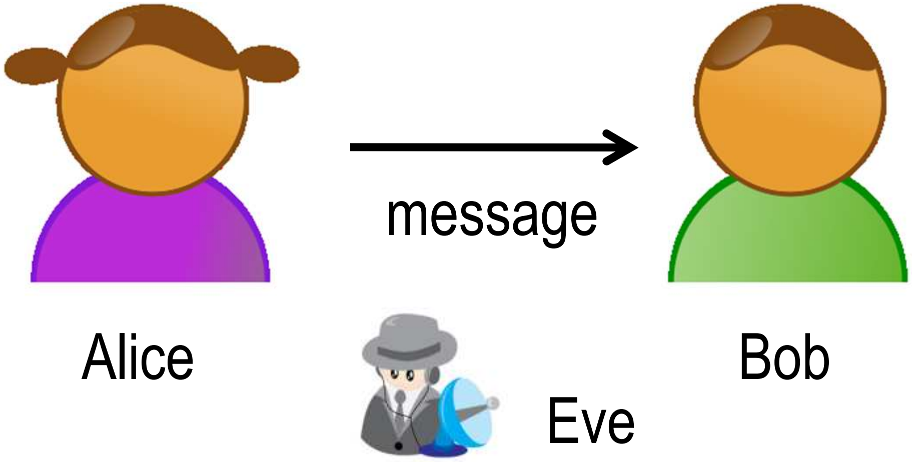
Classical Cryptosystems

Cryptography and Protocols

Andrei Bulatov

Notation



message

Alice

Eve

Bob

Plaintext

Ciphertext

Key

Protocol: (K, E, D)

- K – key generation algorithm
- E – encryption algorithm
- D – decryption algorithm

Three Types of Cryptosystems

- Steganography

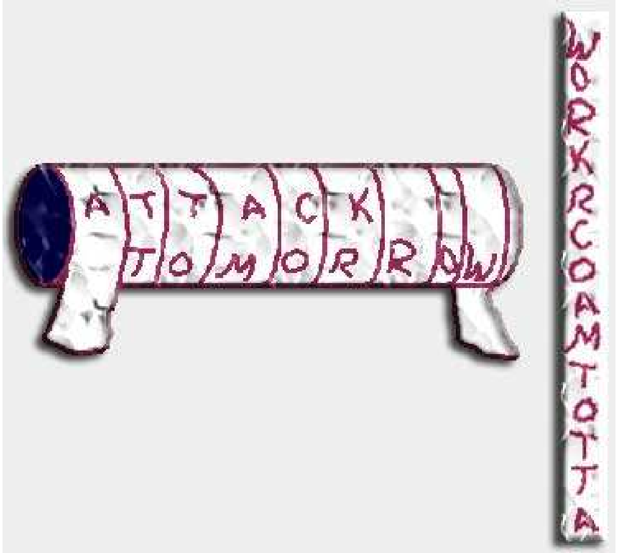
  `Security by obscurity’

- Transposition cryptosystems:

  E permutes (transposes) the letters of plaintext

  D applies the converse transposition

  Example: Spartans Scytale



Three Types of Cryptosystems (cntd)

- Substitution cryptosystems

  E substitutes each letter of the plaintext with another letter or symbol

  D applies the converse substitution

Example: Caesar cipher

He made messages secret by shifting each letter three letters forward.

Thus we can replace letters by integers from 0 to 25.

Then E adds 3 modulo 25 to every letter.

To decrypt a message, D subtracts 3 from each letter

Caesar Cipher

- Encrypt `SEND MORE MEN AND AMUNITION’

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

S E N D M O R E M E N A N D A M U N I T I O N

18 4 13 3 12 14 17 4 12 4 13 0 13 3 0 12 20 13 8 19 8 14 13

21 7 16 6 15 17 20 7 15 7 16 3 16 6 3 15 23 16 11 22 11 17 16

V H Q G P R U H P H Q D Q G D P X Q L W L R Q

Drawbacks of Classical Cryptosystems

- Too few keys

  If the type of the cryptosystem is known it can be bruteforced

- Kerchoff’s Principle:

  System should be secure even if algorithms are known,
  as long as key is secret

- Problem: How to increase the number of keys?

Transposition: Railfence and Redefence Ciphers

- Railfence cipher:

  `SEND MORE MEN AND AMUNITION’

S				**M**				**M**				**N**				**U**				**I**		
	E		D		O		E		E		A		D		M		N		T		O	
		N				R				N				A				I				N

  `SMMNUIEDOEEADMNTONRNAIN’

- Redefence Cipher

2	S				**M**				**M**				**N**				**U**				**I**		
1		E		D		O		E		E		A		D		M		N		T		O	
3			N				R				N				A				I				N

`EDOEEADMNTOSMMNUINRNAIN’

Substitution: Linear Cipher

- Similar to Caesar cipher, but instead of adding 3, computes a linear function on letters. Say,

$$E: \quad X \rightarrow 4X + 21 \pmod{26}$$

Substitution: Playfair

- Keysquare:

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

- Encryption

`SEND MORE MEN AND AMUNITION’

SE ND MO RE ME NA ND AM UN IT IO NA

QF PC TA GK HF SL PC MF NP TH TL SL

`QFPCTAGKHFSLPCMFNPTHTLSL’

Substitution: Checkerboard

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

Plaintext: THIS IS A BETTER CIPHER

Ciphertext: LH AE LI CE LI CE LE AW EW LH LH BW BT BI LI LW AE BW BT

Drawbacks of Classical Cryptosystems

- Frequencies analysis

  Different letters have different probabilities to appear in a text

- Example

Ciphertext:
VXEVWLWXWLRQ
FLSKHUV FDQ
RIWHQ EH EURNHQ
EB IUHTXHQFLHV
DQDOBVLV

Frequencies (in %%):

A	0	6.9	J	0	0.8	S	2	6.8
B	4	0.9	K	2	0.9	T	2	9
C	0	4	L	10	3.9	U	6	2.8
D	6	4.2	M	0	3	V	12	2.1
E	8	13.1	N	2	8	W	8	2.1
F	6	2.7	O	2	8	X	6	1
G	0	2	P	0	2.2	Y	0	2.5
H	14	3	Q	12	1	Z	0	0.8
I	4	7.9	R	6	8.2			

Frequencies Analysis

VXEVWLWXWLRQ FLSKHUV FDQ

RIWHQ EH EURNHQ EB

IUHTXHQFLHV DQDOBVLV

Smoothing Frequencies: Grandpre

	1	2	3	4	5	6	7	8
1	A	B	A	S	H	I	N	G
2	Y	O	K	O	H	A	M	A
3	C	O	E	X	I	S	T	S
4	D	E	A	T	H	F	U	L
5	J	A	C	K	P	O	T	S
6	Q	U	I	V	E	R	E	D
7	W	I	T	C	H	I	N	G
8	Z	O	D	I	A	C	A	L

Plaintext: YOU CANNOT BREAK ME

Ciphertext: 21 22 47 31 11 17 77 24 37 12 66 33 13 23 27 42

Smoothing Frequencies: Vegenere Cipher

Plaintext: SEND MORE MEN AND MUNITION

Key: KEY

Equivalent to shifts by 10 4 24 letters

S E N D M O R E M E N A N D M U N I T I O N

10 4 24

C I L N Q M B I K I L K R B W Y L S X G Y R

$$C_i \equiv P_i + K_{(i \bmod 3)} \pmod{26}$$

Smoothing Frequencies: Vegenere Cipher (cntd)

- Idea: The longer key the better
- Codebooks
- Autokey
- Enigma
- One-time pad