Classic Ciphers I

Lectore 02

Affine, Quadratic, Cubic, and Polynomial Ciphers

Lectore 02

Affine Cipher

Recall: Shift cipher with shift s:

1. Encrypt via $x \to x + s \pmod{26}$.
2. Decrypt via $x \to x - s \pmod{26}$.

We replace $x + s$ with more elaborate functions

Definition: The Affine cipher with a, b:

1. Encrypt via $x \to ax + b \pmod{26}$.
2. Decrypt via $x \to a^{-1}(x - b) \pmod{26}$

Affine Cipher

Recall: Shift cipher with shift s:

1. Encrypt via $x \to x + s \pmod{26}$.
2. Decrypt via $x \to x - s \pmod{26}$.

We replace $x + s$ with more elaborate functions

Definition: The Affine cipher with a, b:

1. Encrypt via $x \to ax + b \pmod{26}$.
2. Decrypt via $x \to a^{-1}(x - b) \pmod{26}$

Does this work? Vote YES or NO or OTHER

Affine Cipher

Recall: Shift cipher with shift s:

1. Encrypt via $x \to x + s \pmod{26}$.
2. Decrypt via $x \to x - s \pmod{26}$.

We replace $x + s$ with more elaborate functions

Definition: The Affine cipher with a, b:

1. Encrypt via $x \to ax + b \pmod{26}$.
2. Decrypt via $x \to a^{-1}(x - b) \pmod{26}$

Does this work? Vote YES or NO or OTHER Answer: OTHER

Affine Cipher

Recall: Shift cipher with shift s:

1. Encrypt via $x \to x + s \pmod{26}$.
2. Decrypt via $x \to x - s \pmod{26}$.

We replace $x + s$ with more elaborate functions

Definition: The Affine cipher with a, b:

1. Encrypt via $x \to ax + b \pmod{26}$.
2. Decrypt via $x \to a^{-1}(x - b) \pmod{26}$

Does this work? Vote YES or NO or OTHER Answer: OTHER

$2x + 1$ does not work: 0 and 13 both map to 1.

Affine Cipher

Recall: Shift cipher with shift s:

1. Encrypt via $x \to x + s \pmod{26}$.
2. Decrypt via $x \to x - s \pmod{26}$.

We replace $x + s$ with more elaborate functions

Definition: The Affine cipher with a, b:

1. Encrypt via $x \to ax + b \pmod{26}$.
2. Decrypt via $x \to a^{-1}(x - b) \pmod{26}$

Does this work? Vote YES or NO or OTHER Answer: OTHER

$2x + 1$ does not work: 0 and 13 both map to 1.

Need the map to be a bijection so it will have a unique inverse.

Affine Cipher

Recall: Shift cipher with shift s:

1. Encrypt via $x \to x + s \pmod{26}$.
2. Decrypt via $x \to x - s \pmod{26}$.

We replace $x + s$ with more elaborate functions

Definition: The Affine cipher with a, b:

1. Encrypt via $x \to ax + b \pmod{26}$.
2. Decrypt via $x \to a^{-1}(x - b) \pmod{26}$

Does this work? Vote YES or NO or OTHER Answer: OTHER
$2x + 1$ does not work: 0 and 13 both map to 1.
Need the map to be a bijection so it will have a unique inverse.

Condition on a, b so that $x \to ax + b$ is a bij: a rel prime to 26.
Condition on a, b so that a has an inv mod 26: a rel prime to 26.

Shift vs Affine

Shift: Key space is size 26

Affine: Key space is
$|\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}| \times 26 = 12 \times 26 = 312$

In an Earlier Era Affine would be harder to crack than Shift.

Shift vs Affine

Shift: Key space is size 26

Affine: Key space is
$|\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}| \times 26 = 12 \times 26 = 312$

In an Earlier Era Affine would be harder to crack than Shift.

Today They are both easy to crack.

Both Need: The Is English algorithm. Reading through 312 transcripts to see which one looks like English would take A LOT of time!

The Quadratic Cipher

Definition: The Quadratic cipher with a, b, c:

1. Encrypt via $x \to ax^2 + bx + c \pmod{26}$.

The Quadratic Cipher

Definition: The Quadratic cipher with a, b, c:

1. Encrypt via $x \to ax^2 + bx + c \pmod{26}$.

Does this work? Vote YES or NO

The Quadratic Cipher

Definition: The Quadratic cipher with a, b, c:

1. Encrypt via $x \to ax^2 + bx + c \pmod{26}$.

Does this work? Vote YES or NO Answer: NO

The Quadratic Cipher

Definition: The Quadratic cipher with a, b, c:

1. Encrypt via $x \to ax^2 + bx + c \pmod{26}$.

Does this work? Vote YES or NO Answer: NO

1. No easy test for Invertibility (depends on def of easy).
2. It turns out that every quadratic function mod 26 is an affine function.

The Polynomial Cipher

Definition: Poly Cipher with poly p (coefficients in $\{0, \ldots, 25\}$.

1. Encrypt via $x \to p(x) \pmod{26}$.
2. Decrypt via $x \to p^{-1}(x) \pmod{26}$.

Given a polynomial over mod 26 (or any mod) does it have an inverse? What is the complexity of this problem?
Vote: P, NP-complete, unknown to science.

The Polynomial Cipher

Definition: Poly Cipher with poly p (coefficients in $\{0, \ldots, 25\}$.

1. Encrypt via $x \to p(x) \pmod{26}$.
2. Decrypt via $x \to p^{-1}(x) \pmod{26}$.

Given a polynomial over mod 26 (or any mod) does it have an inverse? What is the complexity of this problem?
Vote: P, NP-complete, unknown to science.
Unknown to Science but if over mod a prime then in P.

The Polynomial Cipher

Definition: Poly Cipher with poly p (coefficients in $\{0, \ldots, 25\}$.

1. Encrypt via $x \to p(x) \pmod{26}$.
2. Decrypt via $x \to p^{-1}(x) \pmod{26}$.

Given a polynomial over mod 26 (or any mod) does it have an inverse? What is the complexity of this problem?
Vote: P, NP-complete, unknown to science.
Unknown to Science but if over mod a prime then in P.

Course website, Notes, has pointer to blog of mine on this. Some of the comments have theorems and pointers to the literature.

The Polynomial Cipher

Definition: Poly Cipher with poly p (coefficients in $\{0, \ldots, 25\}$.

1. Encrypt via $x \to p(x) \pmod{26}$.
2. Decrypt via $x \to p^{-1}(x) \pmod{26}$.

Given a polynomial over mod 26 (or any mod) does it have an inverse? What is the complexity of this problem?
Vote: P, NP-complete, unknown to science.
Unknown to Science but if over mod a prime then in P.

Course website, Notes, has pointer to blog of mine on this. Some of the comments have theorems and pointers to the literature.

The first place The Polynomial Cipher appeared was

The Polynomial Cipher

Definition: Poly Cipher with poly p (coefficients in $\{0, \ldots, 25\}$.

1. Encrypt via $x \to p(x) \pmod{26}$.
2. Decrypt via $x \to p^{-1}(x) \pmod{26}$.

Given a polynomial over mod 26 (or any mod) does it have an inverse? What is the complexity of this problem?
Vote: P, NP-complete, unknown to science.
Unknown to Science but if over mod a prime then in P.

Course website, Notes, has pointer to blog of mine on this. Some of the comments have theorems and pointers to the literature.

The first place The Polynomial Cipher appeared was

my 3-week summer course on crypto for High School Students.

So, as the kids say, its not a thing.

General Substitution Cipher

Shift and Affine were good for Alice and Bob since

1. Easy to encrypt, Easy to decrypt
2. Short Key: Roughly 5 bits for Shift, 10 bits for Affine.

Definition: Gen Sub Cipher with perm f on $\{0, \ldots, 25\}$.

1. Encrypt via $x \to f(x)$.
2. Decrypt via $x \to f^{-1}(x)$

1. Key is now permutation, roughly 125 bits.
2. Encrypt and Decrypt slightly harder

General Substitution Cipher

Shift and Affine were good for Alice and Bob since

1. Easy to encrypt, Easy to decrypt
2. Short Key: Roughly 5 bits for Shift, 10 bits for Affine.

Definition: Gen Sub Cipher with perm f on $\{0, \ldots, 25\}$.

1. Encrypt via $x \to f(x)$.
2. Decrypt via $x \to f^{-1}(x)$

1. Key is now permutation, roughly 125 bits.
2. Encrypt and Decrypt slightly harder

Uncrackable! Eve has to go through all 26! possibilities!!

General Substitution Cipher

Shift and Affine were good for Alice and Bob since

1. Easy to encrypt, Easy to decrypt
2. Short Key: Roughly 5 bits for Shift, 10 bits for Affine.

Definition: Gen Sub Cipher with perm f on $\{0, \ldots, 25\}$.

1. Encrypt via $x \to f(x)$.
2. Decrypt via $x \to f^{-1}(x)$

1. Key is now permutation, roughly 125 bits.
2. Encrypt and Decrypt slightly harder

Uncrackable! Eve has to go through all 26! possibilities!!

NOT EVEN CLOSE! Eve can use Freq Analysis

Freq Analysis

Alice sends Bob a LONG text encrypted by Gen Sub Cipher.
Eve finds freq of letters, pairs, triples, ...

Text in English.

1. Can use known freq: *e* is most common letter, *th* is most common pair.
2. If Alice is telling Bob about Mid East Politics than may need to adjust: *q* is more common (Iraq, Qatar) and some words more common.

The Vigenére Cipher

Lectore 02

The Vigenère cipher

EDUCATION NOTE: In class we started but did not finish Vig Cipher. I include everything on Vig Cipher in both this set of slides and the next.

The Vigenère cipher

Key: A word or phrase. Example: *dog* = *(3,14,6)*.
Easy to remember and transmit.
Example using *dog*.
Shift 1st letter by 3
Shift 2nd letter by 14
Shift 3nd letter by 6
Shift 4th letter by 3
Shift 5th letter by 14
Shift 6th letter by 6, etc.

Jacob Prinz is a Physics Major
jacob prinz isaph ysics major

encrypts to

MOIRP VUWTC WYDDN BGOFG SDXUU

The Vigenère cipher

Key: $k = (k_1, k_2, \ldots, k_n)$.
Encrypt (all arithmetic is mod 26)

$$Enc(m_1, m_2, \ldots, m_N) =$$

$$m_1 + k_1, m_2 + k_2, \ldots, m_n + k_n,$$

$$m_{n+1} + k_1, m_{n+2} + k_2, \ldots, m_{n+n} + k_n,$$

$$\ldots$$

Decrypt Decryption just reverse the process

The Vigenère cipher

- Size of key space?
  - If keys are 14-char then key space size $26^{14} \approx 2^{66}$
  - If variable length keys, even more.
  - Brute-force search infeasible
- Is the Vigenère cipher secure?
- Believed secure for many years...
- Might not have even been secure then...

Cracking Vig cipher: Step One-find Keylength

Assume T is a text encoded by Vig, key length L unknown.
For $0 \leq i \leq L-1$, letters in pos $\equiv i \pmod{26}$ – same shift.
Look for a sequence of (say) 3-letters to appear (say) 4 times.

Example: aiq appears in the
57-58-59th slot, 87-88-89th slot 102-103-104th slot
162-163-164th slot

Important: Very likely that aiq encrypted the same 3-letter sequence and hence the length of the key is a divisor of
87-57=30 102-87=15 162-102=60
The only possible L's are 1,3,5,15.

Good Enough: We got the key length down to a small finite set.

Important Point about letter Freq

Assume (and its roughly true): In an English text of length N:

e occurs $\sim 13\%$ t occurs $\sim 9\%$ a occurs $\sim 8\%$

Etc- other letters have frequencies that are true for all texts.

Important Point about letter Freq

Assume (and its roughly true): In an English text of length N:

e occurs $\sim 13\%$ t occurs $\sim 9\%$ a occurs $\sim 8\%$

Etc- other letters have frequencies that are true for all texts.

Assume (and its roughly true): In an English text of length N, if $i \ll N$, then if you take every ith letter of T:

e occurs $\sim 13\%$ t occurs $\sim 9\%$ a occurs $\sim 8\%$

Etc- other letters same frequencies as normal texts.

Important Point about letter Freq

Assume (and its roughly true): In an English text of length N:

e occurs $\sim 13\%$ t occurs $\sim 9\%$ a occurs $\sim 8\%$

Etc- other letters have frequencies that are true for all texts.

Assume (and its roughly true): In an English text of length N, if $i \ll N$, then if you take every ith letter of T:

e occurs $\sim 13\%$ t occurs $\sim 9\%$ a occurs $\sim 8\%$

Etc- other letters same frequencies as normal texts.

Relevant to us:

$\vec{q}$ freq of every Lth letter: then $\sum_{i=1}^{26} q_i^2 \approx 0.065$.

$\vec{q}$ is NOT (we won't define that rigorously): $\sum_{i=1}^{26} q_i^2$ MUCH lower.

Cracking Vig cipher: Step One-find Keylength

Let K be the set of possible key lengths. K is small. For every $L \in K$:

- Form a stream of every Lth character.
- Find the frequencies of that stream: $\vec{q}$.
- Compute $Q = \sum q_i^2$
- If $Q \approx 0.065$ then YES L is key length.
- If Q much less than 0.065 then NO L is not key length.
- One of these two will happen
- Just to make sure, check another stream.

Note: Differs from Is English:

Is English wanted to know if the text was actually English

What we do above is see if the text has same dist of English, but okay if diff letters. E.g., if z is 13%, a is 9%, and other letters have roughly same numbers as English then we know the stream is SOME Shift. We later use Is English to see which shift.

A Note on Finding Keylength

We presented one method:

1. Find phrase of length x appearing y times. Differences D.
2. K is set of divisors of all $L \in D$. Correct keylength in K.
3. Test $L \in K$ for key length until find one that works.

Alternative just try all key lengths up to a certain length:

1. Let $K = \{1, \ldots, 100\}$ (I am assuming key length ≤ 100).
2. Test $L \in K$ for key length until find one that works.

Note: With modern computers use Method 2. In days of old eyeballing it made method 1 reasonable.

Cracking the Vig cipher: Step Two-Freq Anal

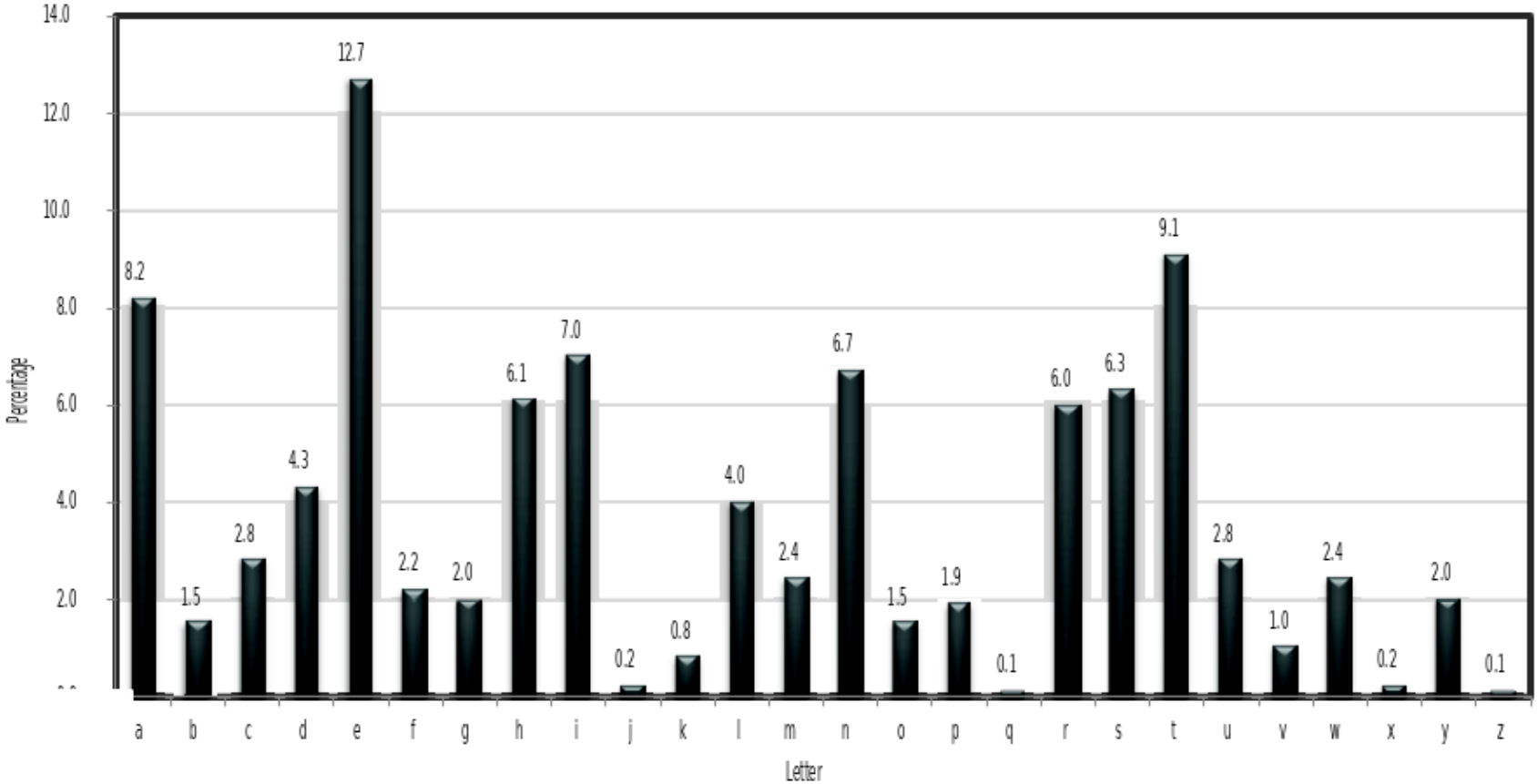
After Step One we have the key length L. Note:

- Every L^{th} character is "encrypted" using the same shift.
- Important: Letter Freq still hold if you look at every L 14th letter!

Step Two:

1. Separate text T into L streams depending on position mod L
2. For each steam try every shift and use Is English to determine which shift is correct.
3. You now know all shifts for all positions. Decrypt!

Using plaintext letter frequencies



Byte-wise Vigenère cipher

- The key is a string of bytes
- The plaintext is a string of bytes
- To encrypt, XOR each character in the plaintext with the next character of the key
  - Wrap around in the key as needed
- Decryption just reverses the process.

Note: Decryption and Encryption both use XOR with same key.
Note: Can be cracked as original Vig can be cracked.