INF 638
Cryptography & Cryptosystems

Section 3: Early Cryptographic Methods

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu

NORTHERN ARIZONA UNIVERSITY

INF 638: Cryptography & Cryptosystems

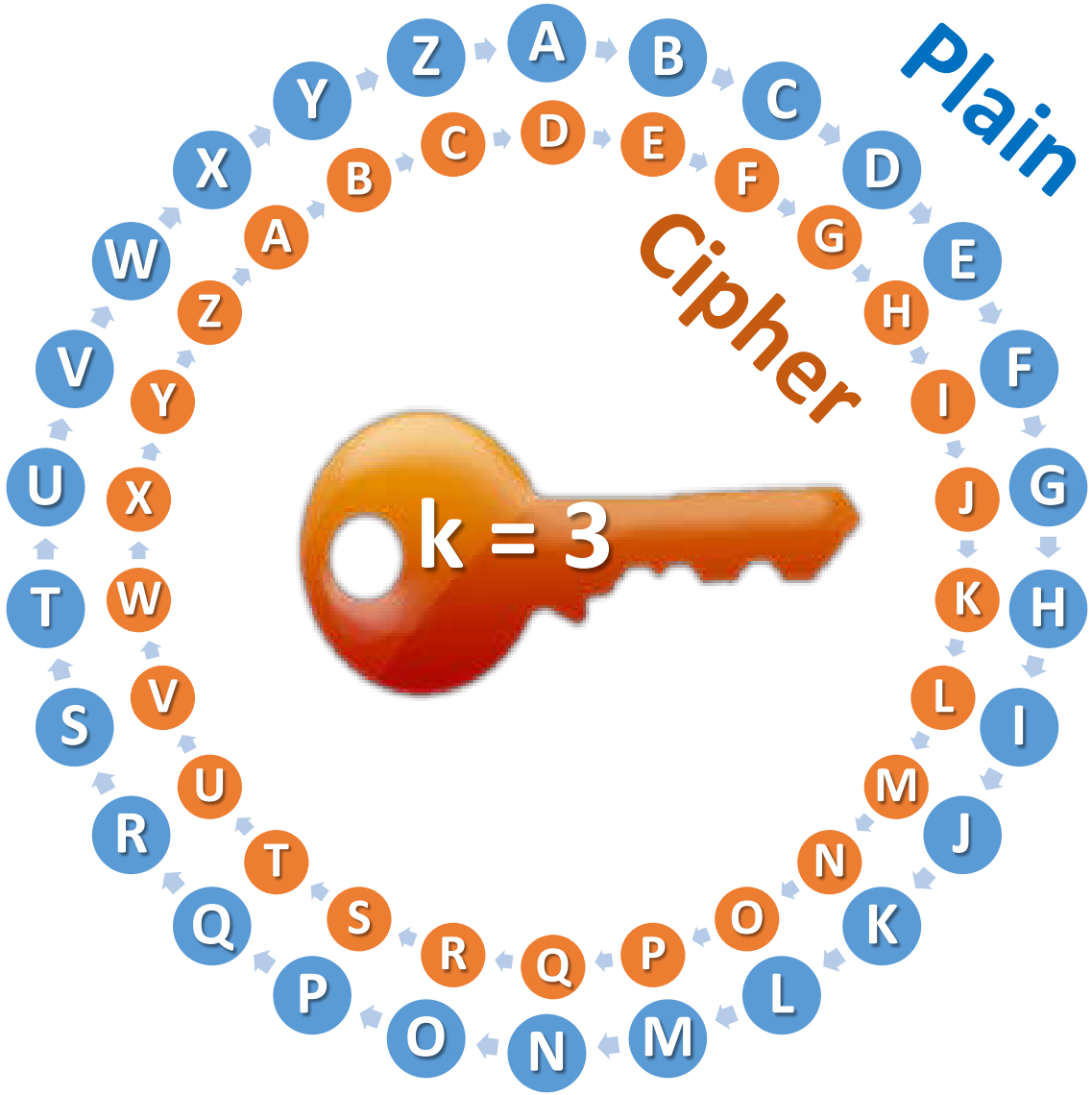
- 1- Motivation & Definitions
- 2- Elements of Number theory
- 3- Early Cryptographic methods
- 4- Symmetrical Cryptography: DES
- 5- Symmetrical Cryptography: AES
- 6- Quantum Cryptography: Key distribution
- 7- Elements of Asymmetrical Cryptography
- 8- Asymmetrical Cryptography: RSA
- 9- ECC Key Distribution
- 10- PKI & Digital Signatures
- 11- Hash Functions
- 12- Smartcards

NORTHERN ARIZONA UNIVERSITY

3-Early Cryptographic methods

- 3-1 Caesar
- 3-2 Vigenere
- 3-3 Transposition
- 3-4 Substitution and Confusion
- 3-5 XOR

Substitution: Caesar cipher

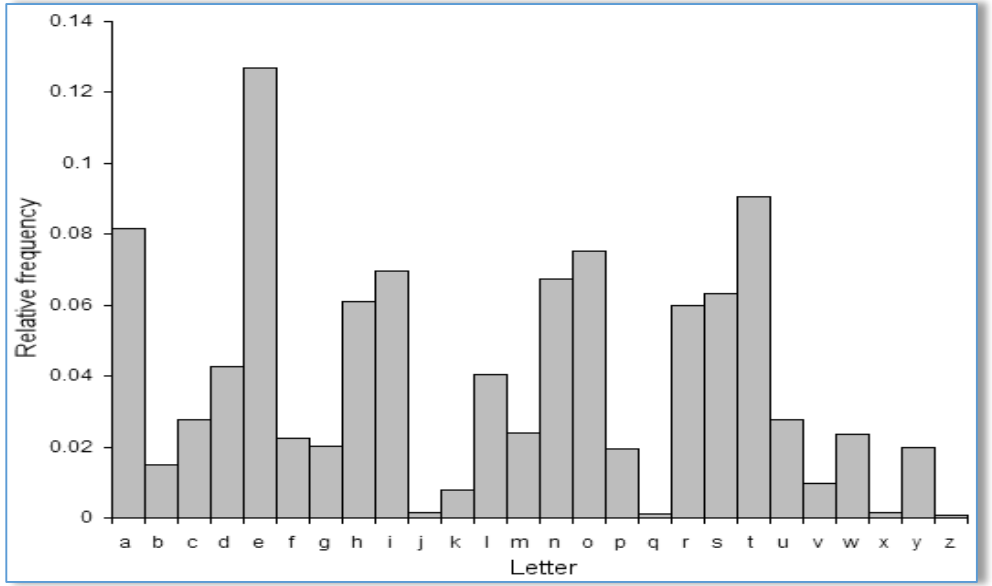


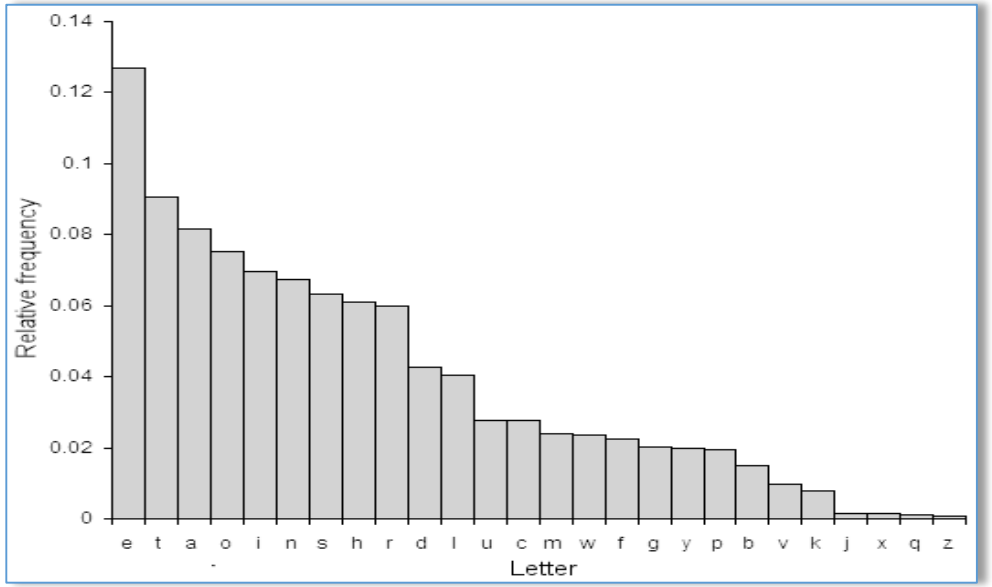
Decrypt Caesar cipher

IURPWKHDULFVLIUZKLFKPHDQCHUR.WKHHXURSHDQPHGL
HYDOPDWKHPDWLFLDQVZHUHZRQIXVHGEBWKHFRQFHS
WRICHURDQGFRPSDUHG

How to improve Caesar cryptography?

Decrypt Caesar with Frequency analysis





Relative frequency of the letters in the English language

NORTHERN ARIZONA UNIVERSITY

3-Early Cryptographic methods

- 3-1 Caesar
- 3-2 Vigenere
- 3-3 Transposition
- 3-4 Substitution and Confusion
- 3-5 XOR

Vigenere Cipher: Complex substitution

Example:

$K_1 = 3$

$K_2 = 17$

$K_3 = 8$

$K_4 = 7$

$K_5 = 1$

(3, 17, 8, 7, 1)

	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
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
K_5 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
K_1 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
K_4 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
K_3 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
K_2 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

Vigenere Cipher: Complex substitution

Example, ***Key:*** $\{K_1=3, K_2=17, K_3=8, K_4=7, K_5=1\}$

Plain	:	“f	r	o	m	t	h	e	a	r	a	b	l	c	s	l	f	r	w	h	i	c	h	m	e	a	n	z	e	r	o”
m	:	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	26	27	28	29	30
h	:	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
K_h	:	3	17	8	7	1	3	17	8	7	1	3	17	8	7	1	3	17	8	7	1	3	17	8	7	1	3	17	8	7	1

Cipher:???

Crypto-analysis Vigenere Cipher

NORTHERN ARIZONA UNIVERSITY

3-Early Cryptographic methods

- 3-1 Caesar
- 3-2 Vigenere
- 3-3 Transposition
- 3-4 Substitution and Confusion
- 3-5 XOR

Transposition Ciphers

Change the order of the plain text

"Please help me now"

"We are discovered – Flee at once"

Example #1

P H N
L E E E O
E S L M W
A P

Ciphertext: PHNLE EEOES LMWAP

Example #2

W R I O R F E O E
E E S V E L A N
A D C E D E T C

The message:

WRIORFEOEEESVELANADCEDETC.

NORTHERN ARIZONA UNIVERSITY

3-Early Cryptographic methods

- 3-1 Caesar
- 3-2 Vigenere
- 3-3 Transposition
- 3-4 Substitution and Confusion
- 3-5 XOR

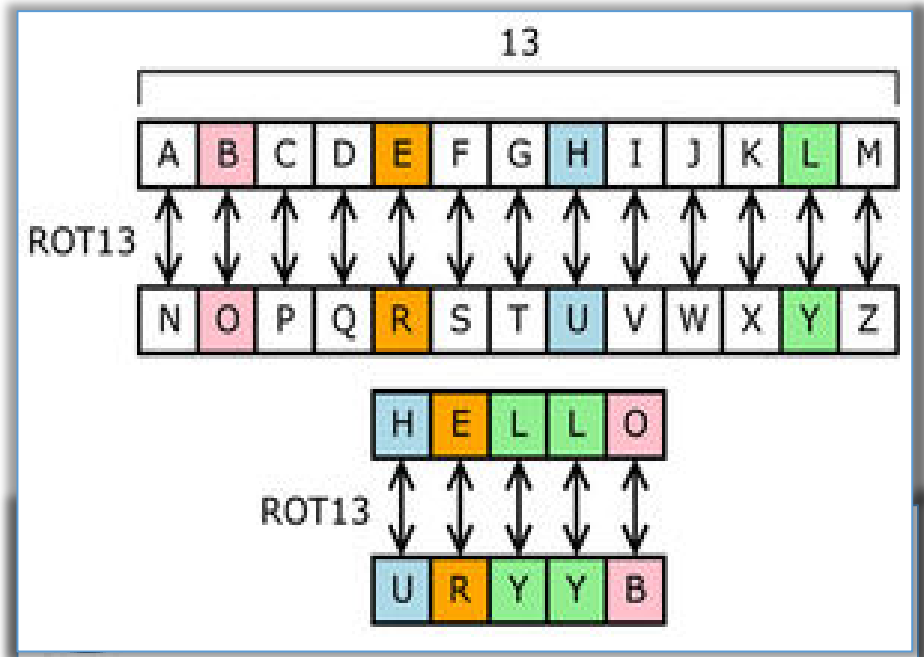
Diffusion & confusion ciphers

Diffuse

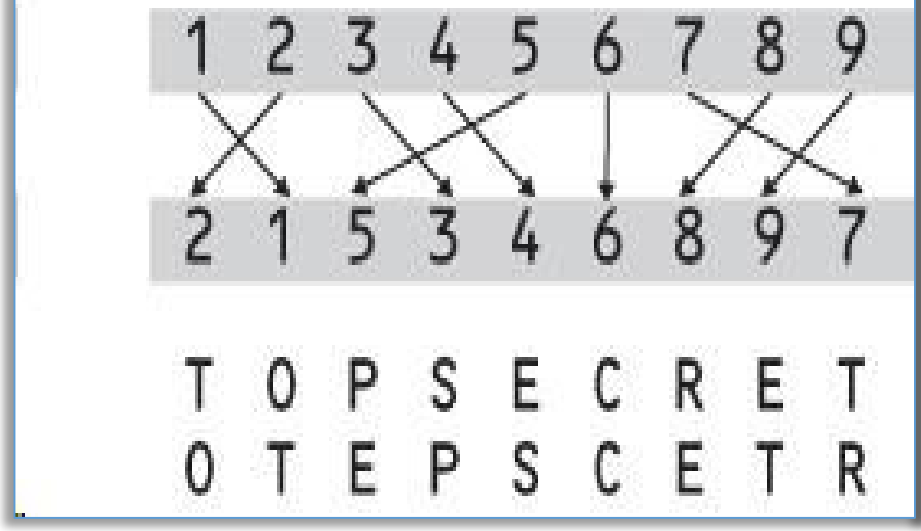
Substitution & Transposition

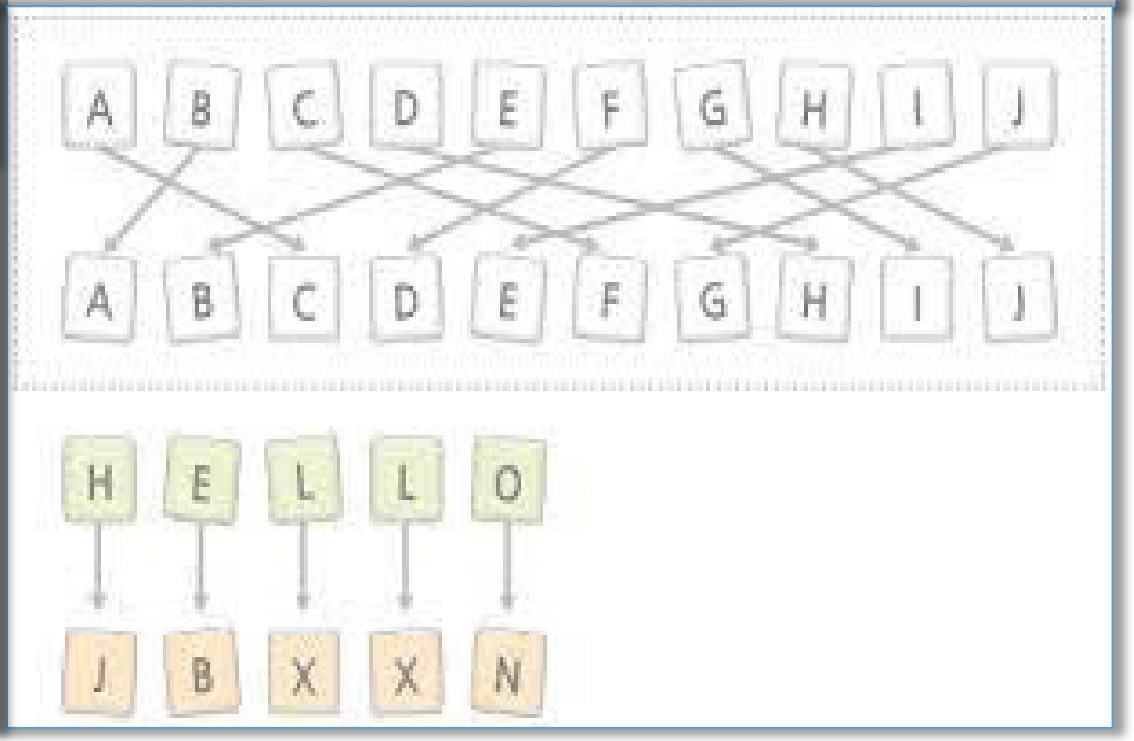
Confuse

Successive diffusions



INPUT	000	001	010	011	100	101	110	111
OUTPUT	010	111	000	110	100	001	011	101





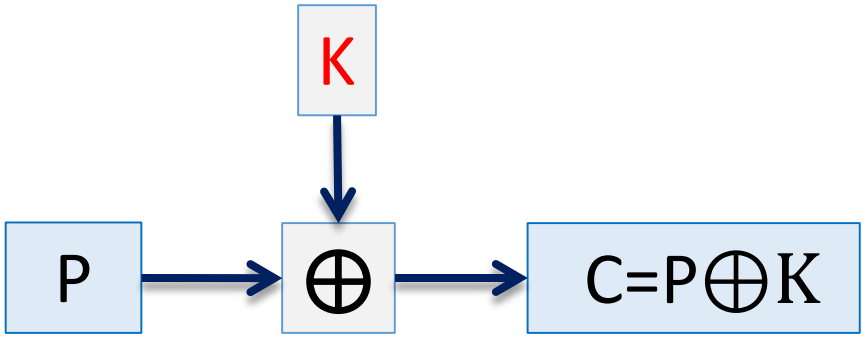
NORTHERN ARIZONA UNIVERSITY

3-Early Cryptographic methods

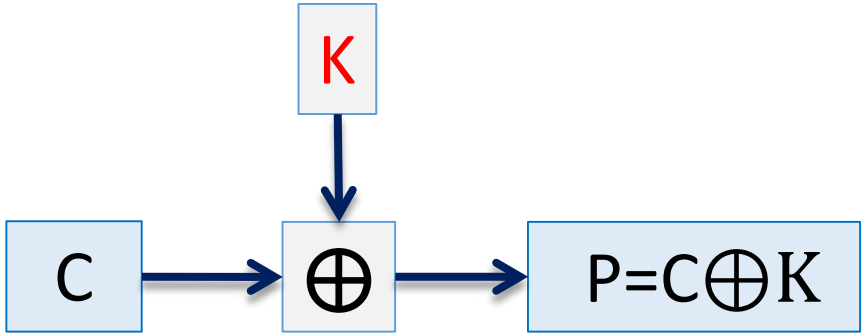
- 3-1 Caesar
- 3-2 Vigenere
- 3-3 Transposition
- 3-4 Substitution and Confusion
- 3-5 XOR

Symmetrical Ciphers: XOR function

Encryption



Decryption



Cryptoanalysis of XOR ciphers

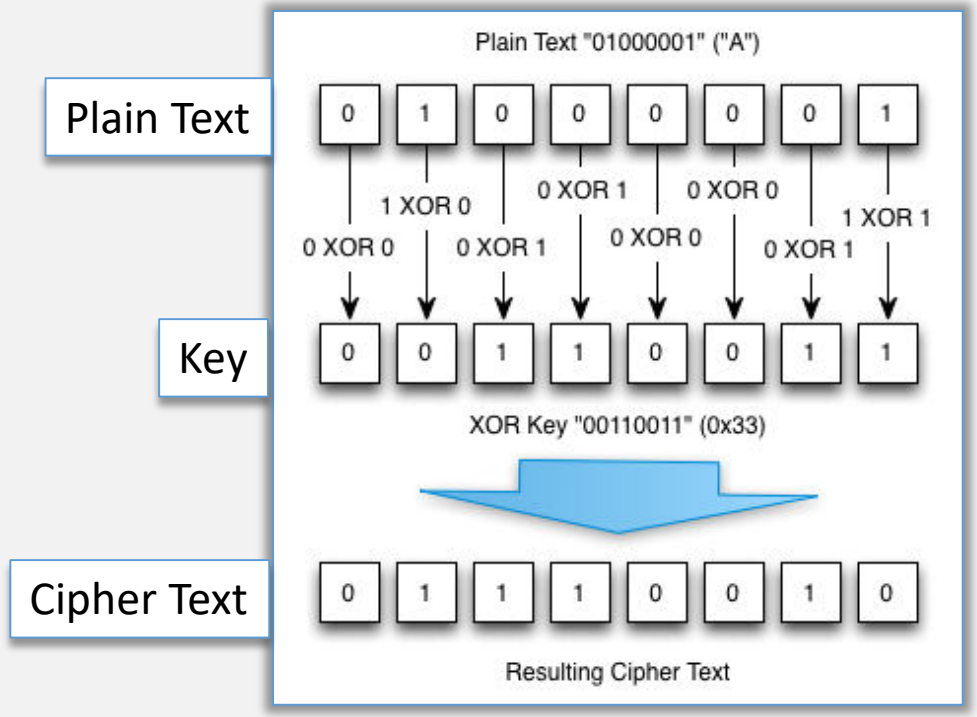
Symmetrical Ciphers: XOR & ASCII

Conversion table: ASCII

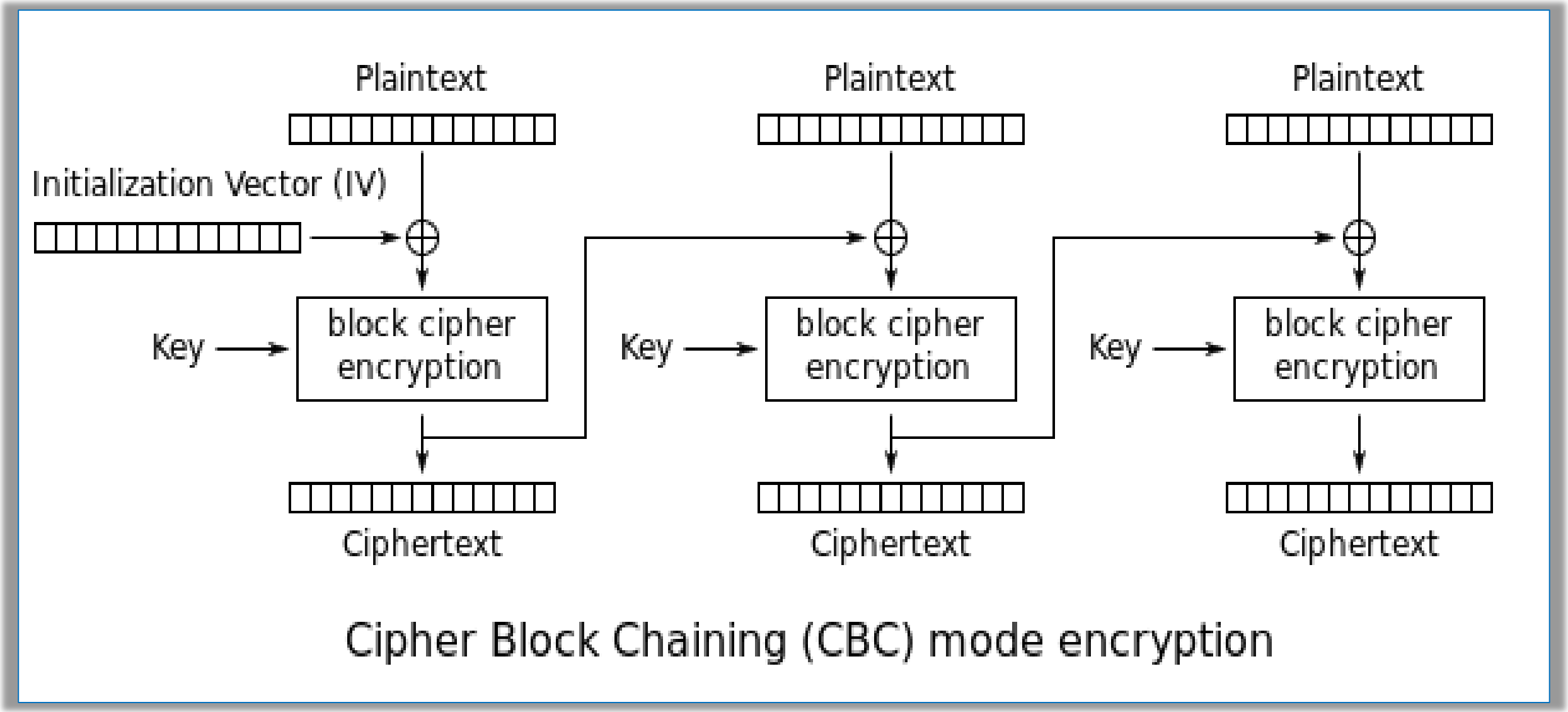
Binary	Hex	Decimal	Character
1000000	40	64	@
1000001	41	65	A
1000010	42	66	B
1000011	43	67	C
1000100	44	68	D
1000101	45	69	E
1000110	46	70	F
1000111	47	71	G
1001000	48	72	H
1001001	49	73	I
1001010	4A	74	J
1001011	4B	75	K
1001100	4C	76	L
1001101	4D	77	M
1001110	4E	78	N
1001111	4F	79	O
1010000	50	80	P
1010001	51	81	Q
1010010	52	82	R
1010011	53	83	S
1010100	54	84	T
1010101	55	85	U
1010110	56	86	V
1010111	57	87	W
1011000	58	88	X
1011001	59	89	Y
1011010	5A	90	Z
1011011	5B	91	[
1011100	5C	92	\
1011101	5D	93	]
1011110	5E	94	^
1011111	5F	95	_

Binary	Hex	Decimal	Character
1100000	60	96	`
1100001	61	97	a
1100010	62	98	b
1100011	63	99	c
1100100	64	100	d
1100101	65	101	e
1100110	66	102	f
1100111	67	103	g
1101000	68	104	h
1101001	69	105	i
1101010	6A	106	j
1101011	6B	107	k
1101100	6C	108	l
1101101	6D	109	m
1101110	6E	110	n
1101111	6F	111	o
1110000	70	112	p
1110001	71	113	q
1110010	72	114	r
1110011	73	115	s
1110100	74	116	t
1110101	75	117	u
1110110	76	118	v
1110111	77	119	w
1111000	78	120	x
1111001	79	121	y
1111010	7A	122	z
1111011	7B	123	{
1111100	7C	124	|
1111101	7D	125	}
1111110	7E	126	~
1111111	7F	127	

Ex: ASCII XOR encryption



Symmetrical Ciphers: XOR & CBC



Cipher Block Chaining (CBC) mode encryption

Number of events versus key size

Reference	Key Size n	2^n	Magnitude
	8	256	
	16	$6.5\ 10^4$	
Second in a year			$3\ 10^7$
	32	$4.2\ 10^9$	
	56 (DES)	$7.2\ 10^{16}$	
Seconds since creation of solar system			$2\ 10^{17}$
	64	$1.8\ 10^{19}$	
	128 (AES)	$3.4\ 10^{38}$	
	192 (AES)	$6.2\ 10^{57}$	
Number of 75-digit prime numbers			$5.2\ 10^{72}$
	256 (AES)	$1.1\ 10^{77}$	
Electrons in universe			$8.3\ 10^{77}$

Key length versus time to crack the code

Key Size n Bits	Number of keys: 2^n	Time to crack at 1 encryption / µs	Time to crack at 10^6 encryption / µs
32	$4.2\ 10^9$	2^{31} µs = 36 minutes	2 milliseconds
56	$7.2\ 10^{16}$	2^{55} µs = 1142 years	10 hours
128	$3.4\ 10^{38}$	2^{127} µs = $5\ 10^{24}$ years	$5\ 10^{18}$ years
256	$1.1\ 10^{77}$	2^{247} µs = $1\ 10^{64}$ years	$1\ 10^{56}$ years

QUESTIONS ?

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu