

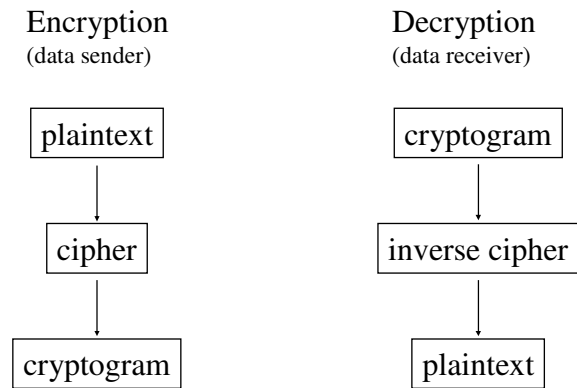
Cryptography

David Morgan

Functional purposes of cryptography

- Confidentiality
 - ensuring illegibility to outsiders
- Authentication
 - ensuring ostensible and actual sender are one and the same
- Data integrity
 - ensuring non-alteration in transit

Cryptographic processing



Crypto system classification

- Type of transformation operations
- Number of keys employed
- “at-a-time” elements processed

Crypto system classification

- transformation types
 - substitution
 - permutation
- key quantities
 - one
 - two
- element quantities per operation
 - one of them at a time
 - a block of them at a time

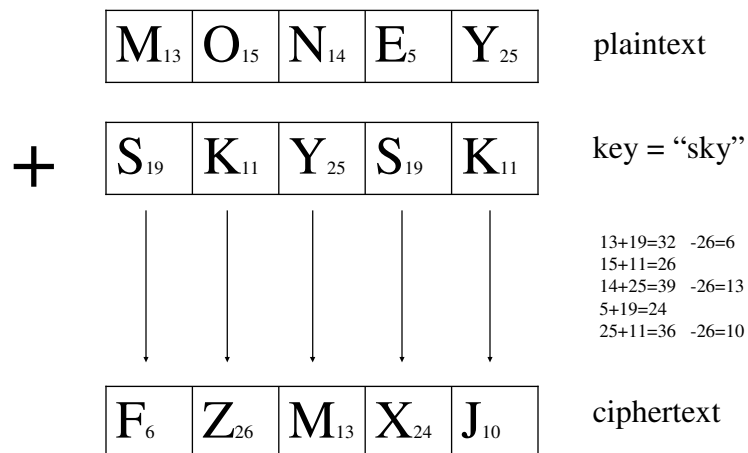
Type of transformation

- Substitution
 - alters identity of element
 - “substitution” becomes “tvctujuvujpo”
- Permutation (= transposition)
 - alters position of element
 - “permutation” becomes “urontempita”

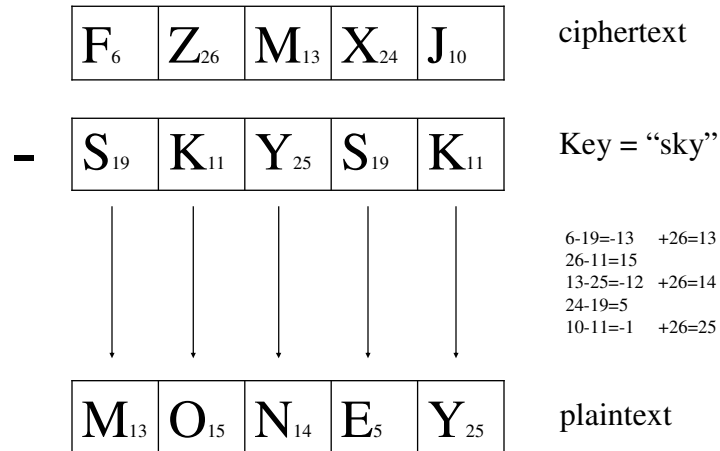
A substitution: Caesar cipher

- letter \leftarrow letter + 3
plain: a b c d . . . w x y z
cipher: d e f g . . . z a b c
- $C = E(p) = (p+3) \bmod (26)$
- meet me after the toga party \leftarrow
phhw ph diwhu wkh wrjd sduwb

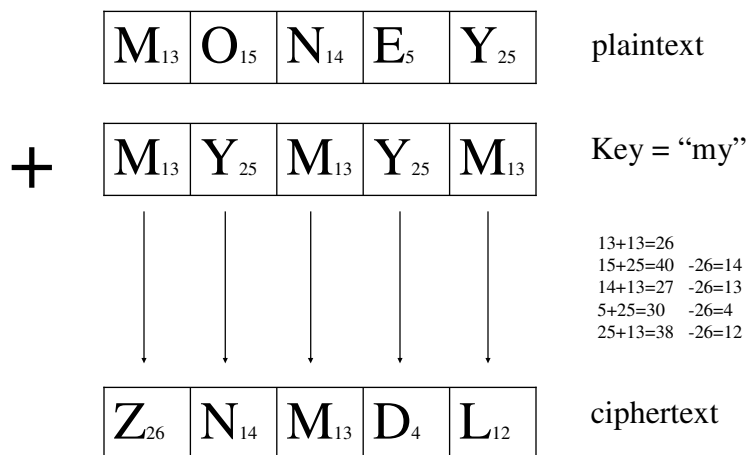
A substitution - encryption



A substitution - decryption



Ciphertext is key-dependent



not FZMXJ

A characterwise permutation

plaintext: meetmeafterthetogaparty

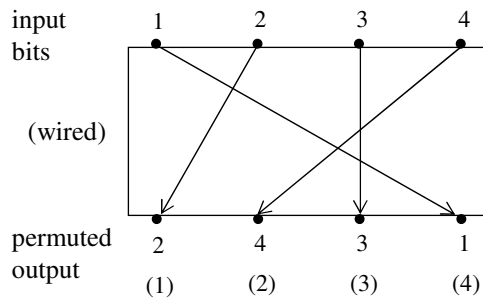
key:	4	3	1	2	5	6	7
plaintext:	m	e	e	t	m	e	a
	f	t	e	r	t	h	e
	t	o	g	a	p	a	r
	t	y	a	b	c	d	e

ciphertext: eegatrabetoymftmtpcchadaere

A bitwise permutation

P			
2	4	3	1

or



e.g.,

0001 → 0100

1010 → 0011

1101 → 1101

Number of keys

- Conventional cryptography
 - One
 - 1000 B.C. to present
- Public-key cryptography
 - Two
 - 1976 A.D. to present

Known synonymously as:

- | | |
|------------------|--------------------|
| ● One technology | ● Versus the other |
| – single-key | – dual-key |
| – private-key | – public-key |
| – symmetric | – asymmetric |
| – secret-key | |
| – shared-key | |
| – conventional | |

Key usage, per technology

Which key encrypts?

Which key decrypts?

secret

the only key!

the only key!

public

the public key

the private key

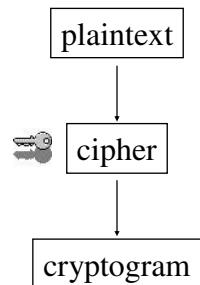
!!-OR-!!

the private key

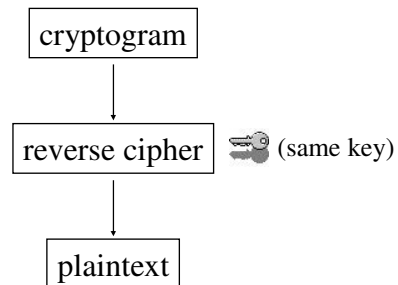
the public key

Keys: conventional crypto

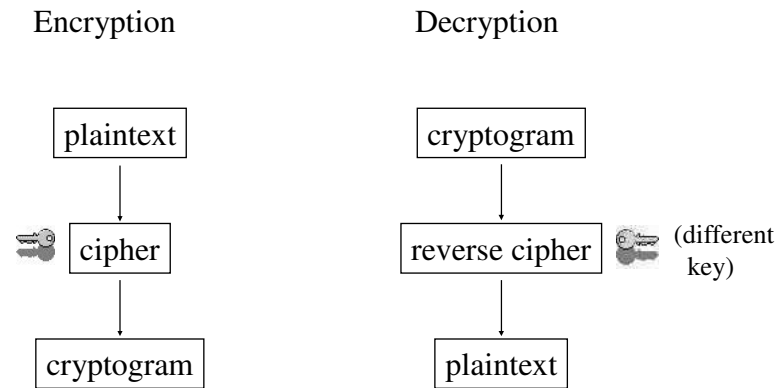
Encryption



Decryption



Keys: public-key crypto



“at-a-time” elements processed

- Block cipher
 - block (multiple elements) at a time
 - one output block per input block
 - predominant
- Stream cipher
 - one element at a time
 - continuous processing
 - rare

Blocking data

- RED APPLE = 826968326580807669
- Assume 3-decimal-digit blocksize
- Separately encrypt:
826 968 326 580 807 669

ASCII Alphabet Characters

Symbol	Decimal	Binary
A	65	01000001
B	66	01000010
C	67	01000011
D	68	01000100
E	69	01000101
F	70	01000110
G	71	01000111
H	72	01001000
I	73	01001001
J	74	01001010
K	75	01001011
L	76	01001100
M	77	01001101
N	78	01001110
O	79	01001111
P	80	01010000
Q	81	01010001
R	82	01010010
S	83	01010011
T	84	01010100
U	85	01010101
V	86	01010110
W	87	01010111
X	88	01011000
Y	89	01011001
Z	90	01011010

Blocking data

- ABC = 010000010100001001000011
- Assume 12-bit blocksize
- Separately encrypt:
010000010100 001001000011

ASCII Alphabet Characters

Symbol	Decimal	Binary
A	65	01000001
B	66	01000010
C	67	01000011
D	68	01000100
E	69	01000101
F	70	01000110
G	71	01000111
H	72	01001000
I	73	01001001
J	74	01001010
K	75	01001011
L	76	01001100
M	77	01001101
N	78	01001110
O	79	01001111
P	80	01010000
Q	81	01010001
R	82	01010010
S	83	01010011
T	84	01010100
U	85	01010101
V	86	01010110
W	87	01010111
X	88	01011000
Y	89	01011001
Z	90	01011010

Mathematically speaking...

- Encryption

$$Y = E_k(X)$$

- Decryption

$$X = D_k(Y)$$

X = plaintext Y = ciphertext

k = key

E_k/D_k = key-dependent en/decryption ciphers

Cryptanalysis-- cracking

- Attempt to discover X or K , given...
- Difficulty depends on what's given
 - encryption algorithm
 - ciphertext to be decoded
 - matching samples of plain/cipher texts

Degree of security

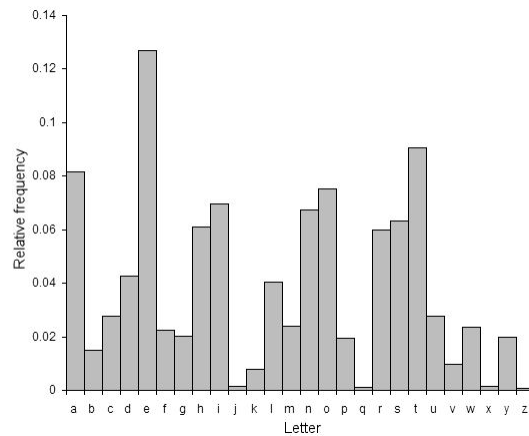
- Unconditional security
 - sufficient information to decrypt does not exist within ciphertext
 - only 1 such cipher
- Computational security
 - sufficient information does reside in ciphertext
 - nevertheless impracticable
 - cracking cost exceeds info's value
 - cracking time exceeds info's useful life

Demo –

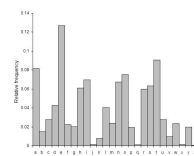
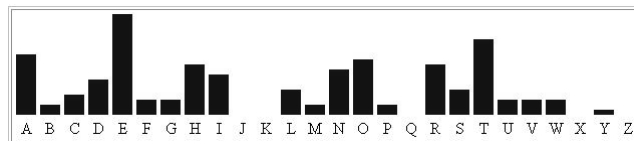
trying to thwart frequency analysis

- plain text exhibits letter frequency patterns
- monoalphabetic substitution preserves patterns
- polyalphabetic substitution destroys them

Occurrence of English letters



Occurrence of letters: Gettysburg address

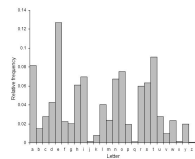


<http://www.mtholyoke.edu/courses/quenell/s2002/crypto/js/count.html>

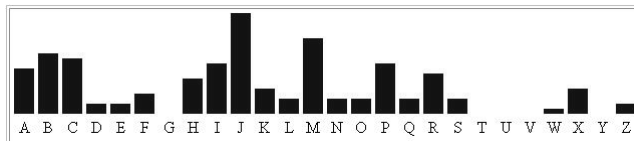
Occurrence of letters: Gettysburg address thru (monoalphabetic) Caesar cipher



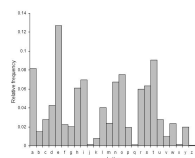
Letters changed but statistical pattern preserved



Occurrence of letters: Gettysburg address thru differently sequenced* monoalphabetic cipher



*the substitution mapping, unlike that of Caesar cipher, doesn't preserve the letters in the same sequence as that of the alphabet. They're all there, but in reassigned positions.
 This mapping was: bdfhjlnprtvxzacegikmqosuwy
 e became j, t became m, etc
 (seen in both the mapping and the chart)

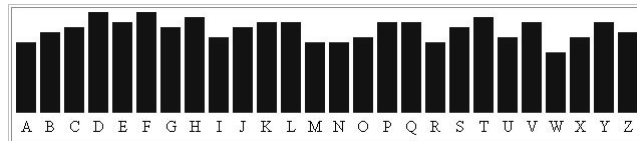


Polyalphabetic ciphering*

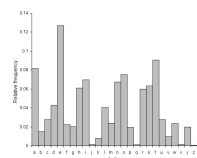
*use many alphabets
 Different ones for determining
 what to substitute for each
 letter in the plaintext. Without
 resequencing the letters, there
 are 25 other alphabets readily
 available.

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

Occurrence of letters: Gettysburg address thru polyalphabetic cipher



Letters changed and statistical pattern destroyed



Ciphers of interest

- Secret-key ciphers
 - Japanese naval code JN-25
 - Digital Encryption Standard (DES)
- Public-key ciphers
 - Rivest-Shamir-Adelman (RSA)