CS557: Cryptography

Classical Ciphers-II

S. Tripathy
IIT Patna

Polyalphabetic Ciphers

Previous ciphers are monoalphabetic

Each alphabetic character mapped to a unique alphabetic character→ makes statistical analysis easier

Obvious idea: Polyalphabetic ciphers:

Encrypt multiple characters at a time

Poly alphabetic Cipher
Vigenère Cipher

Let m be a positive integer (the key length)

$K = Z_{26} \times \ldots \times Z_{26} = (Z_{26})^m$

For $k = (k_1, \ldots, k_m)$:

$e_k(x_1, \ldots, x_m) = (x_1 + k_1 \pmod{26}, \ldots, x_m + k_m \pmod{m})$

$d_k(y_1, \ldots, y_m) = (y_1 - k_1 \pmod{26}, \ldots, y_m - k_m \pmod{m})$

k = C R Y P T O C R Y P T O C R Y P T

m = W H A T A N I C E D A Y T O D A Y (+ mod 26)

---

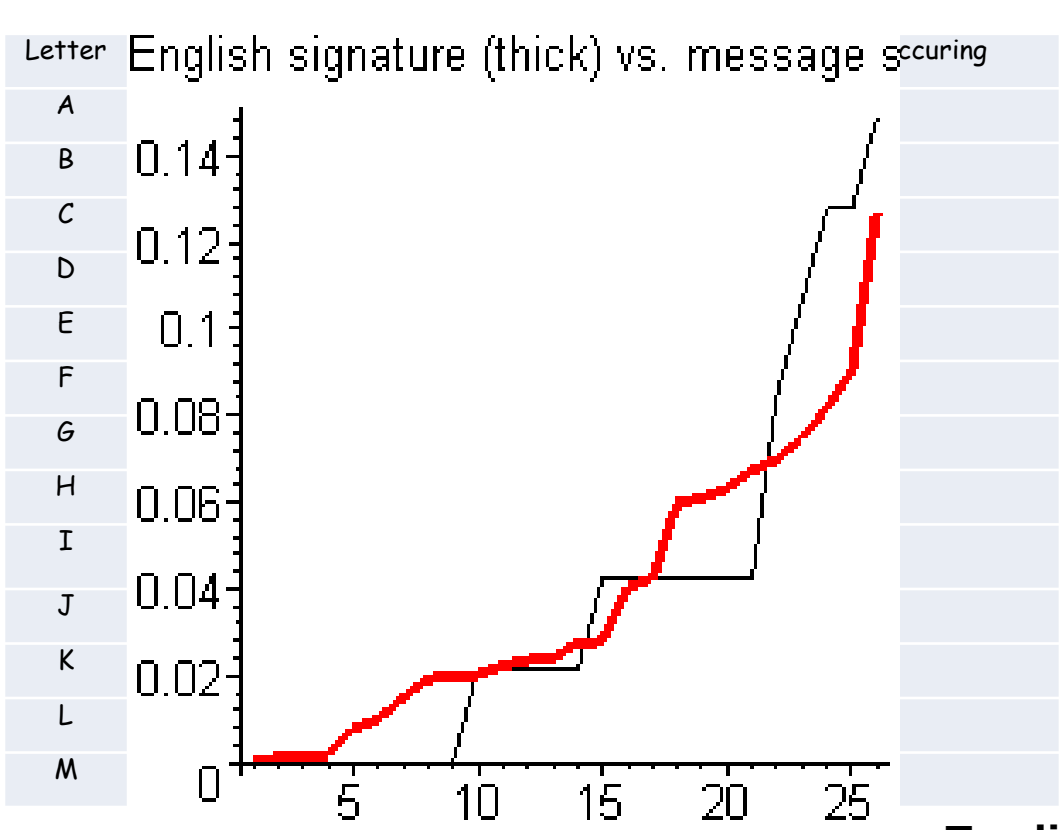
c = Z Z Z J U C L U D T U N W G C Q S

Security of Vigenere

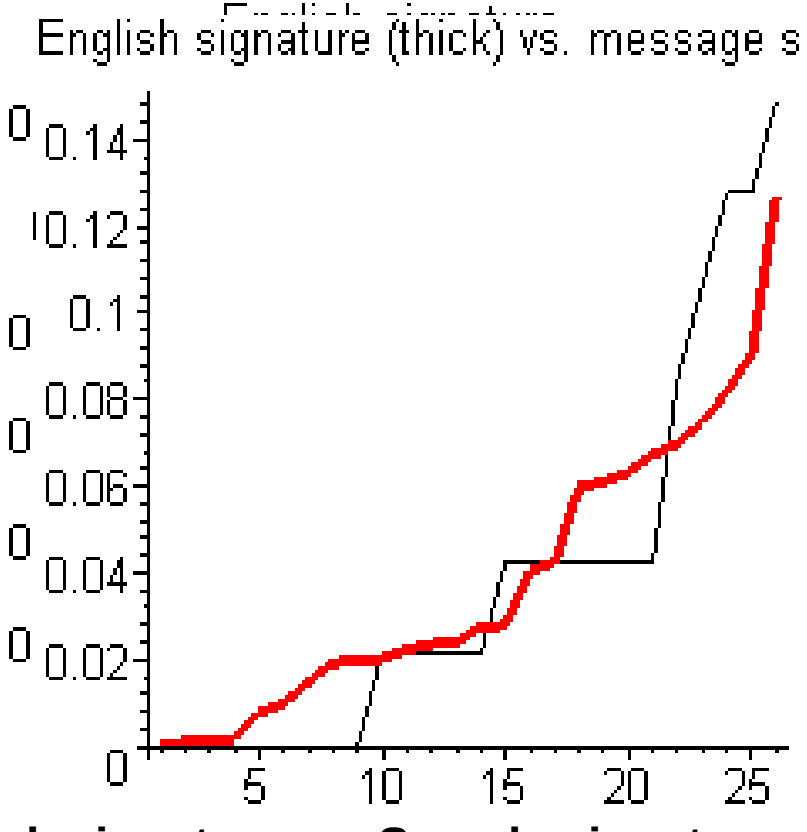
- Vigenere masks the frequency with which a character appears in a language:
  - one letter in the ciphertext corresponds to multiple letters in the plaintext.
  - Makes the use of frequency analysis more difficult.
- Any message encrypted by a Vigenere cipher is a collection of as many shift ciphers as there are letters in the key.

- Cryptanalysis
  - Find the length of the key.
  - Divide the message into that many shift cipher encryptions.
  - Use frequency analysis to solve the resulting shift ciphers
-

Standard English frequencies:



English signature vs. Sample signature for a ciphertext message

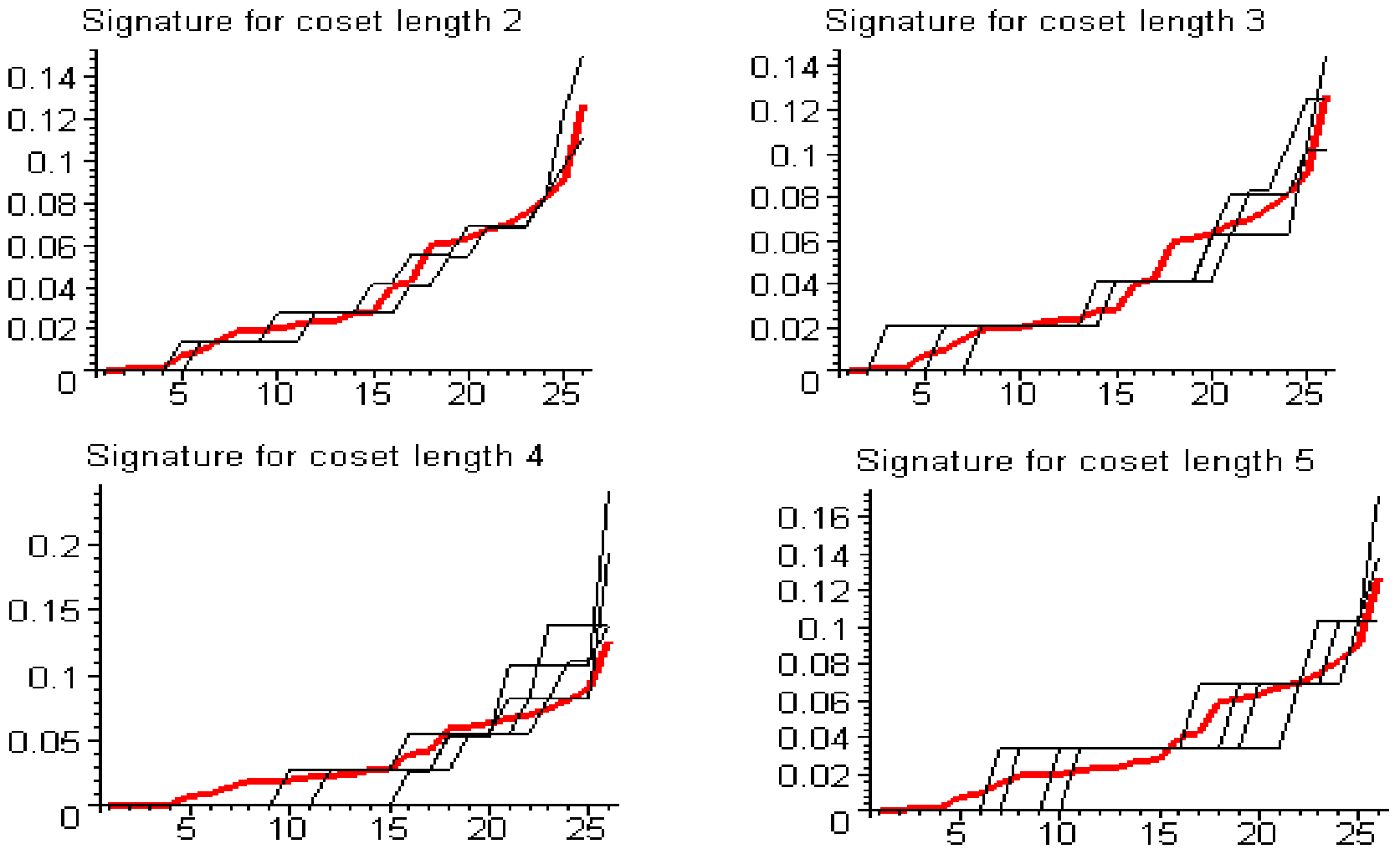


English signature vs. Sample signature for a plaintext mess

EX.: Let the Plain Text (Message)
"WE WANT TO LOOK AT THE SIGNATURE OF THE SAMPLE OF A MESSAGE".

Using the Affine cipher y= (11x+7) mod 26, “PZPHU IIFYF FNHII GZXRV UHITM ZFKIG ZXHJQ YZFKH JZXXH VZ"

Ex.: Let the ciphertext be "LPOFE MYFSO KVKIZ GWVJR VN BAQWV ZFLWS BJMLH DTEHF LKEKB GAVPU JKQMA SBAEW AGAVA IESER FUITO WCYRV BUQWB KEEQT RLPKX WGCBJ LRRFO ZUSVJ XWGCB JLAFW LOALP KIAOK AWZKP AXNRJ"



Comparison of English signatures with various possible coset (keyword) lengths.

Hill Cipher

A more complex form of polyalphabetic cipher

Again, let m be a positive integer

P =C= $(Z_{26})^m$

To encrypt: (case m=2)

Take linear combinations of plaintext (x_1, x_2)

E.g., $y_1 = 2x_1 + x_2 \pmod{26}$

$y_2 = 3x_1 + 4x_2 \pmod{26}$

Can be written as a matrix multiplication (mod 26)

Encryption

- Change message into 2×1 letter vectors
- Change each vector into 2×1 numeric vectors
- Multiply each numeric vector by encryption matrix
- Convert new vectors to letters (ciphertext)

Encryption

Message to encrypt = HELLO WORLD

$$\begin{bmatrix} H \\ E \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix} \quad \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 14+4 \\ 21+16 \end{bmatrix} = \begin{bmatrix} 18 \\ 37 \end{bmatrix} \text{ Mod } 26 = \begin{bmatrix} 18 \\ 11 \end{bmatrix} = \begin{bmatrix} S \\ L \end{bmatrix}$$

$$\begin{bmatrix} L \\ L \end{bmatrix} = \begin{bmatrix} 11 \\ 11 \end{bmatrix} \quad \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 11 \\ 11 \end{bmatrix} = \begin{bmatrix} 22+11 \\ 33+44 \end{bmatrix} \begin{bmatrix} 33 \\ 77 \end{bmatrix} \text{ Mod } 26 = \begin{bmatrix} 7 \\ 25 \end{bmatrix} = \begin{bmatrix} H \\ Z \end{bmatrix}$$

$$\begin{bmatrix} O \\ W \end{bmatrix} = \begin{bmatrix} 14 \\ 22 \end{bmatrix} \quad \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 14 \\ 22 \end{bmatrix} = \begin{bmatrix} 28+22 \\ 42+88 \end{bmatrix} = \begin{bmatrix} 50 \\ 130 \end{bmatrix} \text{ Mod } 26 = \begin{bmatrix} 24 \\ 0 \end{bmatrix} = \begin{bmatrix} Y \\ A \end{bmatrix}$$

$$\begin{bmatrix} O \\ R \end{bmatrix} = \begin{bmatrix} 14 \\ 17 \end{bmatrix} \quad \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 14 \\ 17 \end{bmatrix} = \begin{bmatrix} 28+17 \\ 42+68 \end{bmatrix} = \begin{bmatrix} 45 \\ 110 \end{bmatrix} \text{ Mod } 26 = \begin{bmatrix} 19 \\ 6 \end{bmatrix} = \begin{bmatrix} T \\ G \end{bmatrix}$$

$$\begin{bmatrix} L \\ D \end{bmatrix} = \begin{bmatrix} 11 \\ 3 \end{bmatrix} \quad \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \times \begin{bmatrix} 11 \\ 3 \end{bmatrix} = \begin{bmatrix} 22+3 \\ 33+12 \end{bmatrix} = \begin{bmatrix} 25 \\ 45 \end{bmatrix} \text{ Mod } 26 = \begin{bmatrix} 25 \\ 19 \end{bmatrix} = \begin{bmatrix} Z \\ T \end{bmatrix}$$

HELLO WORLD has been encrypted to SLHZY ATGZT

Decryption

- Change message into 2×1 letter vectors
- Change each vector into 2×1 numeric vectors
- Multiply each numeric vector by decryption matrix
- Convert new vectors to letters (original message)

Cryptanalysis of Hill Cipher

- Much harder to break with ciphertext only.
  - Easy with known plaintext
- Recall: want to find secret matrix K
- Assumptions: m is known

- Construct m distinct plaintext-ciphertext pairs
  - $(X_1, Y_1), \ldots, (X_m, Y_m)$
- Define matrix Y with rows $Y_1, \ldots, Y_m$
- Define matrix X with rows $X_1, \ldots, X_m$ Verify: $Y = X K$

Playfair Poly Alphabetic Cipher

- invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair

Playfair Key Matrix

- a 5X5 matrix of letters based on a keyword
- fill in letters of keyword and fill rest of matrix with other letters
- eg. using the keyword MONARCHY

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Encrypting and Decrypting

- plaintext encrypted two letters at a time:
  1. if a pair is a repeated letter, insert a filler like 'X', eg. "balloon" encrypts as "ba lx loxon"
  2. if both letters fall in the same row, replace each with letter to right (wrapping back to start from end), eg. "ar" encrypts as "RM"
  3. if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom), eg. "mu" encrypts to "CM"
  4. otherwise each letter is replaced by the one in its row in the column of the other letter of the pair, eg. "hs" encrypts to "BP", and "ea" to "IM" or "JM" (as desired)

Security of the Playfair Cipher

- security much improved over monoalphabetic since it is (26 x 26 =) 676 digrams instead of 26
- But attacker would use frequency table (676 entries) to analyse (verses 26 for a monoalphabetic) and correspondingly more ciphertext
- Widely used for many years (eg. US & British military in WW1)
- it can be broken, given a few hundred letters
- since still has much of plaintext structure

Transposition Ciphers

- Also called **permutation** ciphers.
- Shuffle the plaintext, without altering the actual letters used.
- Example: Row Transposition Ciphers

Row Transposition Ciphers

- Plaintext is written row by row in a rectangle.
- Ciphertext: write out the columns in an order specified by a key.
- **Ex:** attack postponed until two am

Key: 3 4 2 1 5 6 7

a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

Plaintext:

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Cryptography in the Computer Age

- Working with binary instead of letters
- We can do things many, many times
  - Think of an Enigma machine that has 2^{128} pairs of symbols on each rotor, and 20 rotors
- Other than that, the basic principles are the same as classical cryptography

Classical to Modern Cryptography

- Classical cryptography
  - Encryption/decryption done by hand
  - Working with letters/ Alphabets
- Modern cryptography
  - Computers to encrypt and decrypt
  - Working with binary instead of letters
  - Same principles, but automation allows ciphers to become much more complex

More Definitions

- computational security
  - given limited computing resources, the cipher cannot be broken
- unconditional security
  - no matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext

- Provable Security
  - Provide evidence of security by reducing the security of the cryptosystem into a well studied problem

- Thanks