Classical Cryptography

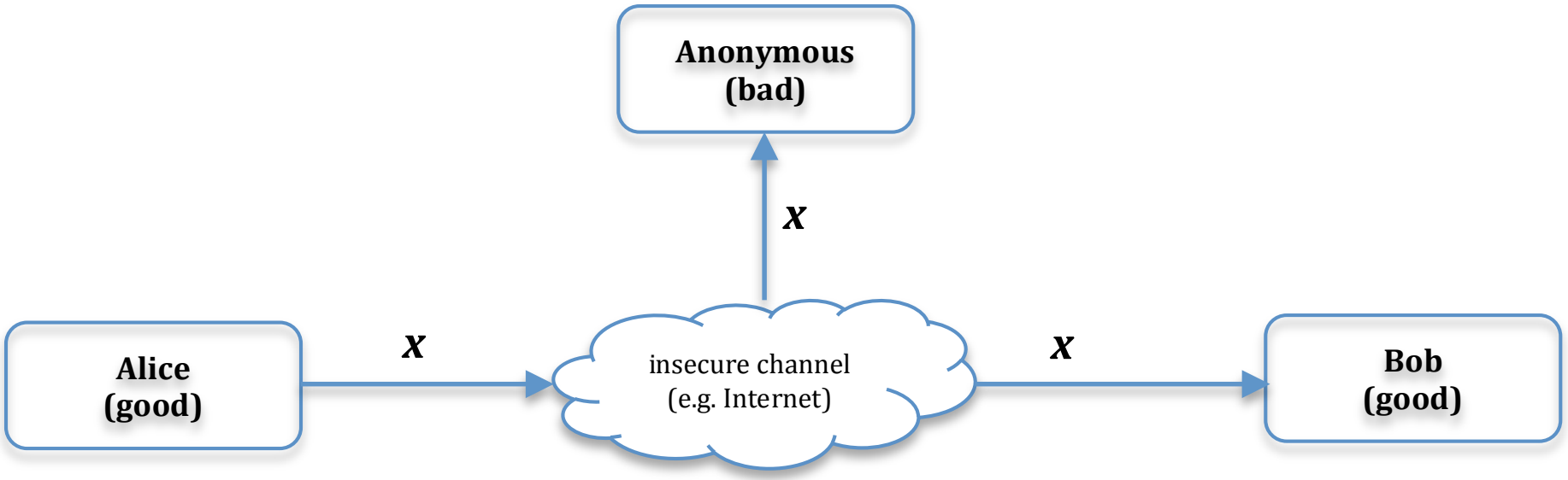
DAT159 – Basic Cryptography Module

Tosin Daniel Oyetoyan

Asset

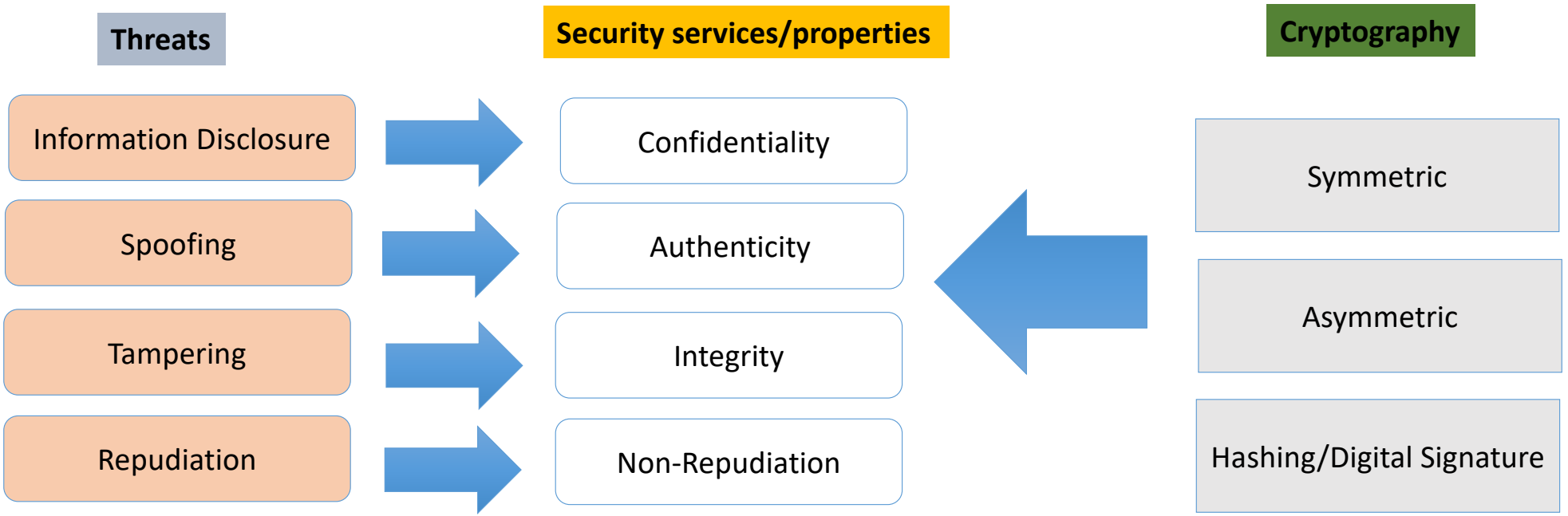
- Something of value
  - To be protected/maintain secrecy
    - Critical information (e.g. Military/Government communications)
    - Patient information
    - Credit card
    - Online transactions
    - …
- Transit, at rest, in use
  - Stored in database, transferred during transactions, under processing (calculations)

Confidentiality

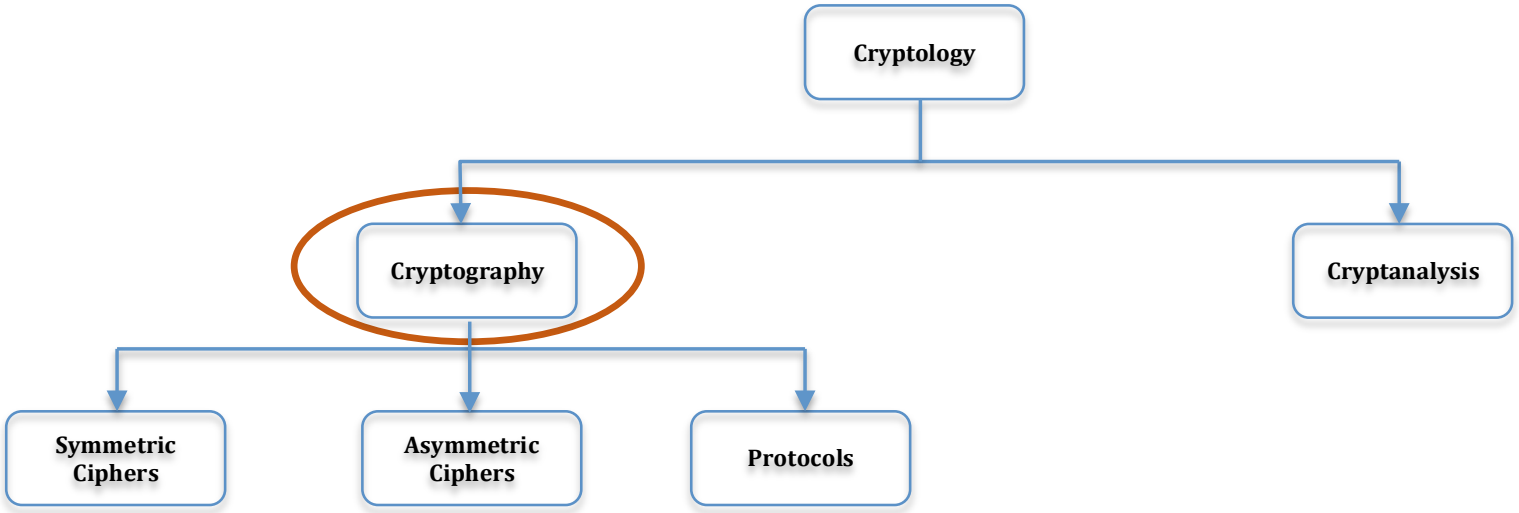


Communication over an insecure channel

Overview


Threats
Security services/properties
Cryptography
Information Disclosure
Spoofing
Tampering
Repudiation
Confidentiality
Authenticity
Integrity
Non-Repudiation
Symmetric
Asymmetric
Hashing/Digital Signature

Overview of Crypt(-ology, -ography, -analysis)



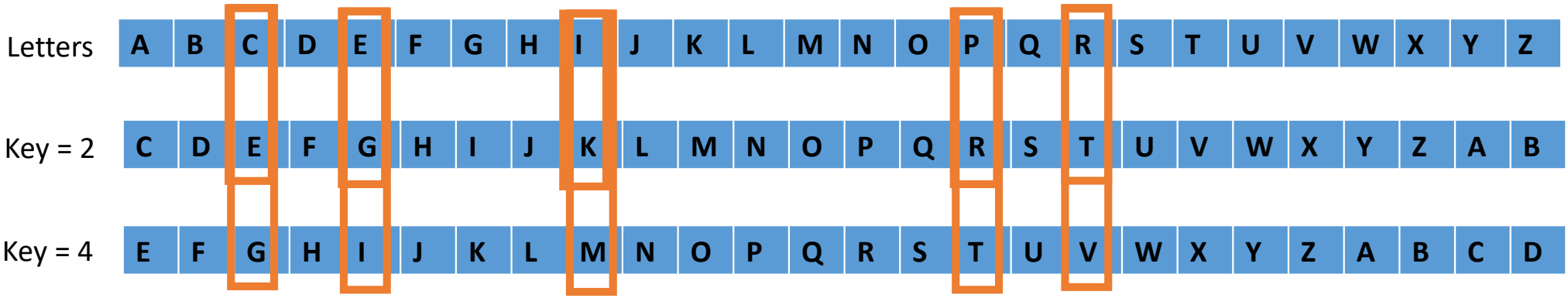
- Cryptography: The science of and art of designing ciphers
- Cryptanalysis: The science and art of breaking ciphers
- Cryptology: The study of Cryptography and Cryptanalysis

History

- Shift cipher (a simple substitution cipher)
- Substitution cipher
- Affine cipher
- Hill cipher
- Vigenere cipher
- Permutation cipher

Shift (Caesar) Cipher

Shift all letters of the plaintext by a constant number of places
Key: Shifted position



Example:

Plaintext CIPHER

Key = 2 EKRJGT

Key = 4 GMTLIV

Number of keys

Key=0

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
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

Key=1

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
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	A

Key=2

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
C	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

.
.
.

How many shift ciphers?

Modular Arithmetic

$Let\ a, r, m\ \in \mathbb{Z}\ (where\ \mathbb{Z}\ is\ a\ set\ of\ all\ integers)\ and\ m > 0. We\ write$:

$a \equiv r\ mod\ m$ reads: ***a*** is congruent/equal to ***r*** in modulo system ***m***

$if\ m\ divides\ a - r.$
$m\ is\ called\ the\ modulus\ and\ r\ is\ called\ the\ remainder$

Operations in the field of cryptography is within a **Finite field**.

Shift (Caesar) Cipher using Modulo Operation

$Let\ x, y, k\ \in\ \mathbb{Z}_{26}.$

$Encryption\colon\ y = e_k(x) \equiv x + k\ mod\ 26$

$Decryption\colon\ x = e_k(y) \equiv y - k\ mod\ 26$

Encode the letters in numbers

$\mathbb{Z}_{26} = \{0,1,2, \dots ,25\}$

x – Plaintext

y – Ciphertext

k – Encryption/Decryption key

- We can then use this algebraic formula for encryption/decryption:

Assume we need to encrypt: **I love pizza** Using the key, k = 5 (Letter F)

x = {ILOVEPIZZA}

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

I		L	O	V	E		P	I	Z	Z	A
8		11	14	21	4		15	8	25	25	0

$x_n = \{x_1, x_2, \ldots x_n\} = \{8,11,14,21,4,15,8,25,25,0\}$

- By using the encryption function: $e_k(x) \equiv x + k \; mod \; 26$

Plaintext: x_n = {8,11,14,21,4,15,8,25,25,0} and k = 5

y = x + k mod 26

Ciphertext: y_n = {13, 16, 19, 0, 9, 20, 13, 4, 4, 5}

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ciphertext: y = {**NQTAJUNEEF**}

- Decryption using the function: $x = e_k(y) \equiv y - k \; mod \; 26$

Ciphertext: y = {**NQTAJUNEEF**} and k = 5

Ciphertext: y_n = {13, 16, 19, 0, 9, 20, 13, 4, 4, 5}

x = y - k mod 26

Plaintext: x_n = {8,11,14,21,4,15,8,25,25,0}

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext: x = {**ILOVEPIZZA**}

Cryptanalysis of Shift Cipher

- Extremely weak and easy to break with insignificant computational effort

Exercise (5mins)

- Decrypt the ciphertext: **ZMIA** using the shift cipher

Brute-Force/Exhaustive key search

- Decrypt the cipher text using each of the 25keys
- Requires:
  - 25 attempts (only)

Cryptotext	Plaintext
ZMIA	YLHZ XKGY WJFX **VIEW** UHDV TGCU SFBT REAS QDZR PCYQ OBXP NAWO MZVN LYUM KXTL JWSK IVRJ HUQI GTPH FSOG ERNF DQME CPLD BOKC ANJB

Substitution Cipher

- Basic idea: We substitute each letter of the alphabet with another one
- The substitution table is the key

$$\begin{aligned} \mathrm{A} &\rightarrow k \\ B &\rightarrow d \\ \mathrm{C} &\rightarrow w \\ &\ldots \end{aligned}$$

Assume we choose a substitution table (key) below for the message, $x = THE\ SUBSTITUTION\ TABLE\ IS\ THE\ KEY$

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
f	i	z	h	t	k	a	n	w	b	v	m	c	q	d	x	g	y	e	l	o	p	r	j	u	s

Our ciphertext becomes: $y = lnt\ eoielwlolwdq\ lfimt\ we\ lnt\ vtu$

Cryptanalysis of substitution cipher

- Attack 1: Brute-Force
  - We need 26! ($4\times10^{26} \approx 2^{88}$) substitution tables

key 1:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	**z**	**y**
key 2:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	**z**	**x**	**y**
key 3:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	**z**	**w**	**x**	**y**

. . .

. . .

key 26!:

We will need several decades with thousands of high-end PCs to perform a brute-force attack on susbtitution cipher!!!

Is it really safe?

- Attack 2: Letter Frequency Analysis
  - The substitution cipher does not hide the statistical property of the encrypted message.
  - It is therefore possible to make inferences of frequent letters from the ciphertext
  - A large key space alone is not sufficient for a strong encryption
  - Ciphertext symbols should appear to be random

Frequency Analysis Attack

- This is based on the assumptions that certain letters in a language appear more frequently than others
- By analysing the cryptotext for repeated letters, we can guess the right letter, etc.
- Example: English letters
  - Probability of occurence of the 26 letters

Letter	Freq/Prob	Letter	Freq/Prob
A	0.082	N	0.067
B	0.015	O	0.075
C	0.028	P	0.019
D	0.043	Q	0.001
E	0.127	R	0.060
F	0.022	S	0.063
G	0.020	T	0.091
H	0.061	U	0.028
I	0.070	V	0.010
J	0.002	W	0.023
K	0.008	X	0.001
L	0.040	Y	0.020
M	0.024	Z	0.001

Digrams and Trigrams

30 most common digrams

Digrams		
TH	NT	TE
HE	HA	SE
IN	ND	HI
ER	OU	OF
AN	EA	
RE	NG	
ED	AS	
ON	OR	
ES	TI	
ST	IS	
EN	ET	
AT	IT	
TO	AR	

12 most common trigrams

Trigrams
THE
ING
AND
HER
ERE
ENT
THA
NTH
WAS
ETH
FOR
DTH

Multiplicative Cipher system – Affine Cipher

- A more complex cipher algorithm
- Requires more computational effort to break compared to shift cipher
  - 2 key systems combining multiplicative and additive operations

$Let\ x, y, k\ \in\ \mathbb{Z}_{26}.$

$Encryption\colon\ y = e_k(x) \equiv a.x + b\ mod\ 26$

$With\ the\ key\colon k = (a, b), with\ the\ restriction\colon \gcd(a, 26) = 1.$

x – Plaintext

y – Ciphertext

a – Multiplicative key

b – Additive key

gcd = Greatest Common Divisor

Encryption (easy part)

$$Encryption: e_k(x) = y \equiv a.x + b \; mod \; 26$$

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Recall the previous example: Plaintext: x = {**ILOVEPIZZA**}

Plaintext: x_n = {8,11,14,21,4,15,8,25,25,0}

This time, we'll use 2 keys (a,b) = (5,7)

y_1 = (5*8+7)%26 = 21
y_2 = (5*11+7)%26 = 10
.
.
.
y_n = (a*n+b)%26

Ciphertext: y_n = {21,10,25,8,1,4,21,2,2,7}

Ciphertext: y = {**VKZIBEVCCH**}

Exercise (2mins)

- Think about how to decrypt the Affine Cipher

Decryption

We can derive the decryption function from the encryption function: $y \equiv a.x + b \; mod \; 26$

$a.x + b \equiv y \; mod \; 26$ ... (1)

$a.x \equiv y - b \; mod \; 26$ ... (2)

$x \equiv a^{-1}.(y - b) \; mod \; 26$ ... (3)

$$Decryption\text{: } x = d_k(y) \equiv a^{-1}(y - b) \; mod \; 26$$

- We will look at 2 main operations necessary to decrypt multiplicative cipher
  - Inverse of the key, *a* (a^{-1})
  - Greatest Common Divisor (gcd) of ***a*** in modulo ***m***

Inverse of multiplicative cipher

- To succeed with finding inverse, 2 properties must hold:

1. $a.a^{-1} \equiv 1\ mod\ 26$
2. $\gcd(a, 26) = 1.$

   - for gcd(*a*, 26) = 1, it means:
     - *a* and the modulus (26) must be relatively prime (coprime)
     - Therefore: $a \in \{1, 3, 5, 7, 9, 11, 13, 15, 17, 21, 23, 25\}$

How to compute the inverse of a key (Trial and Error Approach)

Check until you find the number (a^{-1}) such that $a.a^{-1} \equiv 1 \, mod \, 26$

e.g. Find the inverse of a = 5

First, we check if gcd(5, 26) = 1

What is the greatest common divisor of 5 and 26?

Factor 5 = 1 x 5

Factor 26 = 1 x 2 x 13

Factorization

The inverse (*5* = 21) in modulus 26

Note: The red rows are not to be computed because their gcds are not equal to one

a^{-1}	a	$a.a^{-1}\%26$
1	5	5
2	5	10
3	5	15
4	5	20
5	5	25
6	5	4
7	5	9
8	5	14
9	5	19
10	5	24
11	5	3
12	5	8
13	5	13
14	5	18
15	5	23
16	5	2
17	5	7
18	5	12
19	5	17
20	5	22
21	**5**	**1**

Exercise (5mins)

Find the inverse of the key ***α*** in modulus **26**

a	**1**	**2**	**3**	**7**	**9**
$\mathbf{a^{-1}}$	-	-			

Solution

a	**1**	**2**	**3**	**7**	**9**
$\mathbf{a^{-1}}$	-	-	**9**	15	**3**

Although gcd(1, 26) = 1. However, $\mathbf{a^{-1}} = 1$ (same number)

gcd(2, 26) = 2 ≠ 1

Decrypting Affine Cipher

Decrypt

Ciphertext: y = {**VKZIBEVCCH**}

Decryption function: $x \equiv a^{-1}(y - b)\ mod\ 26$

Ciphertext: y_n = {21,10,25,8,1,4,21,2,2,7}

Previously,

The inverse a^{-1} = 21 in modulus 26
and
b = 7

y_n	21	10	25	8	1	4	21	2	2	7
x_n	8	11	14	21	4	15	8	25	25	0
x	**I**	**L**	**O**	**V**	**E**	**P**	**I**	**Z**	**Z**	**A**

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**
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Computational effort to break Affine Cipher

- What is the key space for Affine Cipher?

key space = #values for a * #values for b

= 12 * 26 = 312

- Brute-force (Exhaustive search)
  - 312 keys
- Frequency Analysis

Cryptanalysis of Affine Cipher

- The Affine cipher increased the key space over shift cipher
- However, it is still susceptible to:
  - Brute-Force and Frequency analysis attacks

Ciphertext: y = {**VKZIBEVCCH**}

Polyalphabetic Cryptosystem

- Previous ciphers are monoalphabetic cryptosystem
  - Means that, letters of the plaintext are mapped to letters of the ciphertext using a single alphabet key
- In polyalphabetic cipher
  - More than one alphabets are used to encrypt the plaintext
  - The main purpose is to defeat frequency analysis attack
- We will look at 2 examples
  - Vigenère cipher
  - Hill cipher

Vigenère cipher

Main difference: We use more than one alphabetical letter as key

Example:

$x = ATTACKATDAWN$
$we\ choose\ the\ key$
$k = NULE$
$Numerical\ equivalent, k = (13, 20, 11, 4)$

x	A	T	T	A	C	K	A	T	D	A	W	N
x_n	0	19	19	0	2	10	0	19	3	0	22	13
k	N	U	L	E	N	U	L	E	N	U	L	E
y	**N**	**N**	**E**	**E**	P	**E**	L	X	Q	U	H	R

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**
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Exercise (5mins)

- Decrypt by hand the Vigenère cipher

y	13	13	4	4	15	4	11	23	16	20	7	17
k	13	20	11	4	13	20	11	4	13	20	11	4
x												

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Vigenère cipher

$Let\ x, y, k\ \in\ \mathbb{Z}_m.$

$We\ can\ define\ encryption\ as:$

$$y_i = e_k(x_i) = (x_i + k_{(i\ mod\ l)})\ mod\ m$$

$and\ decryption\ as:$

$$x_i = d_k(y_i) = (y_i - k_{(i\ mod\ l)})\ mod\ m$$

$where\ m\ is\ the\ modulus$
$and\ l\ is\ the\ length\ of\ key$

Source: Wikipedia

x – Plaintext

y – Ciphertext

k – Encryption/Decryption key

Vigenère cipher

Use the encryption function: $y_i = e_k(x_i) = (x_i + k_{(i \bmod l)}) \bmod m$

$x = ATTACKATDAWN$

$k = NULE$

$Numerical\ value, k = (13, 20, 11, 4)$

$m = 26\ and\ l = 4$

i	0	1	2	3	4	5	6	7	8	9	10	11
x	0	19	19	0	2	10	0	19	3	0	22	13
$i \bmod 4$	0	1	2	3	0	1	2	3	0	1	2	3
$k_{(i \bmod 4)}$	13	20	11	4	13	20	11	4	13	20	11	4
$x_i + k_{(i \bmod 4)} \bmod 26$	13	13	4	4	15	4	11	23	16	20	7	17
y	N	N	E	E	P	E	L	X	Q	U	H	R

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Decrypting the Vigenère cipher

Use function: $x_i = d_k(y_i) = (y_i - k_{(i \bmod l)}) \bmod m$

$y = NNEEPELXQUHR$
$k = NULE$
$Numerical\ equivalent, k = (13, 20, 11, 4)$
$m = 26\ and\ l = 4$

i	0	1	2	3	4	5	6	7	8	9	10	11
y	13	13	4	4	15	4	11	23	16	20	7	17
$i \bmod 4$	0	1	2	3	0	1	2	3	0	1	2	3
$k_{(i \bmod 4)}$	13	20	11	4	13	20	11	4	13	20	11	4
$y_i - k_{(i \bmod 4)} \bmod 26$	0	19	19	0	2	10	0	19	3	0	22	13
x	A	T	T	A	C	K	A	T	D	A	W	N

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Cryptanalysis of Vigenere cipher

- Frequency analysis:
  - If you know that the length of the keyword is n, you can break the ciphertext into n cosets and attack the cipher using frequency analysis if the ciphertext sample is long enough.
- Friedman Test
  - Find the Incidence of Coincidence to determine whether or not a polyaphabetic substitution has been used
  - It is the probability that two randomly selected letters are the same
- Kasisiki test
  - Uses the occasional aligning of groups of letters with keyword to determine the length of the keyword

https://www.cs.uri.edu/cryptography/classicalvigenerecrypt.htm

Hill Cipher

- Polyalphabetic cipher
- Requires at least 2 keys
- Uses a linear combination of the key with the plaintext to form the ciphertext

$Let\ key\ K = (k_1, k_2, k_3, k_4)$ and p$laintext\ be\ x$

We can break x down into 2 parts as $x_1, x_2\ and\ formulate\ our\ ciphersystem\ as\ a\ linear\ combination$:

$$k = \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix} \qquad x = [x_1 \quad x_2]$$

$$[y_1 \quad y_2] = [x_1 \quad x_2] \begin{bmatrix} k_1 & k_2 \\ k_3 & k_4 \end{bmatrix}$$

The ciphertext is obtained from the plaintext by means of a linear transformation

Conditions:

- The matrix **k** must be invertible otherwise we cannot decrypt **y** (Note: not all matrices are invertible)
- If det k = 0, then k is not invertible
- In modulo N, we can check that k has an inverse in modulo N by checking if gcd(det K, N) = 1

Examples

- Use the key *k* = **PATH** to encrypt the message *x* = **CIPHER** using the Hill cipher ($in\ \mathbb{Z}_{26}$)

1. Formulate the matrices

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$$k = (15, 0, 19, 7)$$

$$k = \begin{bmatrix} 15 & 0 \\ 19 & 7 \end{bmatrix}$$

$$x = (2, 8, 15, 7, 4, 17)$$

$$x = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \end{bmatrix}$$

2. Find (a) the determinant of k and (b) check if gcd(det k, 26) = 1

$$det.k = (15\times7 - 0\times19) = 105 \equiv 1\ mod\ 26$$ ✓

$$gcd(1, 26) = 1$$ ✓

k = PATH is a valid key

ENCRYPT:

$$k \times x = \begin{bmatrix} 15 & 0 \\ 19 & 7 \end{bmatrix} \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \end{bmatrix}$$

$$= \begin{bmatrix} 4 & 16 & 17 \\ 9 & 24 & 14 \end{bmatrix} mod\ 26$$

$$y = \begin{bmatrix} E & Q & R \\ J & Y & O \end{bmatrix}$$

$$ciphertext = \boldsymbol{EQRJYO}$$

TO DECRYPT:

$$Inverse\ of\ a\ 2{\times}2\ matrix \begin{bmatrix} a & b \\ c & d \end{bmatrix} = (a.d - b.c)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

3. Find the inverse of k (i.e. k^{-1})

$$k^{-1} = \frac{1}{1} \begin{bmatrix} 7 & 0 \\ -19 & 15 \end{bmatrix}$$

$$k^{-1} = \begin{bmatrix} 7 & 0 \\ 7 & 15 \end{bmatrix} mod\ 26$$

$$x = k^{-1} \times y = \begin{bmatrix} 7 & 0 \\ 7 & 15 \end{bmatrix} \begin{bmatrix} 4 & 16 & 17 \\ 9 & 24 & 14 \end{bmatrix}$$

$$x = \begin{bmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \end{bmatrix} mod\ 26$$

$$x = \begin{bmatrix} C & I & P \\ H & E & R \end{bmatrix}$$

$$plaintext = \boldsymbol{CIPHER}$$

Hill Cipher

- $For\ a\ key\ K, we\ define$:
  - $e_k(x) = xK$
- and
  - $d_k(y) = yK^{-1}$,
- $where\ all\ operations\ are\ performed\ in\ \mathbb{Z}_{26}$
- $and\ \mathcal{K} = \{m \times m\ invertible\ matrices\ over\ \mathbb{Z}_{26}\}$

- Modern cryptography algorithms uses
  - Substitution
  - **Permutation**

Permutation

Example

Let m = 6 and the key is the following permutation π:

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

The inverse π^{-1} can be constructed by interchanging the two rows, and rearranging the columns so that the first row is in increasing order:

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

Encrypt the plaintext: **shesellsseashellsbytheseashore**

since m=6, we partition the message into group of 6 letters:

shesel | lsseas | hellsb | ythese | ashore

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

EESLSH | SALSES | LSHBLE | HSYEET | HRAEOS

EESLSHSALSESLSHBLEHSYEETHRAEOS

Decrypt using the inverse function π^{-1}

Ciphertext: **EESLSH | SALSES | LSHBLE | HSYEET | HRAEOS**

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

Plaintext: **SHESEL | LSSEAS| HELLSB| YTHESE|ASHORE**

Exercise (5mins)

(a) Suppose that π is the following permutation of {1, . . . , 8}:

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

Compute the permutation π^{-1}:

x	1	2	3	4	5	6	7	8
$\pi^{-1}(x)$								

(b) Decrypt the following ciphertext, for a permutation Cipher with m=8, which was encrypted using the key π :

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM

Solution

GENTLE MEN DO NOT READ EACH OTHERS MAIL

Quiz (2mins)

1. An example of a monoalphabetic cipher is:
   a) Shift cipher
   b) Hill cipher
   c) Vigenere cipher
2. Two conditions must hold to find the multiplicative inverse of an integer modulo another integer
   a) The gcd of the integer and the modulo integer must be invertible
   b) The gcd of the integer and the modulo integer must be equal to one
   c) The gcd of the integer and the modulo integer must be equal to zero
3. The main purpose of using a polyalphabetic cipher is to:
   a) Hide the statistical property of the plaintext letters
   b) Increase the number of letters in the ciphertext
   c) Defeat brute-force attack
4. Hill cipher is:
   a) An Asymmetric cipher
   b) A Symmetrric cipher
   c) A Hash function
5. Cyptography can be directly linked to all of these core security properties except:
   a) Confidentiality
   b) Integrity
   c) Availability
   d) Authenticity