Encryption Algorithms & Protocols

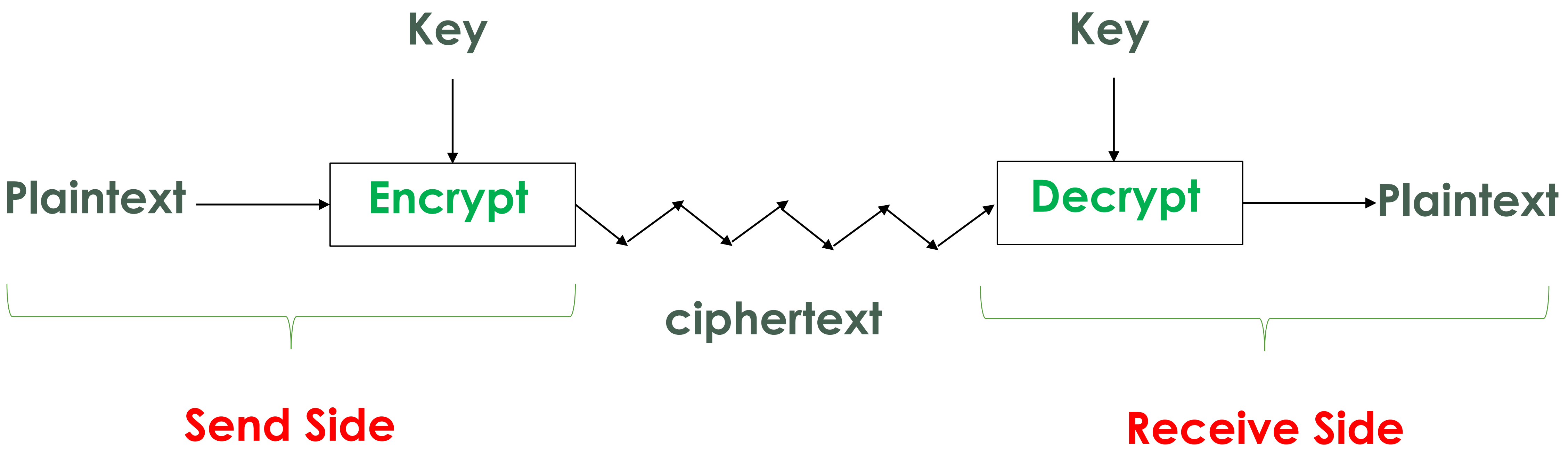
Classical Ciphers

Dr. Omar Abusada
E-mail: abossada1@gmail.com

Classical Ciphers

- Basic Assumptions
  - Only the key is secret
  - The system is completely known to the attacker
  - That is, crypto algorithms are not secret
- This is known as Kerckhoffs' Principle
- 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

Introduction



A generic view of symmetric key crypto

Simple Substitution

- **Caesar's cipher:**
- **Plaintext:** fourscoreandsevenyearsago
- **Key=3**

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:** IRXUVFRUHDQGVHYHQBHDUVDJR

Caesar's Cipher Decryption

- Suppose we know a **Caesar's** cipher is being used. Given Ciphertext as following with Key=3 "Ciphertext, VSRQJHEREVTXDUHSDQWV". Reconstruct the plaintext

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

Simple Substitution

- **Shift by n for some nЄ {0,1,2,3,…………, 25}**
- **Then Key is n**
- **Example Key n=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

Not so Simple Substitution

- A simple substitution (shift by n) is used.
  - But the key is unknown
- Given Ciphertext: CSYEVIXIVQMREXIH
- How to find the key?
- Only 26 possible keys try them all!
  - **Exhaustive key search**, or **brute force attack**
- Solution: key is n = 4

Not Simple Substitution

- In general, simple substitution key can be any permutation of letters
- Not necessarily a shift of the alphabet
- 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

- How to find the Key? … Key might be one of ($26! > 2^{88}$) possible keys!
- 26! =403291461126605635584000000

Does a simple substitution cipher is secure?

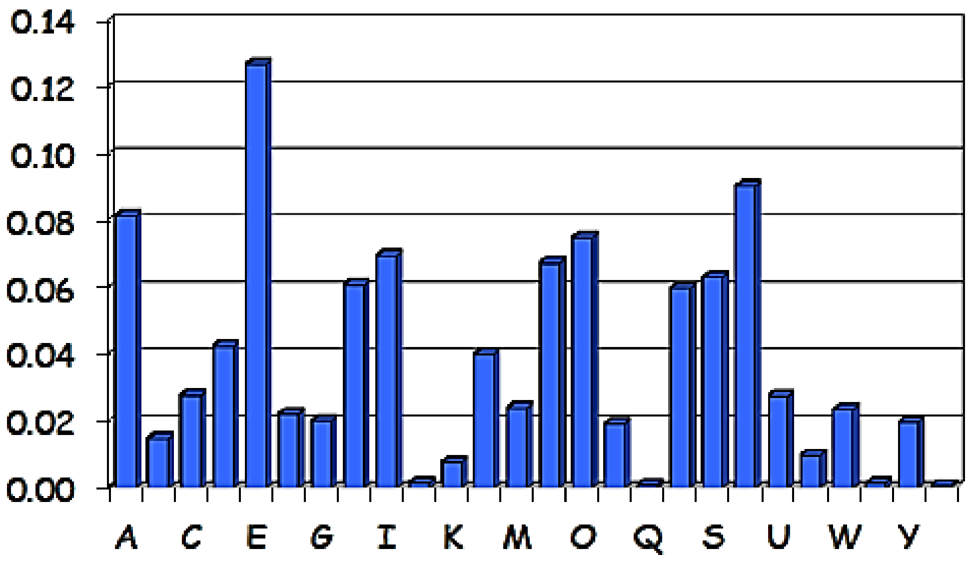
Think Creatively

- Suppose Trudy intercepts the following Ciphertext, and she suspects was produced by a simple substitution cipher, where the key could be any permutation of the alphabet:

PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFX
QWAXBVCXQWAXFQJVWLEQNTOZQGGQLFXQWAKVWLXQWAEBIPBF
XFQVXGTVJVWLBTPQWAEBFPBFHCVLXBQUFEVWLXGDPEQVPQGVPP
BFTIXPFHXZHVFAGFOTHFEFBQUFTDHZBQPOTHXTYFTODXQHFTDPT
OGHFQPBQWAQJJTODXQHFOQPWTBDHHIXQVAPBFZQHCFWPFHPBFI
PBQWKFABVYYDZBOTHPBQPQJTQOTOGHFQAPBFEQJHDXXQVAVXEB
QPEFZBVFOJIWFFACFCCFHQWAUVWFLQHGFXVAFXQHFUFHILTTAV
WAFFAWTEVOITDHFHFQAITIXPFHXAFQHEFZQWGFLVWPTOFFA

Think Creatively

- Trudy cannot try all 2^{88} simple substitution keys
- Can we be more clever?
- English letter frequency counts…
- "E" is the most common letter in the English language.



More about English letter frequency counts

https://www.youtube.com/watch?v=nikWSEjFCWg

Think Creatively

- Going back to Ciphertext and apply Ciphertext frequency counts will end up with:

PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFX
QWAXBVCXQWAXFQJVWLEQNTOZQGGQLFXQWAKVWLXQWAEBIPBF
XFQVXGTVJVWLBTPQWAEBFPBFHCVLXBQUFEVWLXGDPEQVPQGVPP
BFTIXPFHXZHVFAGFOTHFEFBQUFTDHZBQPOTHXTYFTODXQHFTDPT
OGHFQPBQWAQJJTODXQHFOQPWTBDHHIXQVAPBFZQHCFWPFHPBFI
PBQWKFABVYYDZBOTHPBQPQJTQOTOGHFQAPBFEQJHDXXQVAVXEB
QPEFZBVFOJIWFFACFCCFHQWAUVWFLQHGFXVAFXQHFUFHILTTAV
WAFFAWTEVOITDHFHFQAITIXPFHXAFQHEFZQWGFLVWPTOFFA

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
21	26	6	10	12	51	10	25	10	9	3	10	0	1	15	28	42	0	0	27	4	24	22	28	6	8

Transposition Cipher

- Now consider classical transposition or permutation ciphers.
- These hide the message by rearranging the letter order without altering the actual letters used
- Can recognise these since have the same frequency distribution as the original text

Rail Fence Cipher

- Write message letters out diagonally over a number of rows
- Then read off cipher row by row
- Example: Plaintext "MEET ME AFTER THE TOGA PARTY" …. Ciphertext?

M		E		M		A		T		R		H		T		G		P		R		Y
	E		T		E		F		E		T		E		O		A		A		T	

Ciphertext: MEMATRHTGPRYETEFETEOAAT

3 Rail Fence Cipher

Inscribe by a zigzag pattern extract by rows

- Write message letters out diagonally over 3 rows
- Then read off cipher row by row
- Example: Plaintext "WRITHE THE MESSAGE ALTERNATING LETTERS IN THREE ROWS"

…. **Ciphertext?**

W				E				M				A				L				N				G				T				I				R				O		
	R		T		T		E		E		S		G		A		T		R		A		I		L		T		E		S		N		H		E		R		W	
		I				H				S				E				E				T				E				R				T				E				S

Ciphertext: WEMALNGTIRORTTEESGATRAILTESNHERWIHSEETERTES

Double Transposition (Row & Column)

- Key is matrix size and permutations: (3,5,1,4,2) and (1,3,4,2) **(5X4) Matrix**
- Plaintext: **"ENCRYPTION ALGORITHMS"** Ciphertext?

	Col 1	Col 2	Col 3	Col 4
Row 1	E	N	C	R
Row 2	Y	P	T	I
Row 3	O	N	A	L
Row 4	G	O	R	I
Row 5	T	H	M	S

(3,5,1,4,2) →

	Col 1	Col 2	Col 3	Col 4
Row 1	O	N	A	L
Row 2	T	H	M	S
Row 3	E	N	C	R
Row 4	G	O	R	I
Row 5	Y	P	T	I

(1,3,4,2) →

	Col 1	Col 2	Col 3	Col 4
Row 1	O	A	L	N
Row 2	T	M	S	H
Row 3	E	C	R	N
Row 4	G	R	I	O
Row 5	Y	T	I	P

Ciphertext : OALNTMSHECRNGRIOYTIP

One-Time Pad

- **The one-time pad** also known as the **Vernam** cipher.
- For simplicity, let's consider an alphabet with only eight letters. Our alphabet and the corresponding binary representation of letters appear in Table below.

Letter	**e**	**h**	**i**	**k**	**l**	**r**	**s**	**t**
Binary	**000**	**001**	**010**	**011**	**100**	**101**	**110**	**111**

Abbreviated Alphabet

Suppose that Alice, who recently got a job as a spy, wants to use a one-time pad to encrypt the plaintext message **"h e i l h i t l e r"**

One-Time Pad

Letter	e	h	i	k	l	r	s	t
Binary	000	001	010	011	100	101	110	111

- Key is known as 111 101 110 101 111 100 000 101 110 000
- First, Aline converts the plaintext letters to the bit string as following:
- 001 000 010 100 001 010 111 100 000 101 **("h e i l h i t l e r .")**
- The one-time pad key consists of a randomly selected string of bits that is the same length as the message. The key is then XORed with the plaintext to yield the ciphertext.

Encryption: Plaintext ⊕ Key = Ciphertext

Plaintext	**001 000 010 100 001 010 111 100 000 101**
Key	**111 101 110 101 111 100 000 101 110 000**
Ciphertext	**110 101 100 001 110 110 111 001 110 101**
	s r l h s s t h s r

One-Time Pad

- If Aline, wants to decrypt the message then she use the same key with encrypted message.

  Key is known as 111 101 110 101 111 100 000 101 110 000
- **Ciphertext 110 101 100 001 110 110 111 001 110 101**

  s r l h s s t h s r

Decryption: Ciphertext ⊕ Key = Plaintext

	s	r	l	h	s	s	t	h	s	r
Ciphertext	110	101	100	001	110	110	111	001	110	101
Key	111	101	110	101	111	100	000	101	110	000
Plaintext	001	000	010	100	001	010	111	100	000	101
	h	e	i	l	h	i	t	l	e	r

One-Time Pad

- Ciphertext provides no info about plaintext.
- All plaintexts are equally likely but, only when be used correctly.
- Pad (key) must be random, used only once.
- Pad (key) is known only to sender and receiver.
- Note: pad (key) is same size as message.

... Thank you ...