Telling Secrets

Secret Writing Through the Ages

William Turner

Department of Mathematics & Computer Science
Wabash College
Crawfordsville, IN 47933

Tuesday 4 February 2014

Outline

Cryptography

Definition

Practice of the enciphering and deciphering of messages in secret code in order to render them unintelligible to all but the intended receiver.

- *Hidden* communication
- Plaintext $\longleftrightarrow$ ciphertext
- Encrypt and decrypt / encipher and decipher

Etymology

- κρυπτός (hidden, secret) from κρύπτω (hide, cover)
- γράφω (write, draw)

... vs. Coding Theory

Definition

Efficient and reliable communication in an uncooperative (possibly hostile) environment.

- Encode and decode
- *Clear* communication

Examples

- ASCII, Unicode
- Morse Code
- Universal Product Code (UPC)

Symmetric-Key Algorithms

Definition

Cryptographic algorithms that use the same keys for both encryption and decryption.

- Key is a shared secret.
- Alice sends a message to Bob encrypted by a key only she and Bob knows.
- If Eve knows the key, she can decrypt the message.

Transposition Ciphers

Definition

Units of plaintext are rearranged to form the ciphertext.

Encrypt: Bijection acts on characters' positions

Decrypt: Apply the inverse function to the positions

Rail Fence Cipher

- Write plaintext on successive rails of an imaginary fence.
- Read ciphertext from along each rail.

Example

- Encrypt "WABASH ALWAYS FIGHTS" on a three-rail fence.

W . . . S . . . W . . . F . . . T .

. A . A . H . L . A . S . I . H . S

. . B . . . A . . . Y . . . G . . .

- Cipher text is "WSWFTAAHLASIHSBAYG".

Columnar Transposition

- Plaintext is written on successive rows of fixed length.
- Rearrange columns using keyword.
- Ciphertext is read from columns.

Example

- Encrypt "WABASH ALWAYS FIGHTS" using keyword "ZEBRA".

Z	E	B	R	A
W	A	B	A	S
H	A	L	W	A
Y	S	F	I	G
H	T	S		

- Cipher text is "SAGBLFSAASTAWIWHYH".

Substitution Ciphers

Definition

Units of plaintext are replaced with ciphertext.

Encrypt: Bijection acts on *contents* of the units

Decrypt: Apply the inverse function to the *contents*

Types

Simple Substitution Cipher: operates on single letters

Polygraphic Cipher: operates on groups of letters

Monoalphabetic Cipher: uses fixed substitution over entire message

Polyalphabetic cipher: uses different substitutions at different positions in the message

Caesar Cipher

- Supposedly used by Julius Caesar in his private correspondence.
- Replace each letter by a letter some fixed number of positions down the alphabet

Example

- Encrypt "WABASH ALWAYS FIGHTS" with a Caesar right shift of 3.
- A becomes D, B becomes E, C becomes F, ..., W becomes Z, X becomes A, Y becomes B, Z becomes C
- Cipher text is "ZDEDVKDOADBVILJKWV".

Enigma Machine

- Set plugboard and rotors
- Press key on keyboard
- Rotors with randomly wired contacts rotate to new position
- Read letter from the lampboard

Advanced Encryption Standard (AES)

2001: Established by NIST

2002: Approved as federal government standard

2003: Approved by NSA for top secret information

Steps

- Put message in 4×4 column-major order matrix of bytes (the *state*)
- Expand expand a short key into a number of separate round keys
- AddRoundKey – Combine each byte of the state with the round key using bitwise XOR
- SubBytes – Replace each byte with another from lookup table
- ShiftRows – Shift last three rows cyclically some number of steps
- MixColumns – Combine the four bytes of each column

AES Encryption

1. Expand expand a short key into a number of separate round keys
2. InitialRound
    1. AddRoundKey – Combine each byte of the state with the round key using bitwise XOR
3. Rounds
    1. SubBytes – Replace each byte with another from lookup table
    2. ShiftRows – Shift last three rows cyclically some number of steps
    3. MixColumns – Combine the four bytes of each column
    4. AddRoundKey
4. Final Round
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey

Symmetric Cipher Keys

- Symmetric cipher keys must be kept secret
- Requires some means of secure communication to establish key
- Catch-22

Asymmetric Cryptography

Definition

Cryptographic algorithm that requires two separate keys, one of which is secret (or private) and one of which is public.

- Public key cryptography
- Alice and Bob do not need to agree on a key in advance
- Eve can know the public key, but still cannot decrypt the message without the private key
- Security based on operations easy to perform, but hard to invert.
- One-way functions described in 1874 by William Jevons.

Diffie-Hellman Key Exchange

- Published in 1976 by Whitfield Diffie and Martin Hellman.
- Independently used by British GCHQ in 1973.
- Method of establishing a shared secret (e.g., for symmetric cipher)
- Discrete logarithm problem
  - Consider $y = g^x \bmod p$.
  - Relatively easy to compute y given x.
  - Difficult to compute x given y.

Diffie-Hellman Key Exchange

1. Alice and Bob agree on prime p and base g. (Both are public.)
2. Alice chooses a secret integer a and sends Bob $A = g^a \bmod p$.
3. Bob chooses a secret integer b and sends Alice $B = g^b \bmod p$.
4. Alice and Bob can share secret $s = g^{ab} \bmod p$.
   - Alice computes $s = B^a \bmod p$.
   - Bob computes $s = A^b \bmod p$.
5. Eve can know p, g, A, B, but not s.

Example

- $p = 101$, $g = 7$.
- $a = 5 \implies A = 7^5 \bmod 101 = 41$
- $b = 11 \implies B = 7^{11} \bmod 101 = 51$
- $51^5 \bmod 101 = 60$ and $41^{11} \bmod 101 = 60$.

RSA Encryption

- Published in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.
- Asymmetric form of communication.
  - Alice encrypts a message to Bob with Bob's public key.
  - Ciphertext can only be decrypted by Bob's private key.
  - Bob can send a message to Alice using Alice's public key.
- Also used for digital signatures.
  - Alice encrypts a with her private key and sends both the plaintext and the ciphertext.
  - Ciphertext can only be decrypted by Alice's public key.
  - If decrypted message matches, Alice must have sent it.
- Uses exponentiation modulo m to encrypt message.
- Integer factorization problem.

RSA Encryption

1. Bob picks two distinct prime numbers p, q. (Private)
2. Bob computes product $m = pq$. (Public)
3. Bob computes Euler's totient function $\varphi(m) = (p-1)(q-1)$. (Private)
4. Bob picks integer e such that $\gcd(e, \varphi(m)) = 1$. (Public)
5. Bob computes $d \equiv e^{-1} \pmod{\varphi(m)}$. (Private)
   - Solve $ed \equiv 1 \pmod{\varphi(m)}$ by Extended Euclidean Algorithm
6. Alice can encrypt a message M with $\gcd(M, m) = 1$ as $C = M^e \bmod m$.
7. Bob decrypts the ciphertext C as $M = C^d \bmod m$.

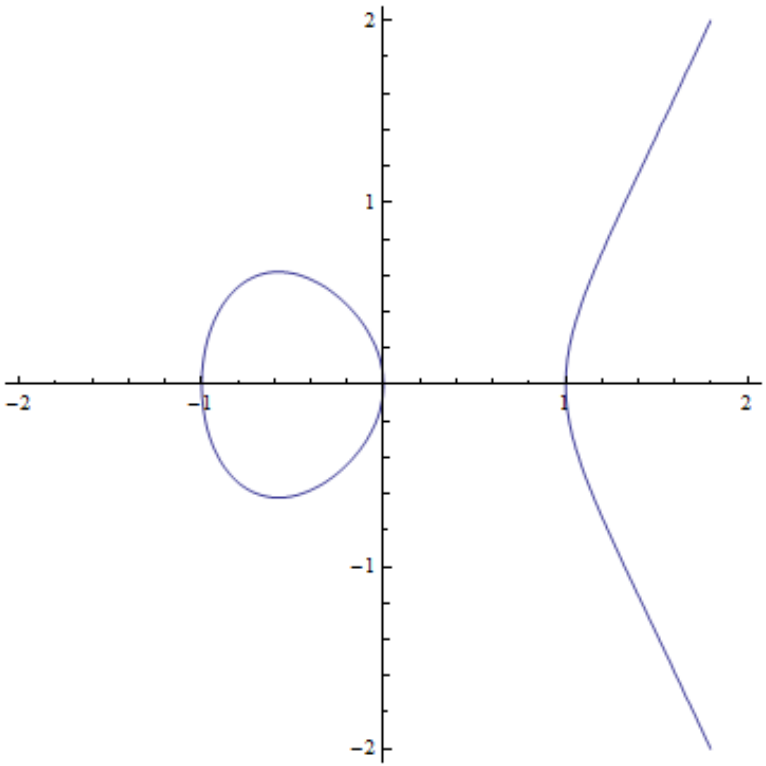
RSA Encryption

Example

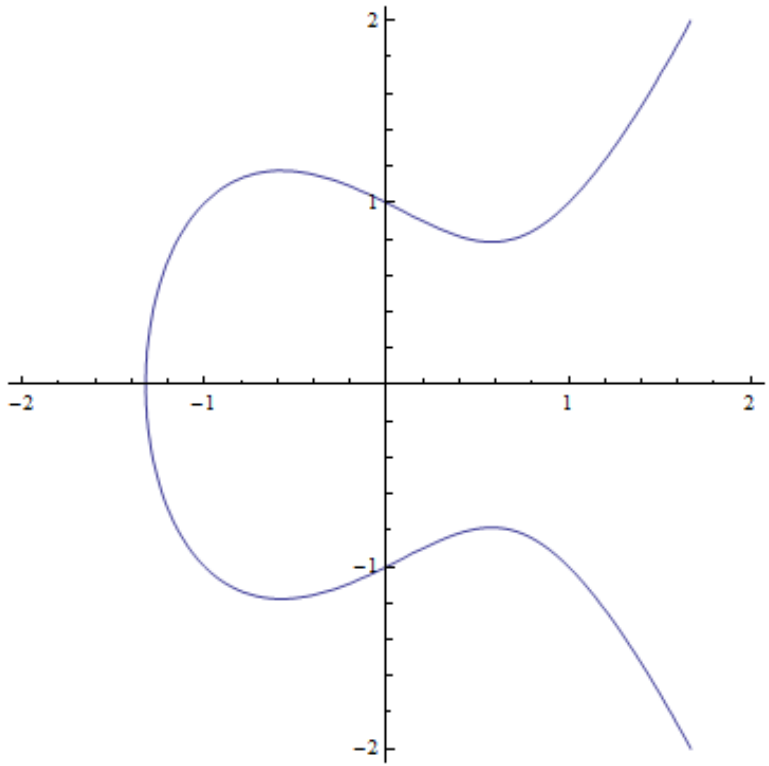
- $p = 101, q = 103 \Longrightarrow m = 10403, \varphi(m) = 10200.$
- $e = 2243 \Longrightarrow d = 5507.$
- Convert "WABASH ALWAYS FIGHTS" to ASCII:
  $M = [87, 65, 66, 65, 83, 72, 32, 65, 76, 87,$
  $65, 89, 83, 32, 70, 73, 71, 72, 84, 83]$
- Encrypt:
  $C = [2620, 1835, 5420, 1835, 6113, 2874, 544,$
  $1835, 8507, 2620, 1835, 7335, 6113, 544,$
  $1726, 848, 9447, 2874, 1198, 6113]$
- Decrypt:
  $M = [87, 65, 66, 65, 83, 72, 32, 65, 76, 87,$
  $65, 89, 83, 32, 70, 73, 71, 72, 84, 83]$

Elliptic Curves

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



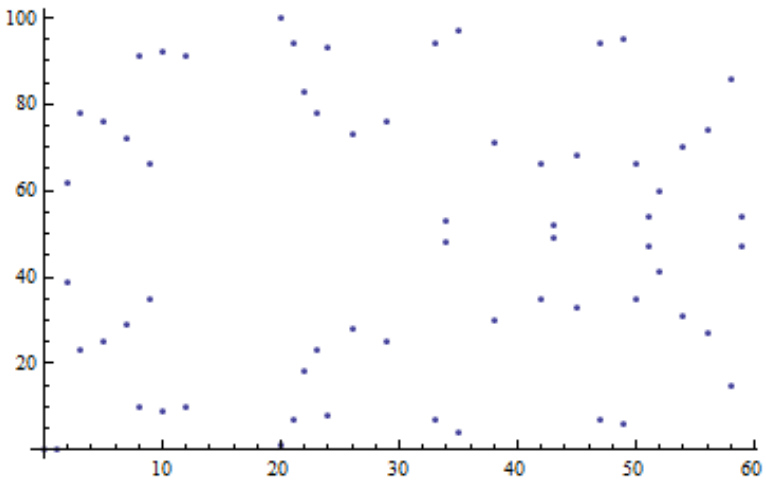
$y^2 = x^3 - x$



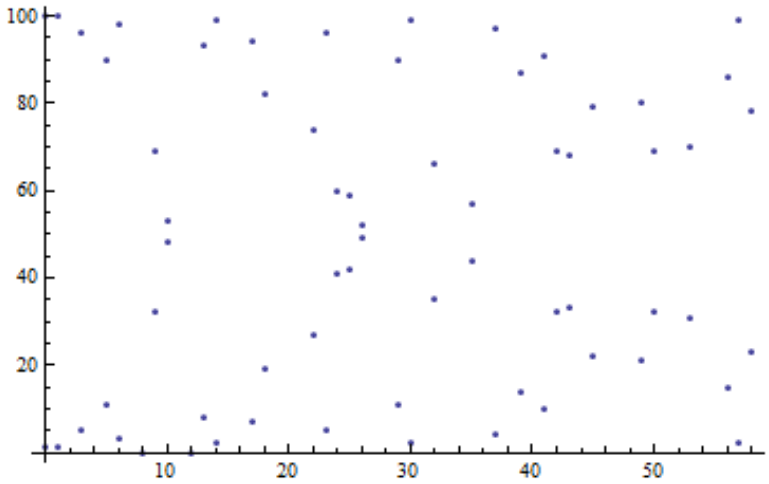
$y^2 = x^3 - x + 1$

Elliptic Curves in Finite Fields

$$y^3 \equiv x^2 + ax + b \pmod{p}$$



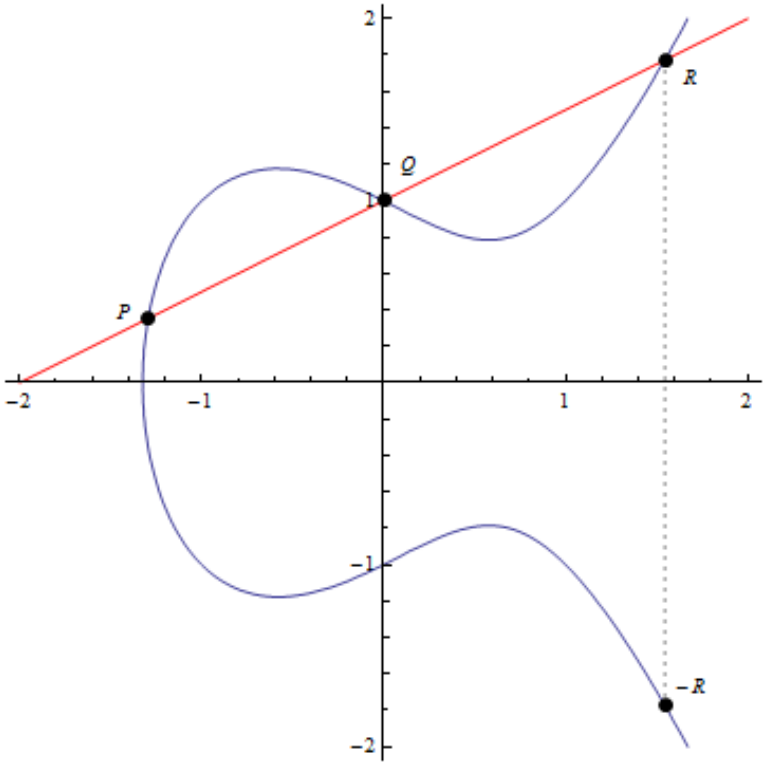
$y^2 = x^3 - x$



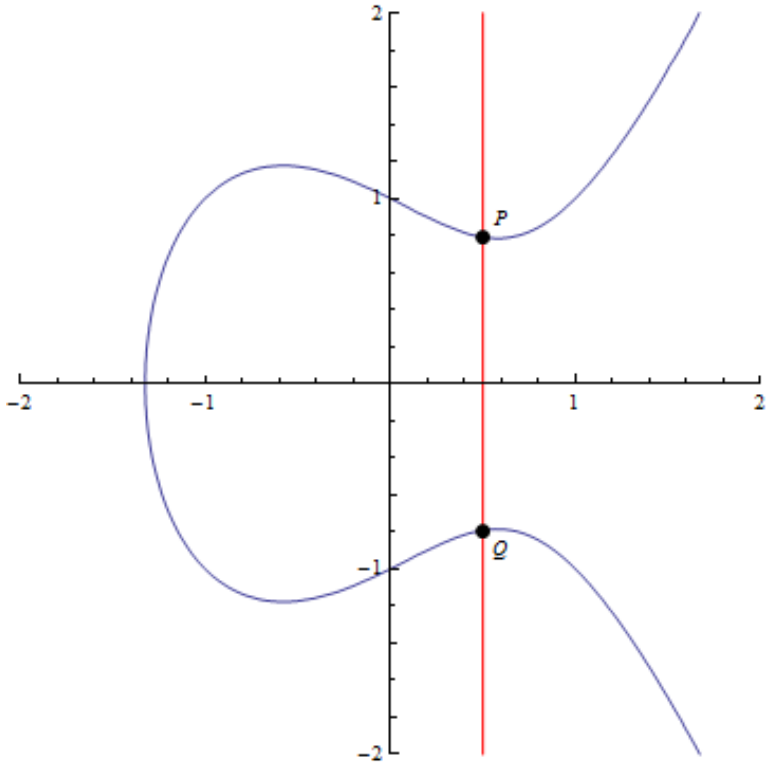
$y^2 = x^3 - x + 1$

Elliptic Curve Group Structure

- Set of all points on the curve plus infinity
  - Additive identity (0)
- Group operation defined by lines intersecting curve

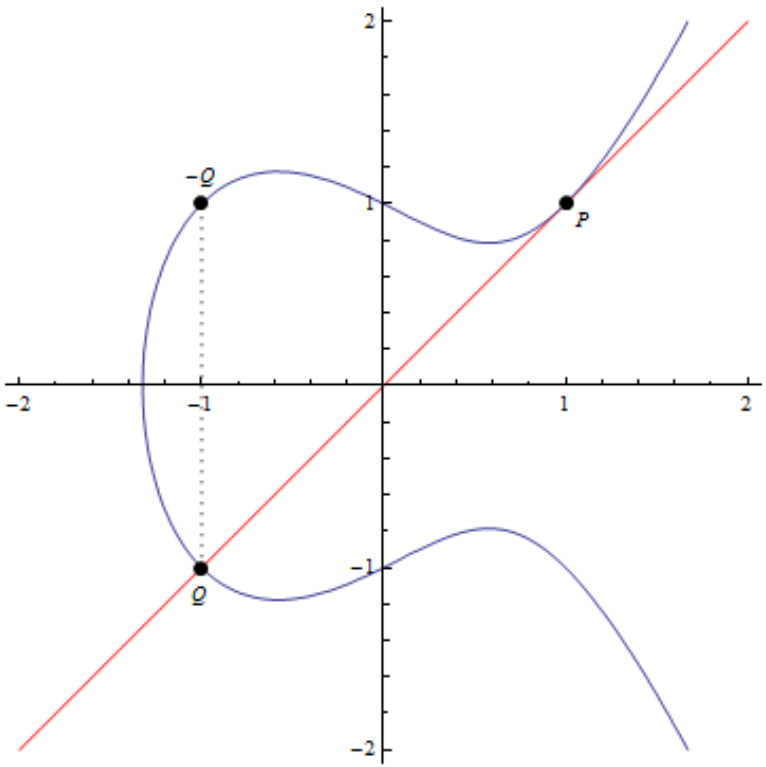


$$P + Q + R = 0$$
$$P + Q = -R$$

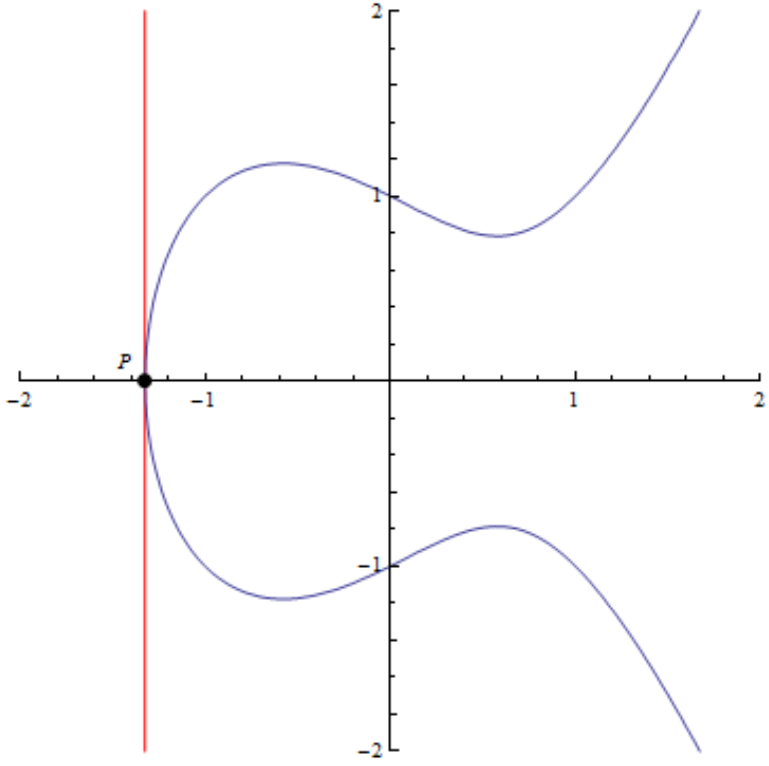


$$P + Q + 0 = 0$$
$$P + Q = 0$$

Elliptic Curve Group Operation



$$P + P + Q = 0$$
$$2P = P + P = -Q$$



$$P + P + 0 = 0$$
$$2P = P + P = 0$$

Elliptic Curve Diffie-Hellman

- Alice and Bob agree on public parameters:
  - Define elliptic curve p, a, b: $y^2 \equiv x^3 + ax + b \pmod{p}$
  - Point on curve G
- Alice picks private integer d_A with $0 \leq d_a < p$.
  - Alice sends Bob $Q_A = d_A G$.
- Similarly, Bob picks d_B and sends Alice $Q_B = d_B G$.
- Alice and Bob compute $(x_k, y_k) = d_A Q_B = d_B Q_A$.
  - Shared secret is x_k.

Transport Layer Security (TLS)

Symmetric Cryptography

- Relatively fast
- Requires shared secret

Asymmetric Cryptography

- Does not require shared secret
- Can authenticate digital signatures
- Typically requires larger keys for same security
- Relatively slow

- Authenticate certificates (Asymmetric)
- Establish shared secret (Asymetric)
- Conduct session communication in secret (Symmetric)