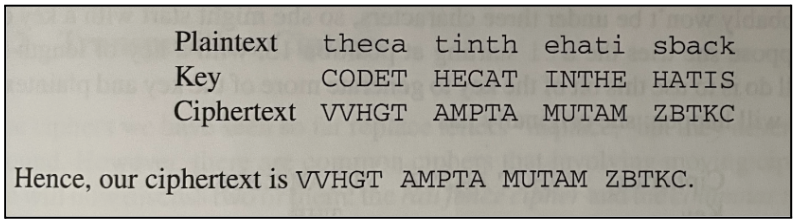
Decryption: Create the 6x6 grid. Line up all cipher text characters in a grid, and then rearrange the columns to match the keyword phrase. Then lookup [row,col] pairs.



Autokey

Structure: Same as the Vigenere, but the key is extended by encoding using the plain text

Attacking: Pick "n-grams" that you expect to be in the plain text and then repeat and use them to decrypt in different positions until you get some recognizable text.



One Time Pad

Only proven crypto-system to be secure. Weakness in the need to generate an extensive amount, as well as keeping code books secure, secure delivery, and maintaining correct position between sender/receiver

Enigma

3 Scramblers with 26 settings = $26^3 = 17,576\ orientations$

Rearrangement of scramblers = $3! * 26^3 = 105,456\ different\ orders$

Plugboard swaps six pairs. 26 Choose 6 = $n!\ /\ k!\,(n-k)!$

$$\binom{26}{12} \cdot 11 \cdot 9 \cdot 7 \cdot 5 \cdot 3 \cdot 1 = 100,391,791,500.$$

Total. The total number of keys is the multiple of these three numbers: $17{,}576 \times 6 \times 100{,}391{,}791{,}500$

$\approx 10{,}000{,}000{,}000{,}000{,}000$

Binary Operation: A binary operation $*$ on a set G is a function s.t. $G\ x\ G \rightarrow G$ that assigns to each pair $(a,\ b) \in G$ a unique element $a * b \in G$

Group: A group (G, $*$) is a set G together with a binary operation $*$ that satisfies the following

→ $*$ is associative $(a*b)*c = a*(b*c)\ for\ all\ a,\ b,\ c \in G$

→ an identity element exists $e \in G$ s.t. $e*a = a\ and\ a*e = a\ for\ any\ a \in G$

→ an inverse element exists $a^{-1} \in G$ s.t. $a*a^{-1} = a^{-1}*a = e$

Abelian Group: A group (G, $*$) that satisfies the commutative property $a*b = b*a\ for\ all\ a \in G$ is called an Abelian Group

Sub Group: A group (H, $*$) is a subgroup of (G,$*$) if H is a subset of G and when the operation $*$ is restricted to the set H, (H,$*$) is also a group

Cyclic Group: A group is said to be cyclic if there is some $a \in G$ s.t. For every $g \in G,\ g = a^n\ for\ some\ integer\ n$. a is said to be a generator.

→ **Cyclic SubGroups:** Let G be a group and $a \in G$. Then $< a >$ is a subgroup of G. $< a >$ is called the cyclic subgroup generated by a

→ every cyclic group is abelian

Order of a Group: If G is a finite group, then the order of G is the size of G as a set. |G| = n. If G is not finite, then G has infinite order

Order of an Element: Let G be a group and $a \in G$. Define the order of a to be the smallest positive integer $n\ s.t.\ a^n = e$. If there is no such integer, then a has infinite order. If G is a cyclic group and a is a generator, then |a| = |G|

Lagrange's Theorem: Let G be a finite group and H be a subgroup of G. The |H| divides |G|

→ Suppose G is a finite group and $g \in G$. Then the order of g must divide the ofer of G.

Ring: A non-empty set R is a ring if it has two binary operations(+, $*$) s.t

→ $(R, +)$ is a abelian group

→ the binary operation $*$ is associative

→ $a(b+c) = ab + bc\ and\ (a+b)c = ac + bc\ for\ all\ a,\ b,\ c \in R$

The multiplication operator $*$ does not need to be commutative in a general ring. If $*$ is commutative, we call it a commutative ring

Field: A field is a set F with two binary operations(+, $*$) s.t.

→$(F, +, *)$ is a commutative ring

→The non-zero elements of F, denoted F^xalso form an Abelian group under multiplication.

In a field, multiplication is commutative and every non-zero element has a multiplicative inverse

Characteristic of a Field: The characteristic of a field F is the least positive integer n such that $nx = 0\ for\ all\ x \in F$. If no such integer exists then the characteristic of F is defined to be 0.

Euler's Theorem: Let a and n be integers such that $n > 0$ and $gcd(a,\ n) = 1$. Then $a^{\phi(n)} \equiv 1\ mod\ n$

→ **Fermat's Little Theorem(special case when n = p is prime):** Let p be any prime and suppose that p does not divide a. Then $a^{p-1} \equiv 1\ mod\ p$

Furthermore $b^p \equiv b\ mod\ p\ for\ any\ integer\ b$

Primitive Root Theorem: Let p be a prime. Then there is some $g \in {F_p}^x$ so that all elements of ${F_p}^x$ are powers of g. For such an element g, $g^{p-1} \equiv 1\ mod\ p,\ but\ g^r \neq 1\ mod\ p\ for\ 1 \leq r \leq p-2$

→ The g from this theorem is called a primitive root in ${F_p}^x$

→ another way to say that $((Z/pZ)^x,\ *)$ or $({F_p}^x,\ *)$ is a cyclic group and that g is a generator.

Isomorphism: All cyclic groups with the same number of elements are "essentially the same" structure/group

→ $(Z/(p-1)Z,\ +)\ is\ isomorphic\ to\ ({F_p}^x,\ *)$

→ Group structure is preserved, so the number of generators are the same. There are $\phi(p-1)$ primitive roots in ${F_p}^x$

Fermat Pseudoprime: For an integer $a > 1$, if a is a composite integer n that satisfies $a^{n-1} \equiv 1\ mod\ n$ then n is called a Fermat pseudoprime to base a

→ a fermat pseudoprime to base a will be relatively prime to a

Carmichael number: A composite integer n that satisfies $a^{n-1} \equiv 1\ mod\ n\ for\ all\ integers\ a > 1$

→ The smallest Carmichael number is $561 = 3 * 11 * 17$

Multiplicative Function: A function $f: N \to R$ is called multiplicative if whenever gcd(a, b) = 1 then f(ab) = f(a)f(b)

Divisors of n – d(n)

Let $n \in Z^+$. Define d(n) = the number of divisors of n (including 1 and n).

Suppose $n = \prod_{i=1}^{r} p_i^{e_i}$ is the prime factorization of n, where all p_1's are distinct. $d(n) = \prod_{i=1}^{r} (e_i + 1) \to n = 80 = 2^4 * 5 \quad d(n) = (5)(2) = 10$

Sum of all divisors - $\sigma(n)$

Let $n \in Z^+$. Let $\sigma(n) = sum\ of\ all\ divisors\ of\ n.$

If p is a prime, and $e \in Z^+$, $\sigma(p^e) = 1 + p + p^2 + \ldots + p^e = \frac{p^{e+1}-1}{p-1}$

$\to \sigma(60) = \sigma(2^2)\sigma(3^1)\sigma(5^1) = (1 + 2 + 2^2)(1 + 3)(1 + 5) = 168$

Euler's Totient: $\phi(n) = \prod_{i=1}^{r} \sigma(p_i^{e_i})$. If p is prime, then $\phi(p^e) = p^e - p^{e-1}$

$\to \phi(66) = \phi(2)\phi(3)\phi(11) = (2 - 1)(3 - 1)(11 - 1) = 20$

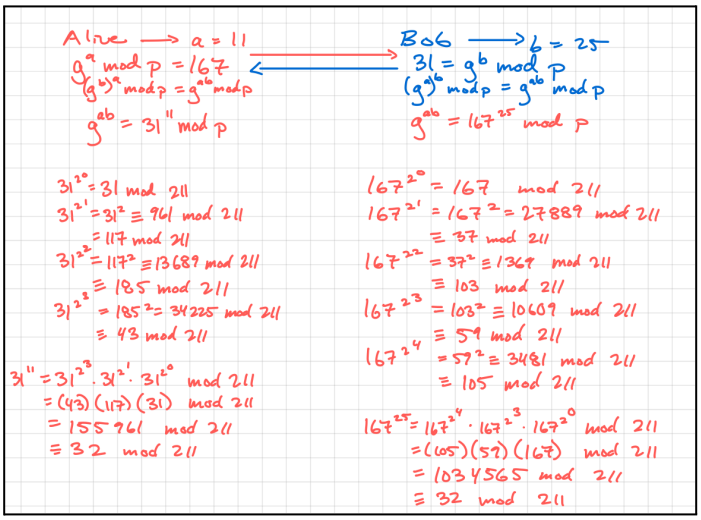
$\to \phi(32) = \phi(2^5) = 2^5 - 2^4 = 32 - 16 = 16$

Diffie-Hellman Key Exchange: Sharing of $g^a mod\ p$ and $g^b mod\ p$ allowing both parties to calculate $g^{ab} mod\ p$ without third parties knowing either a or b. $g^{p-1} \equiv 1\ mod\ p \to 0 \leq a,\ b,\ \leq p - 2$. If p is huge, then guessing a or b becomes infeasible. No mechanism for encrypt/decrypt

→ **Discrete Logarithm Problem:** Given a cyclic group G, a generator $g \in G$ and $x \in G$, find a number n so $x = g^n$

1. DLP is hard in general, DLP in $(F_p^{\ x}, \bullet)$ is not easy
2. Structure/form of the group may make it harder
3. If you can solve DLP, then it's easy to solve DHP

→ **Diffie-Hellman Problem:** Given a cyclic group G, a generator $g \in G$ and two element in g^a and g^b in G, compute g^{ab}



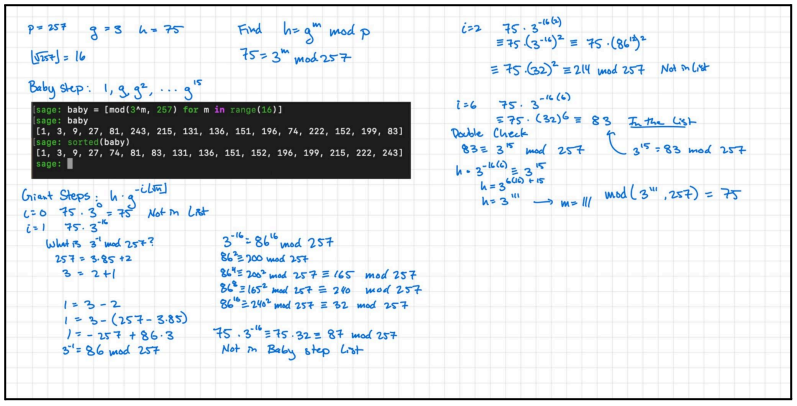
El Gamal: Full Cryptosystem based on Diffie-Hellman Key Exchange

Encryption: Pick prime and generator in $F_p^{\ x}$. Choose $0 \leq a \leq p - 2$. Compute $h = g^a mod\ p \to (h,\ g,\ p)$. Choose $0 \leq b \leq p - 2$. Compute $s = h^b mod\ p \to c_1 = g^b mod\ p\ and\ c_1 = ms\ mod\ p \dashrightarrow (c_1,\ c_2)$

Decryption: Compute $s = c_1^{\ a} mod\ p \to s^{-1} c_2 mod\ p$

Shank's Baby-Step Giant-Step Algorithm: Let G by a cyclic group of size n with a generator g. Given $h \in G$, the following algorithm computers an m such that $h = g^m$ in $O(n^{\frac{1}{2}+\epsilon})\ time$

1. Compute and store the "baby step" values: $1,\ g,\ g^2,\ \ldots\ g^{\lfloor\sqrt{x}\rfloor - 1}$
2. Compute the "giant step" values: $hg^{i\lfloor\sqrt{n}\rfloor}\ for\ i = 0,\ 1,\ 2,\ \ldots.$
   a. For each i, check whether the result is on the baby step list. If a match is found, stop. Otherwise, increment i and keep going.
3. Once your have found a match, you have found an i and j such that $hg^{-i\lfloor\sqrt{n}\rfloor} = g^j$, so, $h = g^{i\lfloor\sqrt{n}\rfloor + j}$



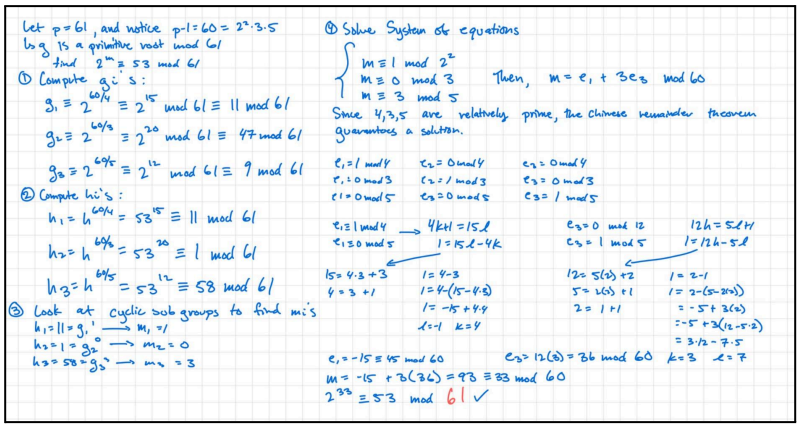
Pollhig-Hellman: Let p be a prime such that $p - 1 = \prod_{i=1}^{r} p_i^{e_i}$ and suppose g is a generator of $F_p^{\ x}$. The Pollhig Hellman algorithm to find the discrete log of h in $F_p^{\ x}$ is:

1. For $i = 1, \ldots, r$ compute $g_i = g^{(p-1)/p_i^{e_i}}$ This e has order $p_i^{e_i}\ in\ F_p^{\ x}$
2. For $i = 1, \ldots, r$ compute $h_i = h^{(p-1)/p_i^{e_i}}$ By construction $h_i \in < g_i >$
3. Since the p_i's are small, it should be easy to solve the DLP in $< g_i >$ i.e. find $m_i \in \{0, \ldots, p_i^{e_i} - 1\}$ such that $g_i^{m_i} = h_i$
4. The Chinese remainder Theorem guarantees a solution to be the system of equations: $m \equiv m_i\ mod\ p_i^{e_i}$ and this solution m will be the discrete log of h in $F_p^{\ x}$ (with generator g)

→ For Diffie-Hellman, or El Gamal in $F_p^{\ x}$, we'd want to pick a prime that does not have p - 1 factoring into a lot of small primes

–? If p is greater than 2, then p - 1 is even. Ideally $(p - 1)/2$ is prime so that $p - 1$ has the largest possible prime factor

→ If p and $2p + 1$ are both primes, then p is called a Sophie Germain prime and $2p + 1$ is called a safe prime



RSA: public key (n, e) private key d

Encryption: Prime numbers p, q. $n = p * q \quad \phi(n) = (p - 1)(q - 1)$

Choose $1 < e < \phi(p)$ and $gcd(e,\ n) = 1$ Compute $d = e^{-1} mod\ \phi(n)$.

$c = m^e mod\ n \qquad c^d = m$ is the plaintext

→Security of RSA relies on $\phi(n)$ being hard to find

→ Malleable: changing m predictably also changes c in predictably

$$c = (2m)^e = 2^e m^e = 2^e c\ mod\ n \mid r^e c\ mod\ n$$

$$\text{Decrypt}: u = (2^e c)^d = 2^{ed} c^d = 2c^d\ mod\ n$$

→ Padding: Append some random digits into plaintext message before

→ blocking: RSA Encryption is slow→ encrypt a set number of characters

→ e is usually $2^{16} + 1 = 65,537$

RSA Digital Signature(encrypt-then-sign)

Receiver public/sender private: $c = e_b(m) \to s = d_a(c)$

Sender public/receiver private: $c = e_a(s) \to m = d_b(c)$

Rabin Cryptosystem: $p \equiv 3 mod 4 // q \equiv 3\ mod\ 4\ //\ n = pq$

Encryption: plaintext m is a number in {0, …, n1-} $c = m^2\ mod\ n.$ computationally more efficient than RSA

1. Compute

$$m_p = c^{(p+1)/4} \mod p$$
$$m_q = c^{(q+1)/4} \mod q$$

Note: $p \equiv 3 \mod 4$ implies 4 divides $(p+1)$.
Likewise, 4 divides $(q+1)$.

2. Use the Extended Euclidean Algorithm to find y_p and y_q such that

$$y_p p + y_q q = 1.$$

3. Then compute

$$r = (y_p p m_q + y_q q m_p) \mod n$$
$$s = (y_p p m_q - y_q q m_p) \mod n$$

$\pm r, \pm s$ are the four square roots of $c \mod n$.
So, one of them is the original plaintext message m.

Generalized Birthday: collisions of n possible requires $\sqrt{2n\,ln(2)}$

Pollard Rho Algorithm for factoring

The following algorithm tends to find a factor of an integer n significantly faster than the "guess-and-check" method.

1. Choose a random polynomial $f(x)$ that takes values in $\mathbb{Z}/n\mathbb{Z}$ and returns values in $\mathbb{Z}/n\mathbb{Z}$ (e.g., $f(x) = x^2 + 1 \mod n$)
2. Set $x = 2, y = 2$ [you could start elsewhere if you like]
3. Replace x with $f(x)$ and replace y with $f(f(y))$
4. Compute $d = \gcd(|x - y|, n)$
5.
   - If $d = 1$, go to Step 3.
   - If $d = n$, algorithm fails. Pick another function $f(x)$ and try it.
   - If $d \neq 1$ and $d \neq n$, SUCCESS! You've found a factor of n.

Miller-Rabin Primality Test

Theorem

Let n be an odd positive integer and let $s = \max\{r \in \mathbb{N} : 2^r \text{ divides } (n-1)\}$. So, 2^s is the largest power of 2 dividing $(n-1)$. Set $d = (n-1)/2^s$.

If n is prime and a is an integer relatively prime to n, then either

$$a^d \equiv 1 \mod n,$$

or there exists an r in the set $\{0, 1, \ldots, s-1\}$ with

$$a^{2^r d} \equiv -1 \mod n.$$

→ when a number a allows us to prove the compositeness of an integer n via the miller rabin test, a is miller rabin witness to the compositeness of n
→ If n is a fermat pseudoprime to base a, but a is not miller-rabin witness to the compositeness of n, we call a miller-rabin non-witness
→ if a is a miller non-witness, we say n is a strong pseudoprime to base a

Rational Points Curves: Which $(x, y) s.t.\ x,\ y \in Q$ lie on Unit Circle

$t = (\frac{1-t^2}{1+t^2},\ \frac{2t}{1+t^2})$ gives rational parametrization of $x^2 + y^2 = 1$

Let $t = \frac{m}{n}$ for integers m, n → $(\frac{n^2-m^2}{n^2+m^2},\ \frac{2mn}{n^2+m^2})$

Let (a, b, c) *be values s.t.* $a^2 + b^2 = c^2$ *where* $gcd(a, b) = 1$
Then for some integers m,n we have: gcd(m,n) = 1 // m,n not both odd
$(a, b, c) = (m^2 - n^2, 2mn, m^2 + n^2)$ *or* $= (2mn, m^2 - n^2, m^2 + n^2)$

Elliptic Curve: a curve of the form $y^2 = x^3 + ax + b$ where a,b are such that $4a^3 + 27b^2 \neq 0$. Discriminant is $-(4a^3 + 27b^2)$.
$D = 0 \Rightarrow$ *no repeated roots* // $D > 0 \Rightarrow 3$ *real* // $D < 0 \Rightarrow 1$ *real*, 2 *imag*
Points on elliptic curves form an abelian group

Elliptic Curves and Cryptography: provide the same level of security with much smaller key sizes. 3072 bit RSA equivalent to 256 bit. Analog of Baby Shank takes too much memory, Pohlig-Hellman can be avoided

- DHKE: send over aP and bP to compute the shared key
- El G: $(p, E(F_p), P, aP$ // $c_1 = bP$ *and* $c_2 = m + b(aP)$ // $c_2 - ac_1 = m$
- Encoding: X will be within 100. Find intersection of X on E, where y^2

N-Torsion: g is a n-torsion element of g if $n * g = g + g \ldots + g = e$
Elliptic Curve subgroup: <p> denotes {P+2P+...+nP+infinity}

Elliptic Curve Addition: Define Abelian group where elements are points (x,y) on an elliptic curve. Take 2 points, P, Q on the elliptic curve. Pass a line through P and Q. It will intersect in exactly one more point.

Let E be given by

$$y^2 = x^3 + ax + b$$

and let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$.

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

$$x_3 = m^2 - x_1 - x_2$$
$$y_3 = m(x_1 - x_3) - y_1$$

and

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

If the slope m is infinite, then $P_3 = \infty$.

Also, $\infty + P = P$ for all points P.

Elliptic Curves over Finite Fields: Apply the same formula over F_p

At random, we expect $x^3 + ax + b \bmod p$ to be a square about half the time, and when it is a square it will produce 2 points on the curve unless it's 0, then it produces only 1 point. We expect p + 1, with infinity point

Let p be a prime.

Now we look at an elliptic curve

$$E: \quad y^2 = x^3 + ax + b$$

where $x, y \in \mathbb{F}_p$.

So we say

$$E(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p \text{ and } y^2 \equiv x^3 + ax + b \mod p\}.$$

We also still include a point at ∞ (with the same meaning as before); and ∞ is still the group's identity.

We also still need the discriminant to be "$\neq 0$", which in the finite field context means we need

$$4a^3 + 27b^2 \not\equiv 0 \mod p.$$

Let E be the elliptic curve:

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

Note:

$$4a^3 + 27b^2 = 4 \cdot 4^3 + 27 \cdot 4^2$$
$$\equiv 1 + 2(1) \mod 5$$
$$\equiv 3 \not\equiv 0 \mod 5$$

Theorem (Hasse's Theorem (or the "Hasse-Weil Bound"))

Let E be an elliptic curve over $\mathbb{F}_p$. Let $\#E(\mathbb{F}_p)$ indicate the number of points in $E(\mathbb{F}_p)$. Then

$$|\,\#E(\mathbb{F}_p) - (p+1)\,| \leq 2\sqrt{p}.$$

$x = 4 \Rightarrow y^2 = 64 + 16 + 4 \equiv 4 \mod 5$
$\Rightarrow y = 2, 3$
So we have found that
$E(\mathbb{F}_5) = \{\infty, (0,2), (0,3), (1,2), (1,3), (2,0), (4,2), (4,3)\}$
points on $E(\mathbb{F}_5) = 8$

Let's try $(0,2) + (4,3)$ on this example curve $E(\mathbb{F}_5)$.

First we calculate
$m = \frac{3-2}{4-0} = \frac{1}{4} = 1 \cdot 4^{-1} \mod 5$
(needs to happen in $\mathbb{F}_5$)

What is $4^{-1} \mod 5$
$4 \cdot 4 = 16 \equiv 1 \mod 5$
so $4^{-1} = 4 \mod 5$
so $m = 4$

Then $x_3 = m^2 - x_1 - x_2$
$= 4^2 - 0 - 4 = 12 \equiv 2 \mod 5$
$y_3 = m(x_1 - x_3) - y_1$
$= 4(0-2) - 2$
$= -10 \equiv 0 \mod 5$
so on $E(\mathbb{F}_5)$:
$(0,2) + (4,3) = (2,0)$

Now let's try
$2 \cdot (0,2)$ or $(0,2) + (0,2)$
now we use the "$P_1 = P_2$" formula for m:
$m = \frac{3 \cdot 0^2 + 4}{2 \cdot 2} = \frac{4}{4} = 1$
so then $x_3 = 1^2 - 0 - 0 = 1$
$y_3 = 1(0-1) - 2 = -3 \equiv 2 \mod 5$

So $(0,2) + (0,2) = (1,2)$