POLITÉCNICO DE LEIRIA
ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Information Security

Symmetric Ciphers

Classical Encryption Techniques

Lecturer (Academic year 2016-2017):
Marisa Maximiano

UNDERGRADUATE DEGREE IN
COMPUTER ENGINEERING

Summary

- Symmetric Cipher – Classical encryption techniques
  - Symmetric cipher model
    - Cryptography
    - Cryptanalysis and Bruce-force attack
  - Substitution techniques
  - Transposition techniques
  - Rotor machines
  - Conclusions

Some key points and definitions…

- **Plain text**
  - The original message or data in readable form
- **Cypher text**
  - The unreadable message (results from encryption algorithm)
- **Secret key**
  - The other input of the encryption algorithm (+ plain text)

Some key points and definitions…

- **Encryption algorithm**
  - Generates the cipher text from plain text (and key)
- **Decryption algorithm**
  - Recovers the plain text from the cipher text (and key)

Some key points and definitions…

Cryptography

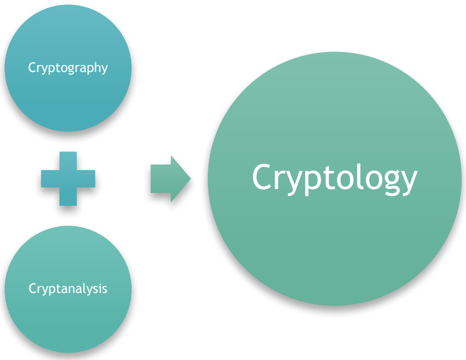
- **Schemes used for encryption** constitute the area of study known as cryptography

Cryptanalysis

- **Techniques used for deciphering a message** without any knowledge of the enciphering details ("breaking the code")

Cryptology

- The areas of cryptography and cryptanalysis together are called cryptology



Symmetric encryption

Also known as Conventional encryption or Single key encryption

Some key points and definitions…

- **Symmetric encryption**
  - Cryptosystem which uses the **same key** for both encryption and decryption
  - Transforms plain text into cipher text and needs:
    - A secret key
    - An encryption algorithm
  - Using the same key and decryption algorithm, the plain text is recovered from the cipher text

Some key points and definitions…

- Symmetric encryption

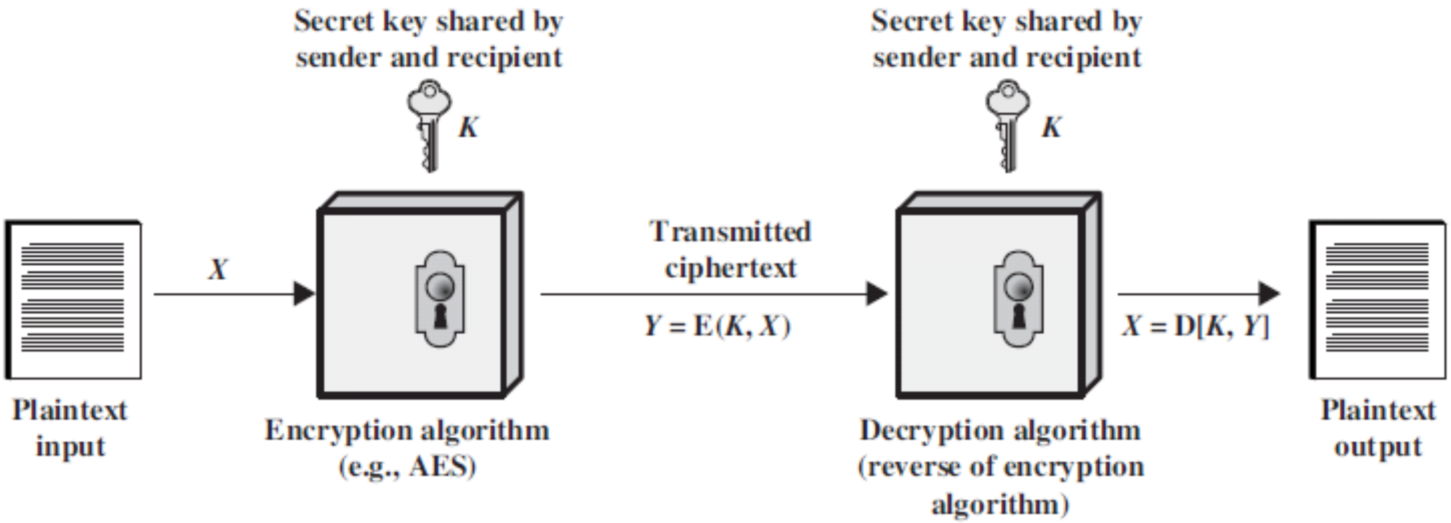


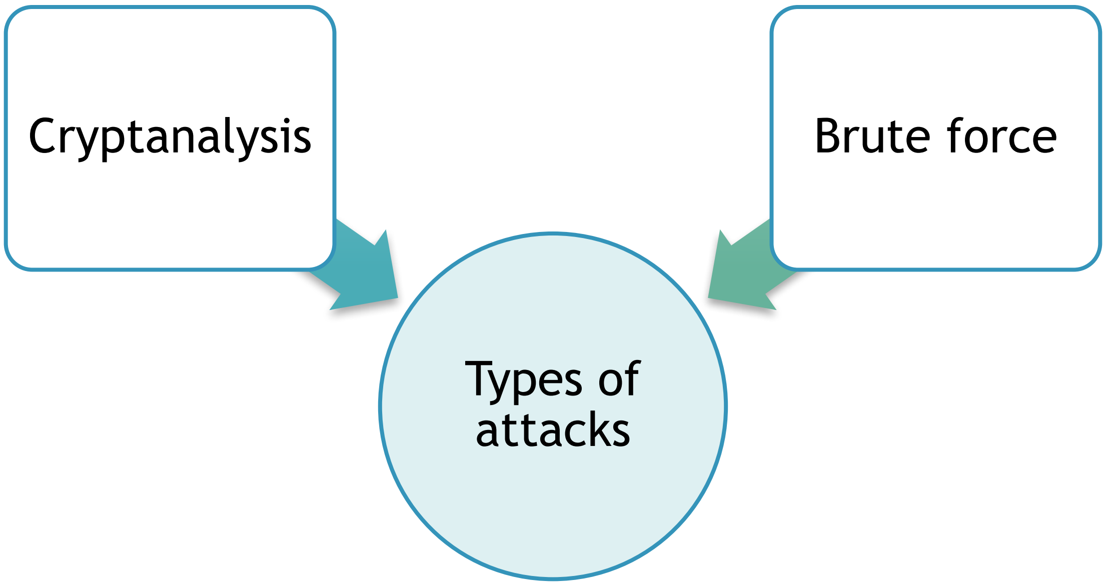
Fig. – Simplified symmetric encryption and decryption

Some key points and definitions…

- **Symmetric encryption**
  - An opponent should be unable to decrypt cipher text or discover the key even if he has examples of cipher texts/plain text
  - Sender/receiver must obtain the secret key in a secure fashion
  - If someone discovers the key and knows the algorithm, all communication using this key is readable
  - It is not need to keep the algorithm secret, only the **key needs to be secret**

Some key points and definitions…

- **Types of attacks on an encryption algorithm**



Some key points and definitions…

- **Types of attacks on an encryption algorithm:**
  - **Cryptanalysis** – explores the “known“ information
    - Can have two possible goals:
      - Cryptanalyst might have cipher text and want to **discover the plain text**
      - Cryptanalyst might have the cipher text and want to **discover the encryption key** used to encrypt the message

Cryptanalysis

Some key points and definitions…

- **Types of attacks on an encryption algorithm:**
  - **Cryptanalysis** – explores the “known“ information
    - French document (statistics)
    - English document (statistics)
    - Executable file (format/headers/etc.)
    - Class file (signature 0xCAFEBABE)

Cryptanalysis

Some key points and definitions…

- **Types of attacks on an encryption algorithm:**
  - **Brute force** – tries every possible key

Brute force

- The most straight-forward attack on a encrypted message is simply to attempt to **decrypt the message with every possible key**
- Most of these attacks fail! But one might work!

⇩

At which point you can **decrypt the message** and any **others in that the key** is used on

Some key points and definitions…

- **Types of attacks on an encryption algorithm:**
  - **Brute force** – tries every possible key
    - On average, half of possible keys are enough

Brute force

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

Fig. – Time required to exhaustive key search

Some key points and definitions…

- **Techniques used in symmetric ciphers:**
  - **Substitution** – map plain text into cipher text elements
  - **Transposition** – plain text elements are transposed

Most systems involve multiple stages of substitutions and transpositions

Symmetric cipher main requirements

- **A strong algorithm**
  - If we know the **algorithm** and some resulting **cipher texts**
    - We are unable to figure out the key
    - We are unable to decipher the cipher text
- **Secret key must remain secret**
  - Key must be shared in a secure way

Symmetric cipher main requirements

- **Remember:**
  - Only the key must remain secret
  - Algorithm is usually public domain

✓ **Main challenge:**

Keep the secret key

Symmetric ciphers

- Model of symmetric cryptosystem

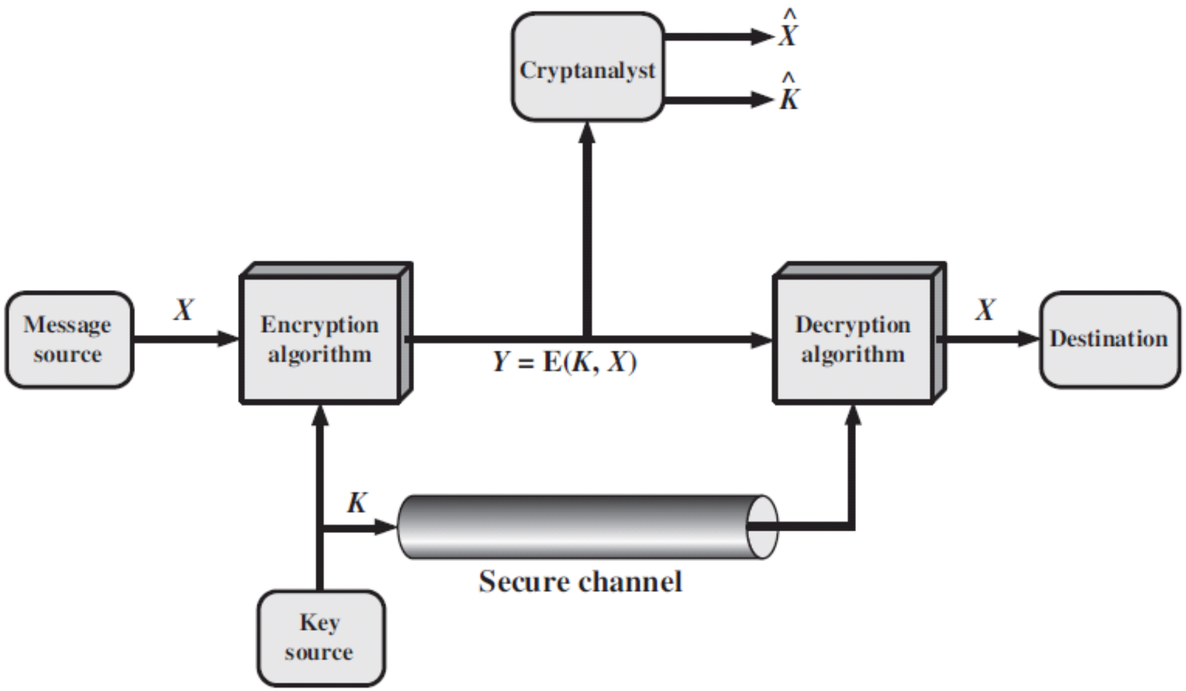


Fig. – Complete model of a symmetric cryptosystem

Substitution techniques

A letter is replaced by other letter, number or symbol

Substitution techniques

- A letter is replaced by other letter, number of symbol
- Classic encryption:
  1. **Caesar cipher**
  2. **Monoalphabetic ciphers**
  3. **Playfair cipher**
  4. **Polyalphabetic cipher (e.g. Vigenère cipher)**
  5. **Vernam cipher (“One-time pad”)**

Substitution techniques

- **Caesar Cipher**
  - The earliest known substitution cipher (Julius Caesar)
  - **Three** places further down the alphabet
    - Example:

```
plain:  meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB
```

    - Transformation:

```
plain:   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
cipher:  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
```

Substitution techniques

- **Caesar Cipher**
  - The algorithm

	0	1	2…																							25
plain:	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
cipher:	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

  - $C = E(3, p) = (p + 3) \bmod 26$ Caesar encryption
  - $C = E(k, p) = (p + k) \bmod 26$ Generic (Caesar) encryption
  - $p = D(k, C) = (C - k) \bmod 26$ Generic (Caesar) decryption

Substitution techniques

- **Caesar Cipher**
  - If *Darth* knows that it is Caesar cipher text…
    - Brute force attack…

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

✓ **Which properties allow this?**

Substitution techniques

- **Caesar Cipher**
  - If *Darth* knows that it is Caesar cipher text…
    - Brute force attack…

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

✓ **Which properties allow this?**

- Algorithm
- Number of keys
- Plain text language

Substitution techniques

- **Caesar Cipher**
  - If *Darth* knows that it is Caesar cipher text…
    - Brute force attack…

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

- Algorithm
- Number of keys
- Plain text language

✓ **Can we (user) increase the difficult in getting the plain text?**

Substitution techniques

- **Caesar Cipher**
  - If *Darth* knows that it is Caesar cipher text…
    - Brute force attack…

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

✓ **Can we (user) increase the difficult in getting the plain text?**

- Choose other language
- Abbreviate
- Compress
- Expand 26 chars

Substitution techniques

- **Evolution from Caesar Cipher**
  - What about **permutations** instead of right shifts?
    - **Example:** consider characters 'a', 'b', 'c'
      - a,b,c; a,c,b; b,a,c; b,c,a; c,a,b; c,b,a (6=3!)
    - **Example:** consider alphabet
      - Number of keys : 26! = $4 * 10^{26}$ (Huge!)

✓ Bruce force attack extremely complicated

✓ Also called a **monoalphabetic substitution cipher**

Substitution techniques

- **Monoalphabetic ciphers**
  - What about cryptanalysis attack?
    - If the cryptanalyst knows the nature of the plaintext (e.g., noncompressed English text)
    - **Cipher text:**

      UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
      VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
      EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

    - **Frequencies:**

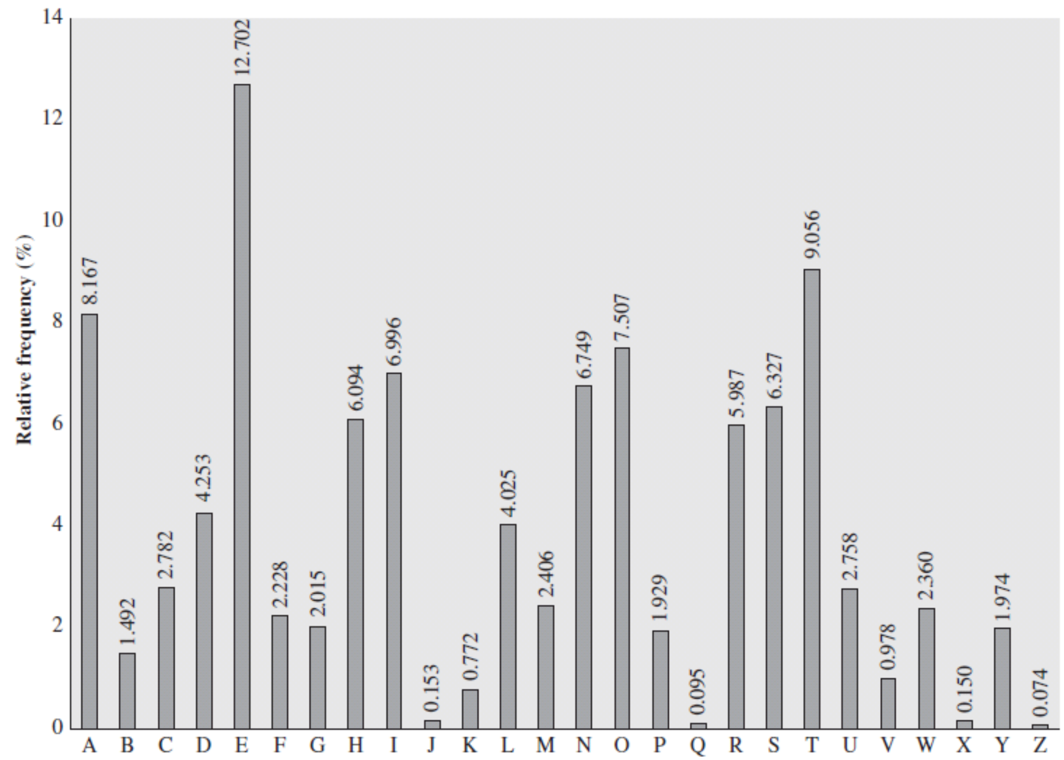
P	13.33	H	5.83	F	3.33	B	1.67	C	0.00
Z	11.67	D	5.00	W	3.33	G	1.67	K	0.00
S	8.33	E	5.00	Q	2.50	Y	1.67	L	0.00
U	8.33	V	4.17	T	2.50	I	0.83	N	0.00
O	7.50	X	4.17	A	1.67	J	0.83	R	0.00
M	6.67								

Frequency of the letters in cipher text (in %)

Substitution techniques

- **Monoalphabetic ciphers**
  - What about cryptanalysis attack?
    - **Cipher text:**

Relative Frequency of Letters in English Text



Substitution techniques

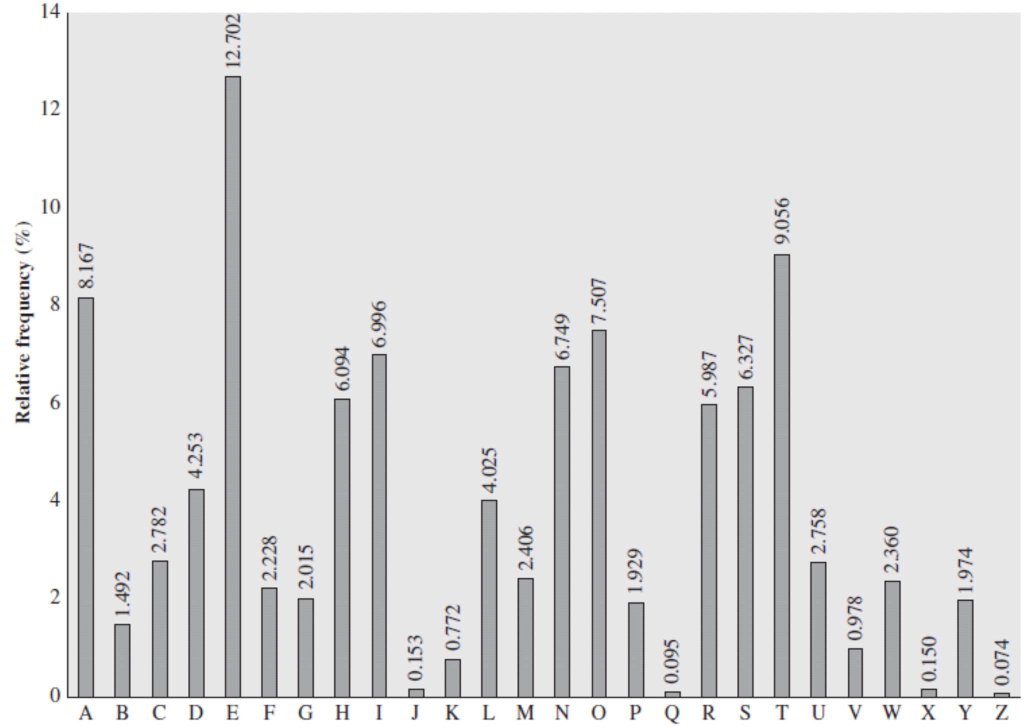
- **Monoalphabetic ciphers**
  - What about cryptanalysis attack?

P	13.33	H	5.83	F	3.33	B	1.67	C	0.00
Z	11.67	D	5.00	W	3.33	G	1.67	K	0.00
S	8.33	E	5.00	Q	2.50	Y	1.67	L	0.00
U	8.33	V	4.17	T	2.50	I	0.83	N	0.00
O	7.50	X	4.17	A	1.67	J	0.83	R	0.00
M	6.67								

The letters P and Z are the equivalents of plain letters e and t

The letters S, U, O, M, and H are all of relatively high frequency, probably correspond to plain letters from the set {a, h, i, n, o, r, s}

The letters with the lowest frequencies (namely, A, B, G, Y, I, J) are likely included in the set {b, j, k, q, v, x, z}



Substitution techniques

- **Monoalphabetic ciphers**
  - What about cryptanalysis attack?
    - If the plain text is too long this could be enough…
    - Otherwise, find regular sets of two letters (**th** or **the**)
    - Etc…

Sensitive to frequency data of the alphabet

    - Monoalphabetic ciphers are easy to break…
    - Coutermeasure, e.g. is to provide multiple substitutes

Substitution techniques

- **Playfair Cipher (used in world war I by UK and USA)**
  - Key: 5x5 matrix with all alphabetic chars. I and J together
    - Fill it using alphabetic (random)
    - Or a well-known word at the beginning (no duplicates). Normally constructed using a keyword
    - Etc...

e.g.

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

Keyword: Harpsichord

e.g.

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

Keyword: Monarchy

Substitution techniques

- Playfair Cipher (used in world war I by UK and USA)
  - **Repeating plain text**
    - Rule 1: split plain text into groups of two letters
      - If duplicated, replace second char by a filler letter (such as X) and shift right the second char to the next group
      - If number of characters is odd pad it with an additional X at the end
    - Example:

“SOSSEGO” → SO–SS–EG–O → SO–SX–SE–GO

“BALLOON” → BA–LL–OO–N → BA–LX–LO–ON

Substitution techniques

- **Playfair Cipher (used in world war I by UK and USA)**
  - **Rules to encrypt/decrypt**
    - Rule 2: If *m1* and *m2* are on the **same line**, then encrypted characters are the **right** characters of *m1* and *m2*
      - With the first letter of the row circularly following the last
    - Example:
      - PA encrypts as SR

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

Substitution techniques

- **Playfair Cipher (used in world war I by UK and USA)**
  - **Rules to encrypt/decrypt**
    - Rule 3: If *m1* and *m2* are on the **same column**, then encrypted characters are **beneath** *m1* and *m2*
      - With the first letter of the row circularly following the last
    - Example:
      - BZ encrypts as LS

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

Substitution techniques

- **Playfair Cipher (used in world war I by UK and USA)**
  - **Rules to encrypt/decrypt**
    - Rule 4: If *m1* and *m2* are in **different lines and columns**, return the rectangle vertex (its own row, column occupied by the other letter)
    - Example:

"SOSSEGO" → SO-SS-EG-O → SO-SX-SE-GO

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

- SO encrypts as RB
- SX as RZ
- SE as HL
- GO as QG
- Etc.

Other examples:

- OH as IR (or JR)
- TC as ND

Substitution techniques

- **Playfair Cipher (used in world war I by UK and USA)**
  - Number of keys
    - $25! = 2^{84}$
  - Character frequency are more flat now
  - It was considered a strong encryption method
  - Today it is cracked using brute force and a computer

Substitution techniques

- **Polyalphabetic Ciphers**
  - Uses different mono alphabetic substitutions

Substitution techniques

- **Polyalphabetic Ciphers**
  - **Vigenère cipher**
    - One character has multiple correspondences
    - There is a password
    - Lots of alphabets applied
    - It uses 25 Caesar Keys

Substitution techniques

- **Polyalphabetic Ciphers**
  - **Vigenère cipher**

Vigenère table

The plain text char indexes column

The password character indexes lines

The **interception** is the encrypted char

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

Substitution techniques

- **Polyalphabetic Ciphers**
  - **Vigenère cipher:** example

Plain text: `temos um novo presidente`
Key: `NUMABOA`

⇩

Plain text: `t e m o s u m n o v o p r e s i d e n t e`
Key: `N U M A B O A N U M A B O A N U M A B O A`
Displacem.: 13 20 12 01 1401320120114013201201140
Cipher text: `G Y Y O T I M A I H O Q F E F C P E O H E`

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

Substitution techniques

- **Polyalphabetic Ciphers**
  - **Vigenère cipher:** properties
    - Multiple cipher text letters for each plain text letter
    - Letter frequency information is obscured

Substitution techniques

- **Polyalphabetic Ciphers**
  - **Vigenère cipher** vs **monoalphabetics**
    - Suppose *Darth* believes that cipher text was encrypted either with vigenère or monoalphabetic substitution...

✓ **How to make a determination (which one) ?**

If **monoalphabetic** then plain text frequency close to cipher text frequency

Substitution techniques

- **Polyalphabetic Ciphers**
  - **Vigenère cipher** vs **monoalphabetics**
    - Suppose *Darth* believes that cipher text was encrypted either with vigenère or monoalphabetic substitution…

```
CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBWRVXU
OAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAKLXFPSKAU
TEMNDCMGTSXMXBTUIADNGMGPSRELXNJELXVRVPRTULHDNQ
WTWDTYGBPHXTFALJHASVBFXNGLLCHRZBWELEKMSJIKNBHW
RJGNMGJSGLXFEYPHAGNRBIEQJTAMRVLCRREMNDGLXRRIMG
NSNRWCHRQHAEYEVTAQEBBIPEEWEVKAKOEWADREMXMTBHHC
HRTKDNVRZCHRCLQOHPWQAIIWXNRMGWOIIFKEE
```

Substitution techniques

- **Polyalphabetic Ciphers**
  - **Vigenère cipher** vs **monoalphabetics**
    - Suppose *Darth* believes that cipher text was encrypted either with vigenère or monoalphabetic substitution…

```
Positions of 'CHR': 1, 166, 236, 276, 286

Absolute positions:
166 - 1 = 165        236 - 1 = 235
276 - 1 = 275        286 - 1 = 285

It seems that key length is 5…

Continue on: http://math.ucsd.edu/~crypto/java/EARLYCIPHERS/Vigenere.html
```

Substitution techniques

- **Vernam cipher (and the "one-time pad")**
  - Key must be as **long as the plain text**
  - Works on **bits** and not on letters
  - The algorithm can be expressed as:

$$c_i = p_i \oplus k_i$$

p_i = i th binary digit of plain text
k_i = i th binary digit of key
c_i = i th binary digit of cipher text
$\oplus$ = exclusive-or (XOR) operation

Substitution techniques

- **Vernam cipher**

$$c_i = p_i \oplus k_i \qquad\qquad p_i = c_i \oplus k_i$$

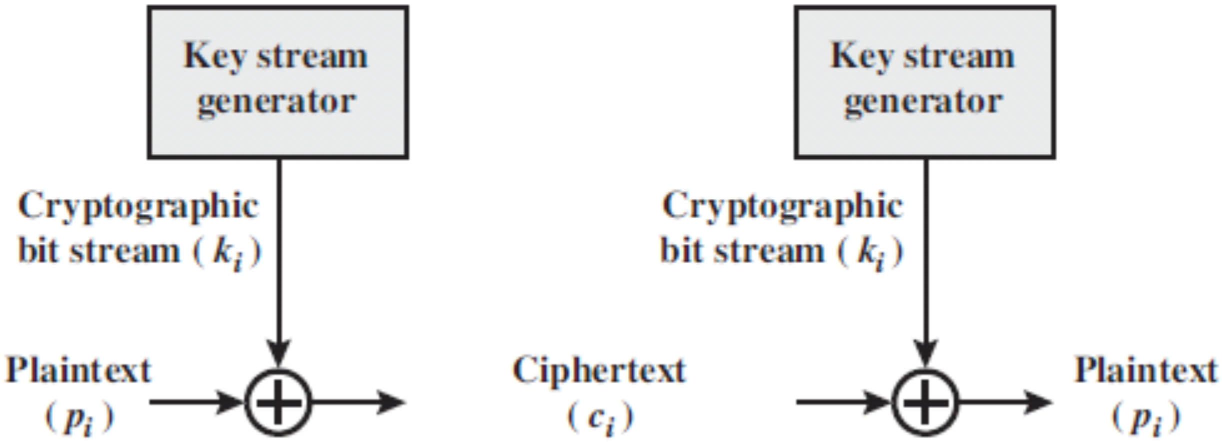


Fig. – Vernam cipher building blocks

Substitution techniques

- **Vernam cipher**
  - Vernam wrote that key could come from a loop tape
    - Key has the same length of plain text
    - For long plain text key must be **repeated**

Very short could be a weakness

  - The ultimate defense against a cryptanalysis is to choose a keyword that is as long as the plaintext and has no statistical relationship to it

Substitution techniques

- **Vernam cipher**
  - **One-time pad**
    - improvement to the Vernam cipher that yields the ultimate in security
    - **random key** that is as **long as the message**, so that the key need not be repeated
    - the key is to be used to encrypt and decrypt **a single message**, and then is discarded

Such a scheme, known as a **one-time pad**, is unbreakable

It produces random output that bears no statistical relationship to the plaintext

Transposition techniques

Permutation on the plain text letters…

Transposition techniques

- Permutation on the plain text letters…
  - **Rail fence technique**
    - Very simple: write diagonal, read in rows

Plain text: `meet me after the toga party`

Rail fence of depth 2

```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

Cipher text: `MEMATRHTGPRYETEFETEOAAT`

Trivial to cryptanalysis

Transposition techniques

- Permutation on the plain text letters…
  - **Route cipher**
    - Uses a grid `NxM`
    - It is filled top/down , top/down, …
    - Key: grid dimension + pattern used to extract cipher text

Transposition techniques

- Permutation on the plain text letters…
  - **Route cipher:** example

Plain text: `This is a secret message`

Key: `3x7 grid + clockwise spiral`

T	S	A	C	T	S	G
H	I	S	R	M	S	E
I	S	E	E	E	A	J

J → Just to fill the space…

Cipher text: `TSACTSGEJAEEESIHISRMS`

Transposition techniques

- Permutation on the plain text letters…
  - **Route cipher:**
    - If a good and creative key is established it is hard to break it
    - If key is weak the plain text is exposed

Transposition techniques keep alphabet frequencies!

Usually transposition techniques are mixed with substitution techniques

Rotor machines

Before the introduction of DES, the most important application of the principle of multiple stages of encryption was a class of systems known as rotor machines

Rotor machines

- **Multiple stages of encryption**
  - Multiple stages of encryption can produce an algorithm that is significantly more difficult to cryptanalyze
  - This is as true of substitution ciphers as it is of transposition ciphers
  - The **best** approach before modern techniques
  - Based on **substitution** techniques
  - They are the ancestors of the **DES** (Data Encryption Standard) symmetric algorithm, very used today (modern technique)

Rotor machines

- Multiple stages of encryption

Key: start of rotor (example: RSC)

Rotor machines

- **Multiple stages of encryption**
  - Each independent cylinder represents an alphabet for substitution
  - Internal wiring connects each (26) input pin to a unique (26) output pin
  - More than one cylinder means "cipher the ciphered"
  - Using *N* cylinders we have 26^n alphabets for substitution before repetitions

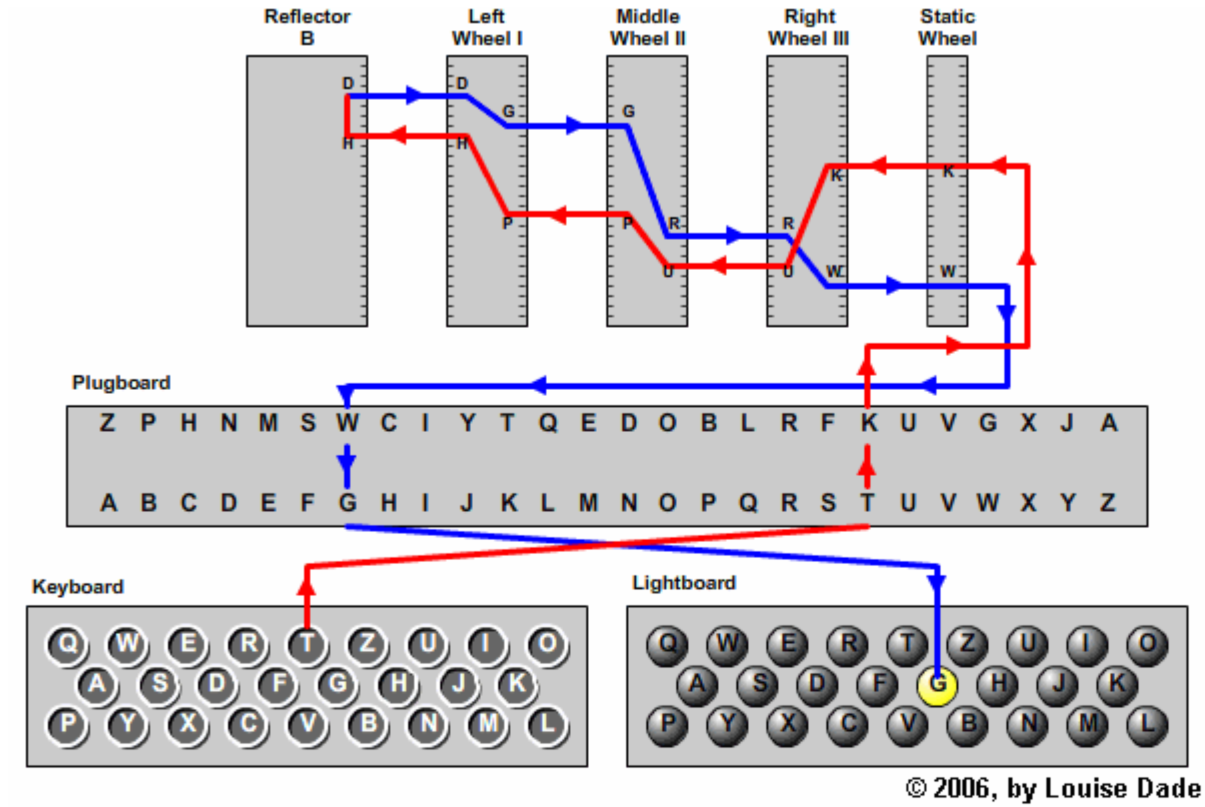
For n=3 we get 17.576

For n=4 we get 456.976

For n=5 we get 11.881.376

Rotor machines (world war II by Germany)

- Multiple stages of encryption



http://enigma.louisedade.co.uk/howitworks.html

Conclusion

- Big achievements
  - XOR operation (Vernam cipher – lightweight and “one way”)
  - “Cipher the ciphered” – rotor machines

Bibliography

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 5th Edition, Prentice Hall, 2010 (Chapter 2).

Note: This presentation is (almost entirely) based on the book [1].
It also uses some adaptations from Prof. Nuno Costa and Vitor Fernandes from previous academic years.