Classical Cryptosystems

Debdeep Mukhopadhyay

Assistant Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
INDIA -721302

Objectives

- **Definitions**
- **Kerckhoffs Principle**
- **Monoalphabetic Ciphers: Shift Cipher**
- **Polyalphabetic Ciphers: Vigenere Cipher**
- **Affine Ciphers and the Euler Totient Function**
- **Permutation Cipher**

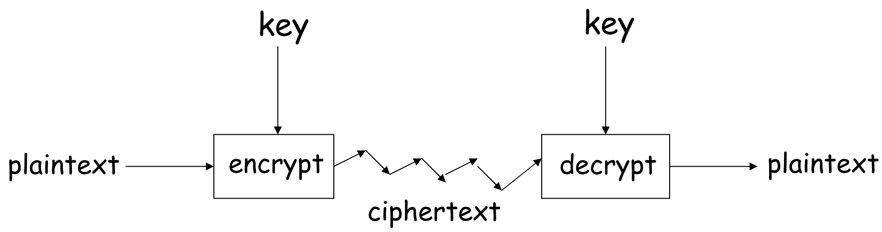
Definitions

- A *cipher* or *cryptosystem* is used to *encrypt* the *plaintext*
- The result of encryption is *ciphertext*
- We *decrypt* ciphertext to recover plaintext
- A *key* is used to configure a cryptosystem
- A *symmetric key* cryptosystem uses the same key to encrypt as to decrypt
- A *public key* cryptosystem uses a *public key* to encrypt and a *private key* to decrypt.

Kerckhoffs Principle

- Basis assumption
  - The system is completely known to the attacker
  - Only the key is secret
- Also known as Kerckhoffs Principle
  - Crypto algorithms are not secret
- Why do we make this assumption?
  - Experience has shown that secret algorithms are weak when exposed
  - Secret algorithms never remain secret
  - Better to find weaknesses beforehand

Cryptographic Communication



A generic use of crypto

Cryptosystem

A cryptosystem **is a five-tuple ($\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D}$), where the following are satisfied:**

1. **$\mathcal{P}$ is a finite set of possible** plaintexts
2. **$\mathcal{C}$ is a finite set of possible** ciphertexts
3. **$\mathcal{K}$, the** keyspace**, is a finite set of possible** keys
4. **$\forall K \in \mathcal{K}$, $\exists e_K \in \mathcal{E}$ (encryption rule), $\exists d_K \in \mathcal{D}$ (decryption rule).**
   Each $e_K: \mathcal{P} \rightarrow \mathcal{C}$ and $d_K: \mathcal{C} \rightarrow \mathcal{P}$ are functions such that $\forall x \in \mathcal{P}$, $d_K(e_K(x)) = x$.

Encryption Function is Injective

- **$y=e_K(x)$: Denotes the encryption transformation.**
- **if $y=e_K(x1) = e_K(x2)$, then Bob does not know whether y has come from x1 or x2.**
- **If the Plaintext set and ciphertext set are same, then the encryption function is just a permutation.**

Classical Cryptography

- **Monoalphabetic Ciphers**
  Once a key is chosen, each alphabetic character of a plaintext is mapped onto a *unique* alphabetic character of a ciphertext.
  - **The Shift Cipher (Caesar Cipher)**
  - **The Substitution Cipher**
  - **The Affine Cipher**

Classical Cryptography

- **Polyalphabetic Ciphers**
  Each alphabetic character of a plaintext can be mapped onto *m* alphabetic characters of a ciphertext. Usually *m* is related to the encryption key.
  - **The Vigenère Cipher**
  - **The Hill Cipher**
  - **The Permutation Cipher**

Shift cipher

- **Consider,**
  - **$P=C=K=Z_{26}$.**
  - **For $0 \le K \le 25$, define**
    - » $e_K(x)=x+K \bmod 26$
    - » $d_k(x) = y-K \bmod 26$
  - $(x,y \in Z_{26})$
    - **It is easy to see that, $x=d_K(e_k(x))$.**

Simple Substitution

- **Plaintext: fourscoreandsevenyearsago**

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- **Ciphertext: IRXUVFRUHDAGVHYHABHDUVDIR**
- **Shift by 3 is "Caesar's cipher"**

Note that the use of smaller letter for plaintext and capital letters for ciphertext is only to improve readibility

Ceasar's Cipher Decryption

- **Suppose we know a Ceasar's cipher is being used**
- **Ciphertext: VSRQJHEREVTXDUHSDQWU**

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- **Plaintext: spongebobsquarepants**

Not-so-Simple Substitution

- **Shift by n for some n ∈ {0,1,2,…,25}**
- **Then key is n**
- **Example: key = 7**

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

Properties required of the encryption

- **Each of encryption and decryption function should be easily computable.**
- **An opponent, on seeing a ciphertext string y, should be unable to determine the key K, that was used, or the plaintext string x.**
- **"Cryptanalysis" is the process of attempting to know the key from given information.**

Cryptanalysis: Try all possibilities

- **Ciphertext: JBCRCLQRWCRVNBJENBWRWN**
- **Try all the 26 possible keys (Exhaustive or brute force search)**
- **jbcrclqrwcrvnbjenbwrwn**

iabqbkpqvbqumaidmavqvm

hzapajopuaptlzhclzupul

…

astitchintimessavesnine: key = 9

Substitution Cipher

- **Key is some permutation of letters**
- **Need not be a shift**
- **For example**

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	J	I	C	A	X	S	E	Y	V	D	K	W	B	Q	T	Z	R	H	F	M	P	N	U	L	G	O

- **Then 26! ≈ 4 x 10^{26} > 2^{88} possible keys!**

But still the cipher can be attacked quite easily.

The Affine Cipher

Let $\mathcal{P} = \mathcal{C} = Z_{26}$, let

$\mathcal{K} = \{(a, b) \in Z_{26} \times Z_{26} \mid \gcd(a, 26) = 1\}$.

$\forall x \in \mathcal{P}$, $\forall y \in \mathcal{C}$, $\forall K \in \mathcal{K}$, define

$$e_K(x) = ax + b \pmod{26}$$

and

$$d_K(y) = a^{-1}(y - b) \pmod{26}.$$

The encryption is injective if and only if gcd(a,26)=1

Multiplicative Inverse of an Element

- **Suppose a is an element from Z_m. Then the multiplicative inverse of an element is an element b also in Z_m, such that ab=1 (mod m).**
  - **Then, gcd(a,m)=1**
- **Note that if m=prime number, p then every element has an inverse. Then Z_p is called a field.**

Inverse of Affine Cipher

- **Affine Cipher is invertible if a has a multiplicative inverse.**
  - **That is gcd(a,m)=1**
  - **{1,3,5,7,9,11,15,17,19,21,23,25} have elements which are co-prime to m**
  - **Thus, $1^{-1}=1$, $3^{-1}=9$, $5^{-1}=21$, $7^{-1}=15$, $11^{-1}=19$, $15^{-1}=7$, $17^{-1}=23$, $25^{-1}=25$**
  - **Thus, the inverse of an element belongs to the above set. Why?**

Key Size of Affine Cipher

- **The possible values of a such that gcd(a,26)=1 are:**

  {1,3,5,7,9,11,15,17,19,21,23,25}

  Thus, there are 12 possible a's

  The coefficient b can be any 26 value: Total key size is 12 x 26 = 312

  Key size is thus too small…can we generalize the affine cipher?

Generalized Affine Cipher

- **Euler's Totient function : Suppose a≥1 and m≥2 are integers. If gcd(a,m)=1, then we say that a and m are relatively prime.**
- **The number of integers in Z_m (m>1), that are relatively prime to m and** does not exceed m **is denoted by Φ(m), called Euler's Totient function or phi function.**

Example

- **m=26 => Φ(26)=12**
- **If p is prime, Φ(p)=p-1**
- **If n=1,2,…,24 the values of Φ(n) are:**
  - **1,1,2,2,4,2,6,4,6,4,10,4,12,6,8,8,16,6,18,8, 12,10,22,8**
  - **Thus we see that the function is very irregular.**

Properties of Φ

- **If m and n are relatively prime numbers,**
  - **$\Phi(mn)= \Phi(m)\, \Phi(n)$**
- **$\Phi(77)= \Phi(7 \times 11)=6 \times 10 = 60$**
- **$\Phi(1896)= \Phi(3 \times 8 \times 79)=2 \times 4 \times 78 =624$**
- **This result can be extended to more than two arguments comprising of pairwise coprime integers.**

An Important Result

- **If m and n are relatively prime, $\Phi(mn)=\Phi(m)\Phi(n)$**

1	**2**	**…**	**k**	**…**	**n**
n+1	**n+2**	**…**	**n+k**	**…**	**n+n**
…					
(m-1)n+1	**(m-1)n+2**	**…**	**(m-1)n+k**	**…**	**(m-1)n+n**

there are Φ(m) elements which are co-prime to m

there are Φ(n) columns in which all the elements are co-prime to n.

contd.

- Thus, there are Φ(n) columns with Φ(m) elements in each which are co-prime to both m and n.
- Thus there are Φ(m) Φ(n) elements which are co-prime to mn.
  - This proves the result…

Further Result

- $\Phi(p^a)=p^a-p^{a-1}$
  - Evident for a=1
  - For a>1, out of the elements 1, 2, …, p^a the elements p, p^2, $p^{a-1}p$ are not co-prime to p^a.

  Rest are co-prime.

  Thus $\Phi(p^a)=p^a-p^{a-1}$

  $=p^a(1-1/p)$

contd.

- $n = p_1^{a1} p_2^{a2} \ldots p_k^{ak}$
- Thus, $\Phi(n) = \Phi(p_1^{a1})\, \Phi(p_2^{a2}) \ldots \Phi(p_k^{ak})$
  $= n(1-1/p_1)(1-1/p_2)\ldots(1-1/p_k)$

Thus, if m=60=4x3x5

$\Phi(60)=60(1-1/2)(1-1/3)(1-1/5)=16$

Hence, no of Affine keys = 16 x 60 = 960.

Monoalphabetic Ciphers

- Once a key is chosen, each alphabetic character is mapped to a unique alphabetic character in the ciphertext.
  - Example: Shift and Substitution Cipher

Polyalphabetic Ciphers

- **In such ciphers, a plaintext can be mapped into more than one possible characters in ciphertexts.**
- **They are harder to cryptanalyze.**
- **Example: Vigenere, Hill Cipher**

Vigenere Cipher

- **Vigenere cipher is a kind of polyalphabetic cipher:**
  - **Each key consists of *m* characters, called *keyword*.**
  - **Encrypt *m* characters at a time**
  - **Devised by Blaise de Vigenere in the sixteen century.**

Example

- thiscryptosystemisnotsecure

- **Let m=6 and key=(2,8,15,7,4,17)**
- **Convert the plaintext into residues modulo 26.**
- **Write them in groups of 6, and then add the keyword**

Example

19	**7**	**8**	**18**	**2**	**17**	**24**	**15**	19	**14**	**18**	**24**
2	**8**	**15**	**7**	**4**	**17**	**2**	**8**	**15**	**7**	**4**	**17**
21	**15**	**23**	**25**	**6**	**8**	**0**	**23**	8	**21**	**22**	**15**

So, this part of the ciphertext is : VPXZGIAXIVWP

Note that character ‘t’ is mapped to ‘V’ and ‘I’. Thus, polyalphabetic.

Vigenere cipher—key size

What is the key space? Suppose the keyword length is *m*.

There are total 26^m possible keys.

Suppose m=5, then $26^5 = 1.1 \times 10^7$, which is large enough to preclude *exhaustive key search* by hand.

However, we will see that there will be a systemic method to break Vigenere cipher.

We see that one character could be mapped into *m* different characters when the character is in *m* different positions.

Hill cipher -- introduction

- **Another polyalphabetic cipher.**
- **Invented in 1929 by Lester S. Hill.**
- **Let *m* be an positive integer, and let $\mathcal{P} = \mathcal{C}$ $(\mathcal{Z}_{26})^m$**
- **First divide the characters in plaintext into blocks of *m* characters, take *m* linear combinations of the *m* characters, thus producing the *m* characters in ciphertext.**

Hill cipher -- example

Suppose m=2, a plaintext element is written as $x=(x_1,x_2)$ and a ciphertext element as $y=(y_1,y_2)$. Here y_1 would be a linear combination of x_1 and x_2, as would y_2.

Suppose we take:

$y_1=(11x_1 + 3x_2) \bmod 26$

$y_2=(8x_1 + 7x_2) \bmod 26$

then y_1 and y_2 can be computed from x_1 and x_2

We can write the above computations in matrix notation:

$$(y_1, y_2) = (x_1, x_2) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

or $\boldsymbol{y = xK}$ where $\boldsymbol{y}=(y_1, y_2)$, $\boldsymbol{x}=(x_1, x_2)$, and $\boldsymbol{K}=\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$

Assume all operations are performed by modulo 26.

Hill cipher – theoretical foundation

- **Given plaintext x, we get ciphertext $y = xK$**
- **If given ciphertext y, we should get plaintext x by yK^{-1}**

Thus, for Hill cipher to work, the matrix K must have an *inverse* K^{-1}.

From linear algebra, suppose I_m is an identity matrix, K is $m \times m$ matrix, Then $KK^{-1}=I_m$. So, $yK^{-1}=xKK^{-1}=xI_m=x$.

Hill cipher – example

Suppose key is:

$K=\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$ then $K^{-1}=\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$

Check that K and K^{-1} are indeed inverses.

Hill cipher – algebra foundation

1. Determinant of a matrix *A*, denoted by *det A* :
   -- if $A(a_{ij})$ is 2×2, then $\det A = a_{11}a_{22} - a_{12}a_{21}$
   -- if $A(a_{ij})$ is 3×3, then $\det A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}$

2. Theorem: suppose $K=\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$ with $k_{ij} \in \mathcal{Z}_{26}$

Then *K* has an inverse if and only if *det K* is invertible in $\mathcal{Z}_{26}$

if and only if gcd(*det K*, 26)=1

Moreover,

$K^{-1}=(\det K)^{-1}\begin{pmatrix} k_{22} & -k_{12} \\ -k_{21} & k_{11} \end{pmatrix}$ Where $\det K = k_{11}k_{22} - k_{12}k_{21}$

Hill cipher – formal definition

- **Let $m \geq 2$, be a positive integer. Let $\mathcal{P} = \mathcal{C} = (\mathcal{Z}_{26})^m$ and let**
  $\mathcal{K} = \{m \times m$ invertible matrices over $\mathcal{Z}_{26}\}$

For each key K, define:

$$e_K(x) = xK \text{ and } d_K(y) = yK^{-1}$$

where all operations are performed in $\mathcal{Z}_{26}$.

Permutation cipher--introduction

- **All previous ciphers include substitutions: plaintext characters are replaced by different ciphertext characters.**
- **The permutation cipher will keep the plaintext characters unchanged, but alter their position by rearranging them using a permutation.**
- **Suppose X is a finite set,**
  a permutation over X is a *bijective function* $\pi: X \to X$. thus the inverse permutation $\pi^{-1}: X \to X$ is defined by the rule:
  $\pi^{-1}(x) = x'$ **if and only if** $\pi(x') = x$

Permutation cipher—formal definition

- Let m be a positive integer, Let $\mathcal{P} = \mathcal{C} = (\mathcal{Z}_{26})^m$ and let $\mathcal{K}$ consists of all permutations of {1,2,…, m}. For a key (i.e., a permutation) π

Define

$$e_\pi(x_1,\ldots,x_m) = (x_{\pi(1)},\ldots, x_{\pi(m)})$$

and

$$d_\pi(y_1,\ldots,y_m) = (y_{\pi^{-1}(1)},\ldots, y_{\pi^{-1}(m)})$$

where π^{-1} is the inverse permutation of π.

Permutation cipher—example

- **Suppose m=6.**

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

Then

x	1	2	3	4	5	6
$\pi^{-1}(x)$	3	6	1	5	2	4

Given plaintext: shesellsseashellsbytheseashore

first split by m=6: shesel lsseas hellsb ythese ashore

Get ciphertext by π: ELSEHS…

Comments: ***the permutation cipher is a special case of Hill cipher.***

Points to Ponder

- **Comment on whether the Euler Totient Function for n>1 is even or odd?**
- **Express permutation cipher as a Hill cipher.**

References

- **B. A. Forouzan, *“Cryptography and Network Security”,* TMH**

Next Days Topic

- **Cryptanalysis of Classical Ciphers**