A BEGINNER'S GUIDE TO CRYPTOGRAPHY

AESTETIX

OCT 14

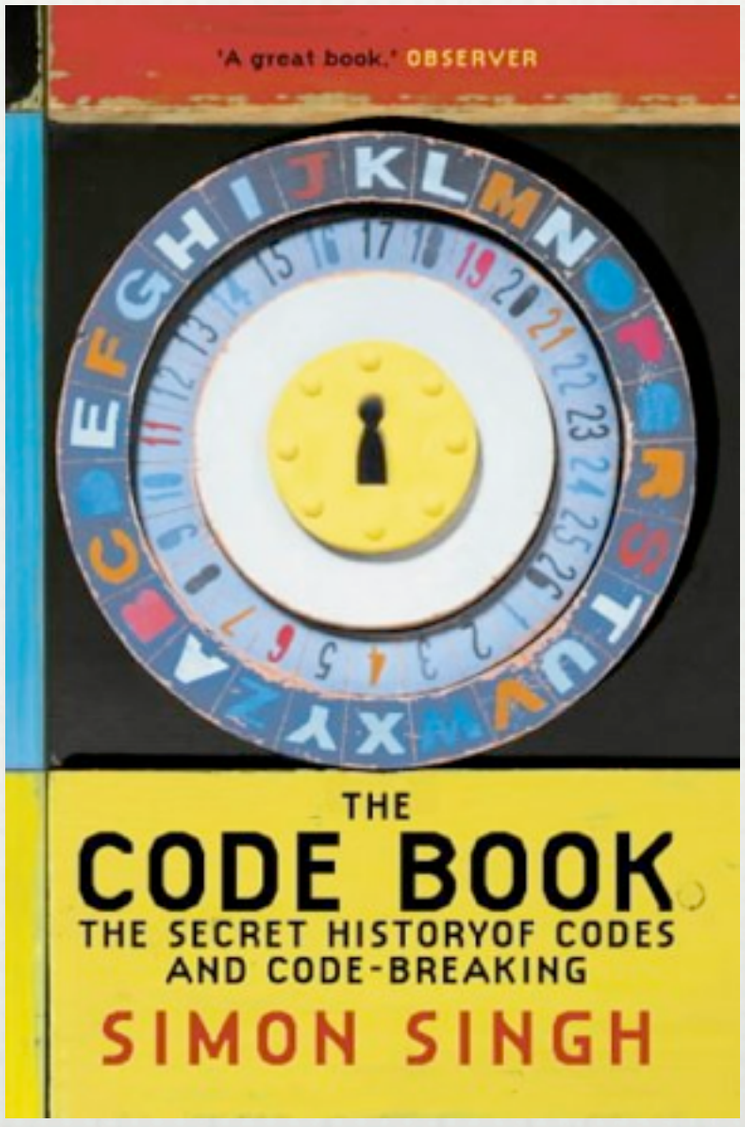
OAKLAND #CRYPTOPARTY @TECH LIMINAL

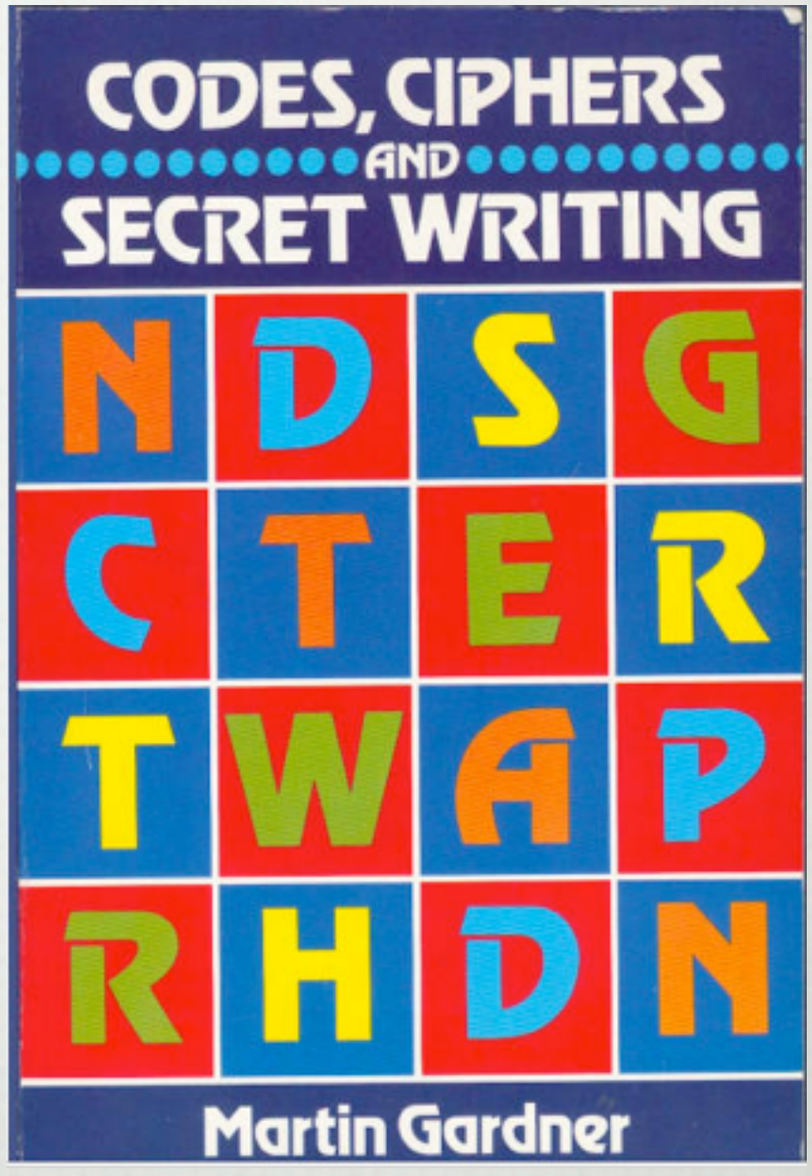
DEFINITIONS

- ☐ CRYPTOGRAPHY
- ☐ CRYPTANALYSIS
- ☐ CRYPTOLOGY
- ☐ STEGANOGRAPHY

CODES AND CIPHERS

- [ ] CODES
- [ ] CIPHERS





EXAMPLE OF A CODE

Evauk Will you meet me there?
Evayo Will you meet us there?
Evboy
Evbew
Evcat
Evcex
Evcib

MISCELLANEOUS

Ewaxo A further amount (of) .....
Ewbum A matter of great importance.
Exabu A trouble has risen about.
Exafy Able to be .....
Exaha About the same.
Exapi Absolutely necessary.
Exawo Absolutely necessary you should.
Exbey Absolutely no truth in the report.
Exbic Accept on condition that .....
Excav According to agreement.
Excez According to instructions.
Excid According to news received here.
Exdaw Acknowledge receipt of this by mail.
Exdok Act according to instructions.
Exdup Act according to instructions contained in letter (dated .....).
Exeda Act according to instructions contained in telegram (cable) dated .....
Exeso Act as you consider best.
Exfay Act cautiously.
Exfec Act cautiously, but quickly.
Exfig Act only under legal advice.
Exfom Act quickly.
Exfus Act upon instructions from .....
Eybez Acting under instructions from .....
Eybid Acting under legal advice.
Eycaw Acting under your instructions.
Eycok Action taken.
Eycup Advance at once.
Eydax Advance continues.
Eydeb Advance generally expected.
Eydif Advise all concerned.
Eydol Advise at once.
Eydur Advise you strongly to .....
Eyfaz Advise you to .....
Eyfed Advise you to attend to the matter at once.
Eyfon Advise you to accept.

Eyfut Advise you to call on .....
Ezady Advise you to come here.
Ezafa Advise you not to .....
Ezani Advise you not to accept.
Ezbaw Advise you not to do it.
Ezbie Affairs in bad shape.
Ezbok Affairs in good shape.
Ezbup Affairs very unsettled.
Ezcax Affidavit will be required.
Ezceb After all.
Ezcif After he (she) has.
Ezcol After I (we) have.
Ezcur After that date.
Ezdec After what has been done.
Ezdig After what has taken place.
Ezdom After you (they) have.
Ezdro After you have seen them.
Ezdus Agree to the proposal.
Fabmi Agree with them if possible.
Fabok Aid them all you can.
Fabup All goes well.
Facax Always the same.
Facby Am able to .....
Facda Am acting under legal advice.
Faceb Am alone. Where can I meet you?
Fache Am coming over.
Facif Am not coming over.
Facli Am not coming over at present.
Facol Am not quite .....
Facso Am not quite sure.
Facur Am unable to .....
Faday Am unable to decide.
Fadca Am unable to decide what to do.
Fadec Am very anxious to hear (about .....).
Fadig Am very anxious to hear from .....
Fadki Am very anxious to hear from you.
Fadom American Ambassador (at .....).
Fadro American Consul (at .....).
Fadus American Embassy (at .....).
Fagab American Legation (at .....).
Fagef American Minister (at .....).
Fagij An accident, not serious, has occurred.
Fibim An accident, quite serious has occurred.
Fibot An accident, very serious has occurred.
Ficaf And perhaps not then.
Ficuz And thence to .....
Fidag Answer at once.

HTTP://ATLANTIC-CABLE.COM/CABLECOS/WESTERNUNION/INDEX.HTM

EXAMPLE OF A CIPHER

- **BS NYY GUR GUVATF V'IR YBFG, V ZVFF ZL ZVAQ GUR ZBFG.**
  - **BMML BFOBHEAR**

EXAMPLE OF A CIPHER

□

OF ALL THE THINGS I'VE LOST, I MISS MY MIND THE MOST.

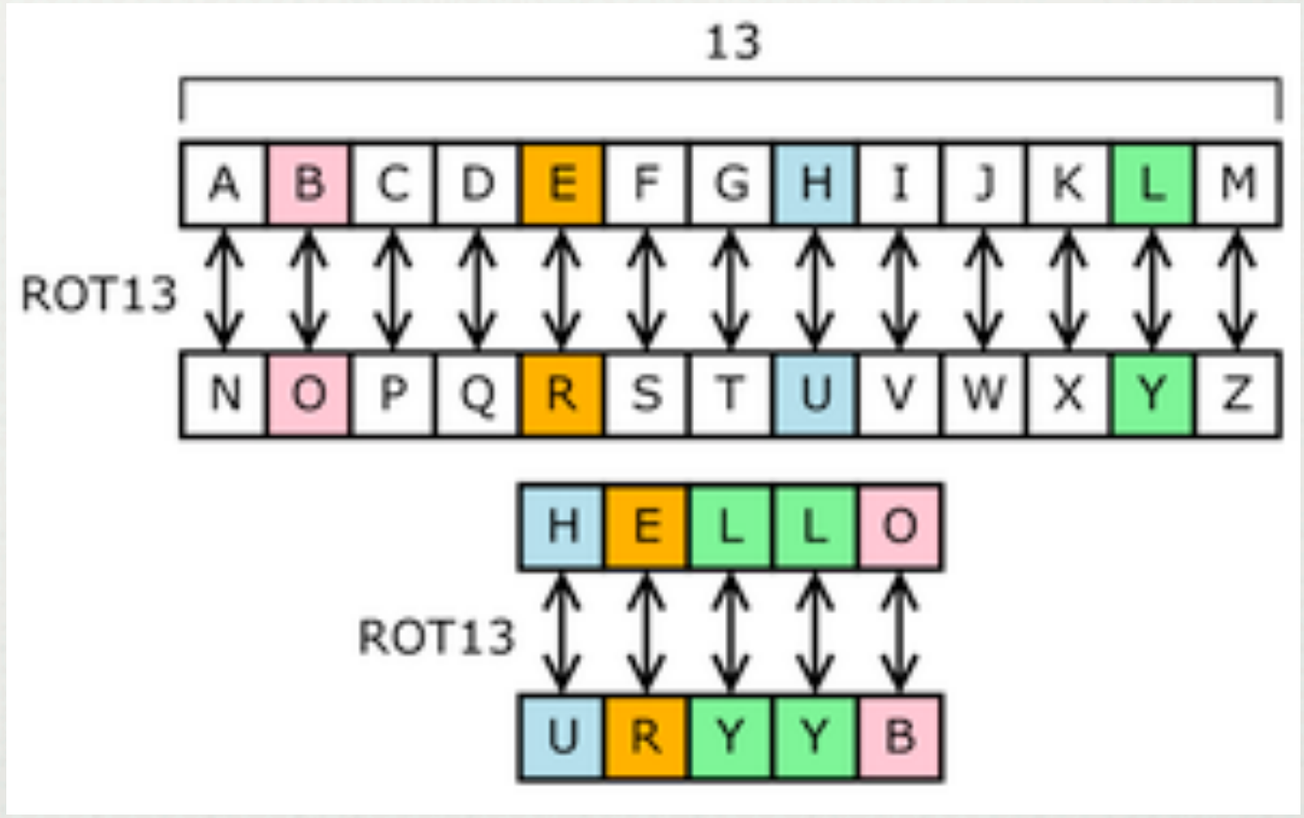
– OZZY OSBOURNE

DEFINITIONS

- [ ] PLAINTEXT (CLEARTEXT)
- [ ] CIPHERTEXT
- [ ] KEY
- [ ] CRYPTOSYSTEM
- [ ] KERCKHOFF'S PRINCIPLE

TYPES OF SUBSTITUTION CIPHERS

- ☐ ROT13
- ☐ CAESAR CIPHER
- ☐ CRYPTO-GRAMS
- ☐ "MONALPHABETIC"



HTTP://EN.WIKIPEDIA.ORG/WIKI/FILE:ROT13.PNG

MONALPHABETIC CIPHERS

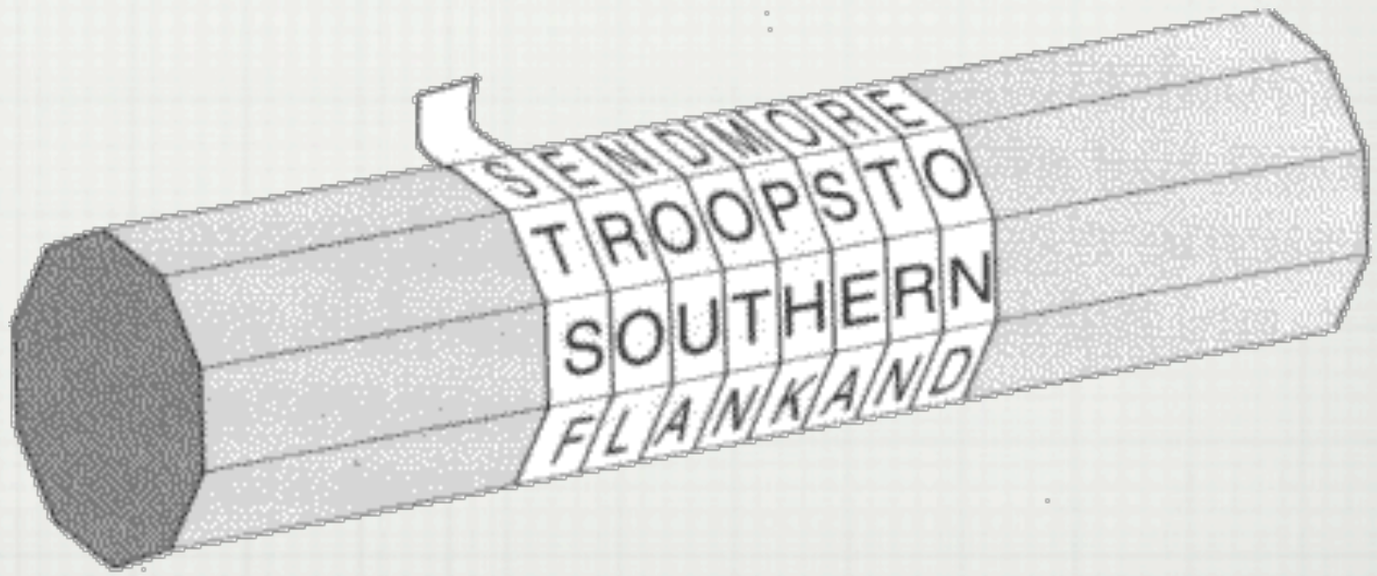
- [ ] FREQUENCY ANALYSIS
- [ ] STRUCTURE OF THE CIPHERTEXT
- [ ] CONTEXT
- [ ] COMPARISON TO OTHER CIPHERTEXTS

EXAMPLE OF A CIPHER

- **BS NYY GUR GUVATF V'IR YBFG, V ZVFF ZL ZVAQ GUR ZBFG.**
  - **BMML BFOBHEAR**

TRANSPOSITION CIPHERS

- [ ] SCYTALE
- [ ] KRYPTOS K3



HTTP://MAIL.COLONIAL.NET/~ABECKWITH/F0V1-0004FCD4/S00FB0FF5-036322DF

POLYALPHABETIC CIPHERS

- TRITHEMIUS
  - 1ST BOOK ON CRYPTO
- ALBERTI - CIPHER WHEEL
- BLAISE DE VIGENERE

	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

HTTP://WWW.CS.TRINCOLL.EDU/~CRYPTO/HISTORICAL/ALBERTI.HTML

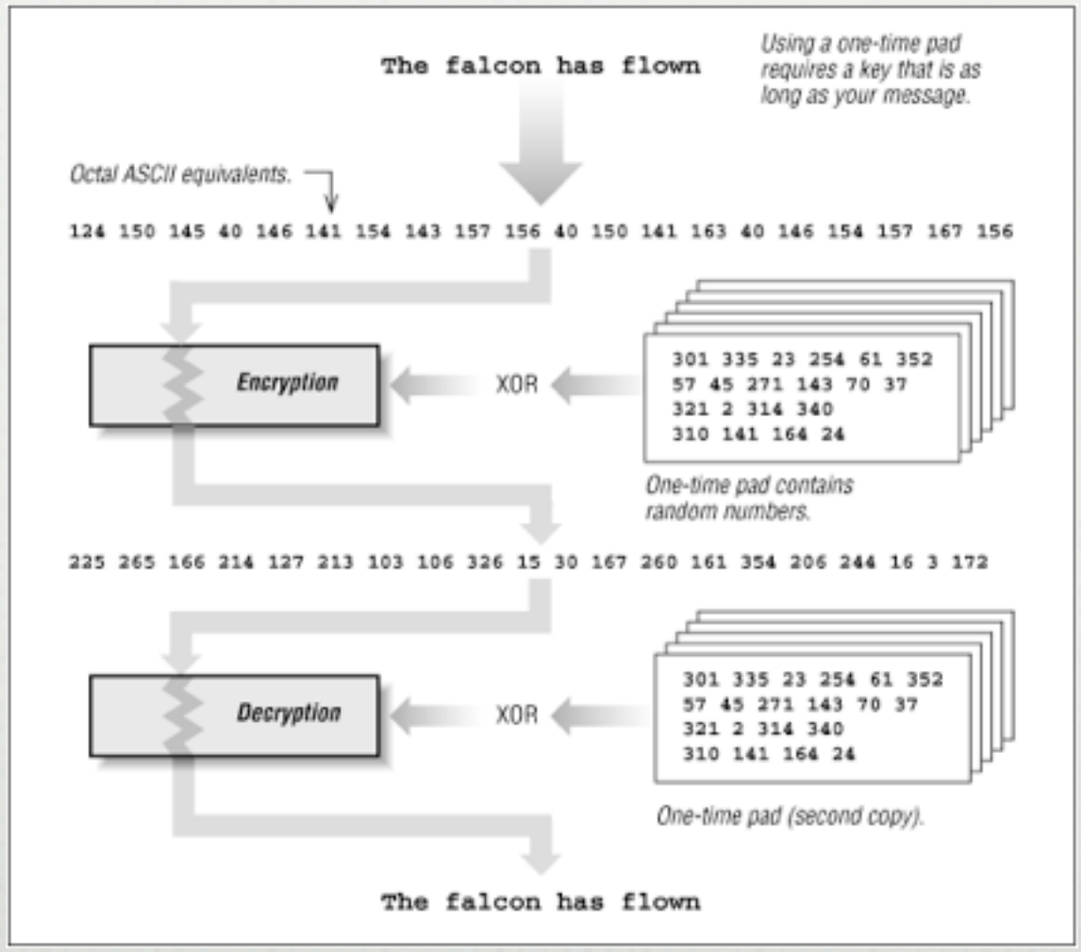
HTTP://CARREZ.CHRISTOPHE.PAGESPERSO-ORANGE.FR/CODE_VIGENERE.HTML

EXAMPLE OF A VIGENERE

VIDEO FROM DOCUMENTARY OF "THE CODE BOOK" BY SIMON SINGH

ONE TIME PADS

- [ ] VERNAM CIPHERS (1917)
- [ ] KEY IS AS LONG AS THE MESSAGE



AMERICAN CRYPTOHISTORY

- HERBERT YARDLEY

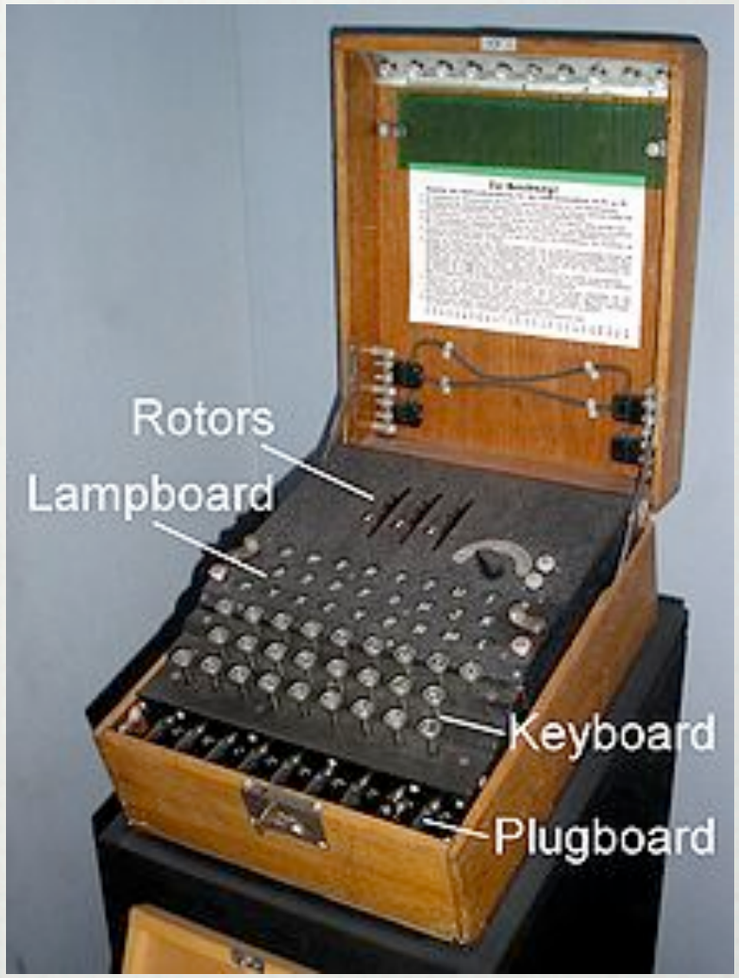
- WILLIAM FRIEDMAN

- AMERICAN BLACK CHAMBER

HTTPS://EN.WIKIPEDIA.ORG/WIKI/FILE:FRIEDMAN-1919.JPG

ENIGMA

- [ ] BLETCHLEY PARK
- [ ] ALAN TURING
- [ ] TURING BOMBE
- [ ] COLOSSUS

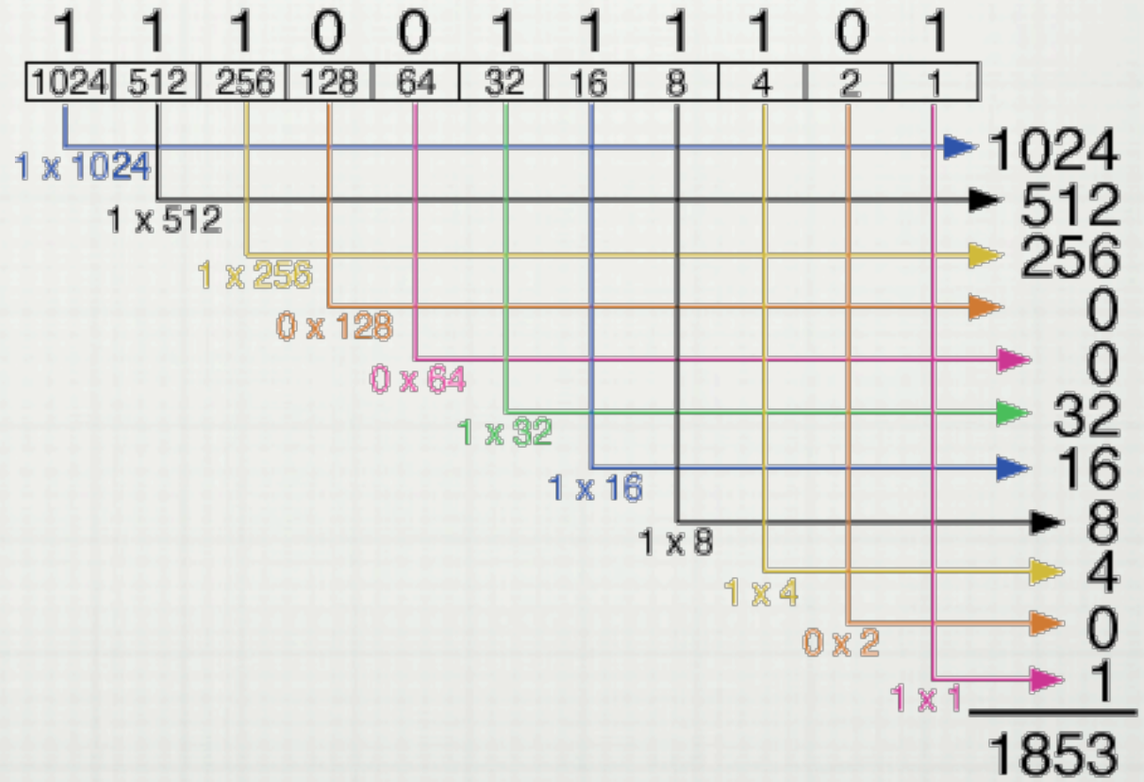


HTTP://UPLOAD.WIKIMEDIA.ORG/WIKIPEDIA/COMMONS/THUMB/3/3E/ENIGMAMACHINELABELED.JPG/220PX-ENIGMAMACHINELABELED.JPG

HTTPS://EN.WIKIPEDIA.ORG/WIKI/ALAN_TURING

QUICK MATH LESSON

- [ ] BASE SYSTEMS
- [ ] DECIMAL (BASE 10)
- [ ] BINARY (BASE 2)
- [ ] MSB, LSB



QUICK MATH LESSON

- XOR TRUTH TABLES

Exclusive-OR gate

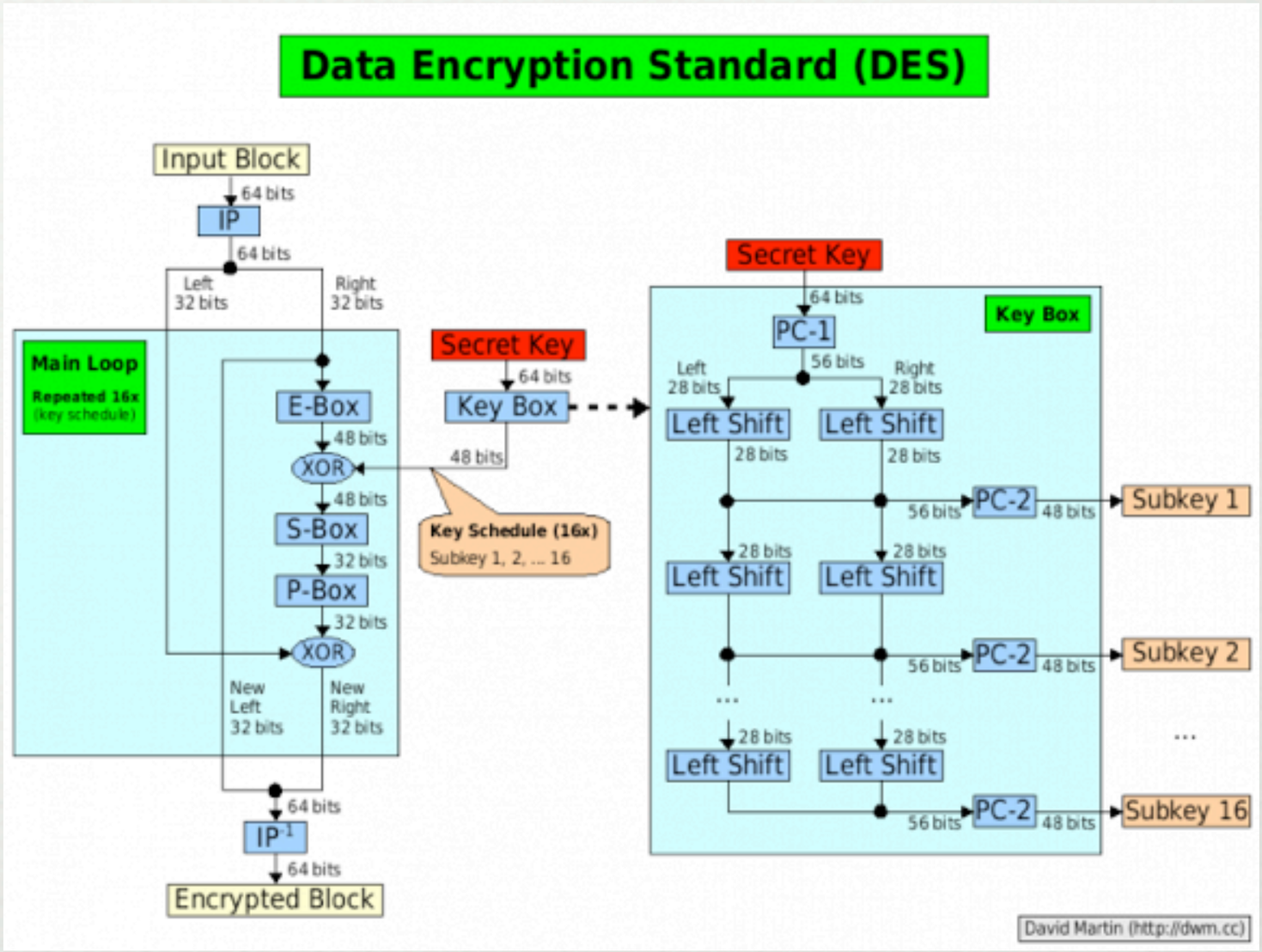
A	B	Output
0	0	0
0	1	1
1	0	1
1	1	0

MODERN CRYPTOGRAPHY

- TWO TYPES:
  - SYMMETRIC CRYPTOGRAPHY
  - ASYMMETRIC CRYPTOGRAPHY
- TWO PURPOSES:
  - SECURE COMMUNICATION
  - AUTHENTICATION AND VERIFICATION

SYMMETRIC CRYPTOGRAPHY

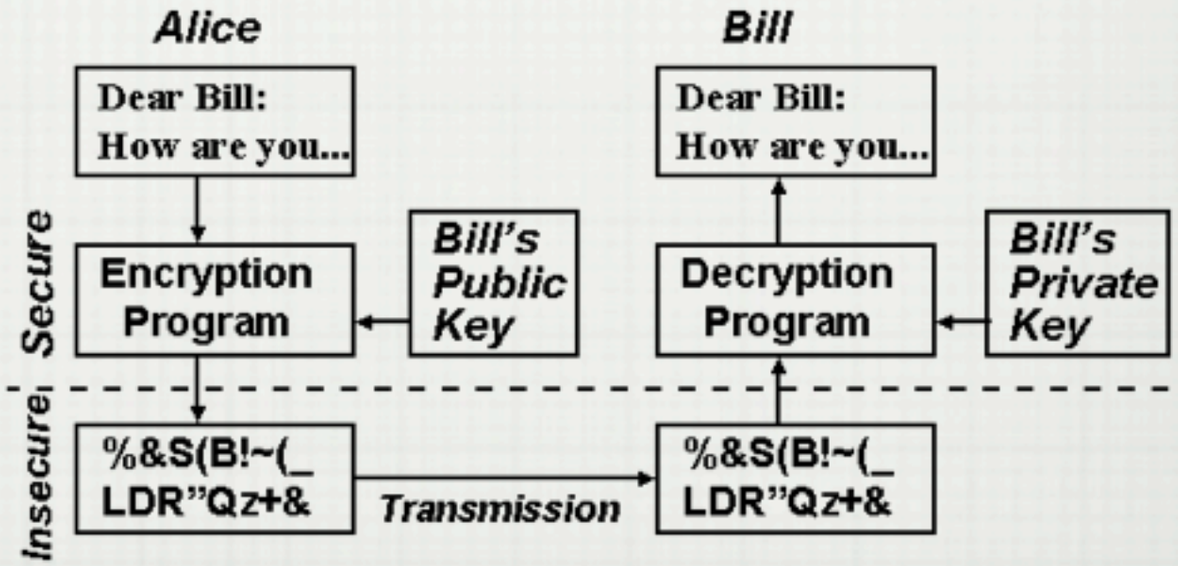
- SAME KEY TO ENCRYPT AND DECRYPT
- DES USES ITERATIONS



HTTP://DWM.CC/GALLERY2/V/UCF/HOW+DES+WORKS.PNG.HTML

ASYMMETRIC CRYPTOGRAPHY

- DIFFERENT KEYS TO ENCRYPT AND DECRYPT
- PUBLIC KEY
- PRIVATE KEY
- "DIFFIE-HELLMAN"



HTTP://WWW.HOLOWCZAK.COM/RSADEMO/PUBLICKEY.GIF

ASYMMETRIC CRYPTOGRAPHY

- RSA USES PRIME NUMBERS

Key Generation

Select p, q	p, q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

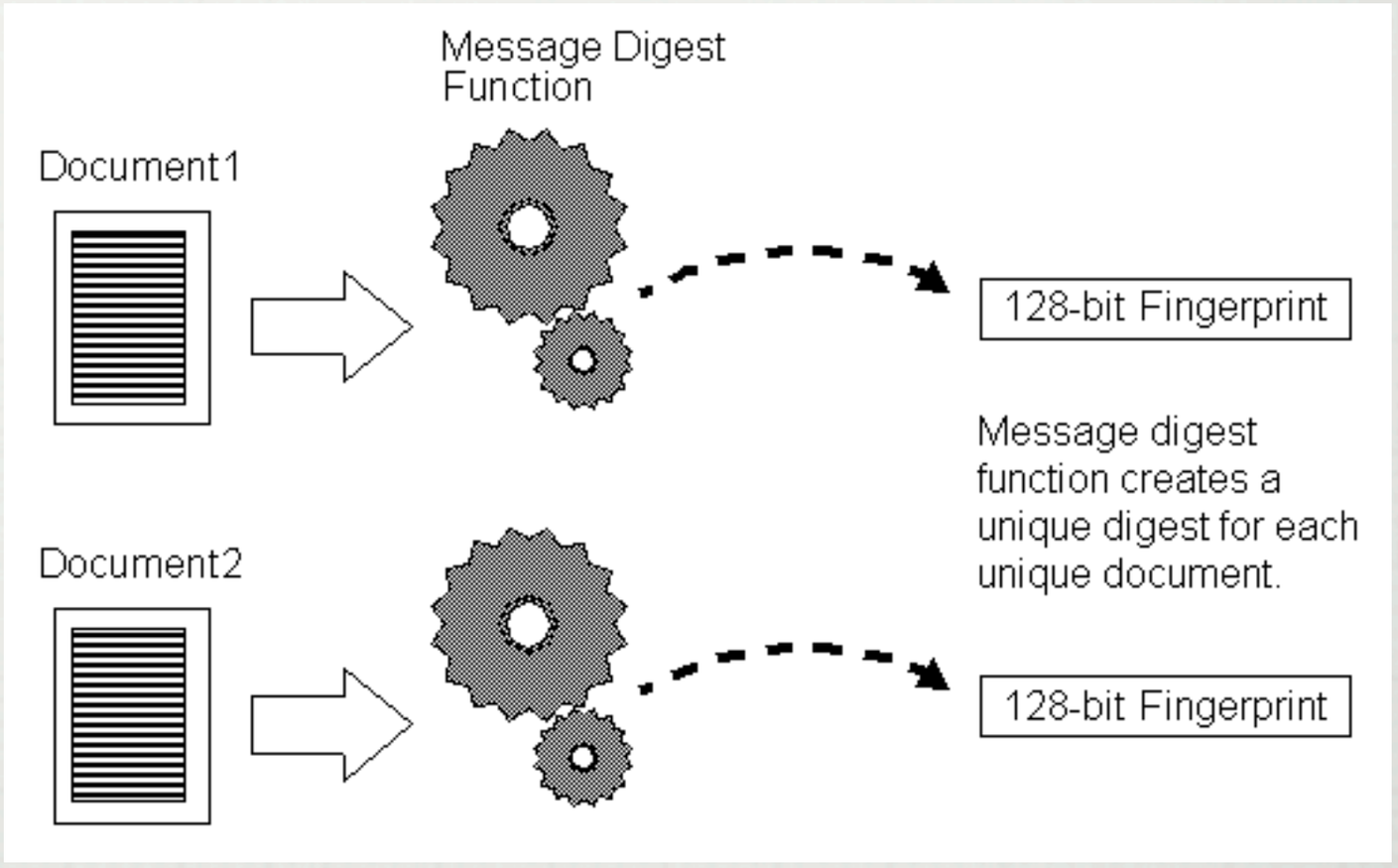
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

HASH FUNCTIONS

- ONE WAY HASH
- AUTHENTICATION, VALIDATION
- CRC, MD5, SHA256



HTTP://WWW.AKADIA.COM/SERVICES/MD5.HTML

STEGANOGRAPHY

- [ ] HIDING MESSAGES IN OTHER MEDIA (MUSIC, IMAGES)
- [ ] "AFTER THE THEATRE, ALL CLIENTS KEEP A TAB DOWN AT WESLEY'S NOOK."

(THANKS, ELONKA!) HTTP://ELONKA.COM/STEGO/STEGOLR.HTM

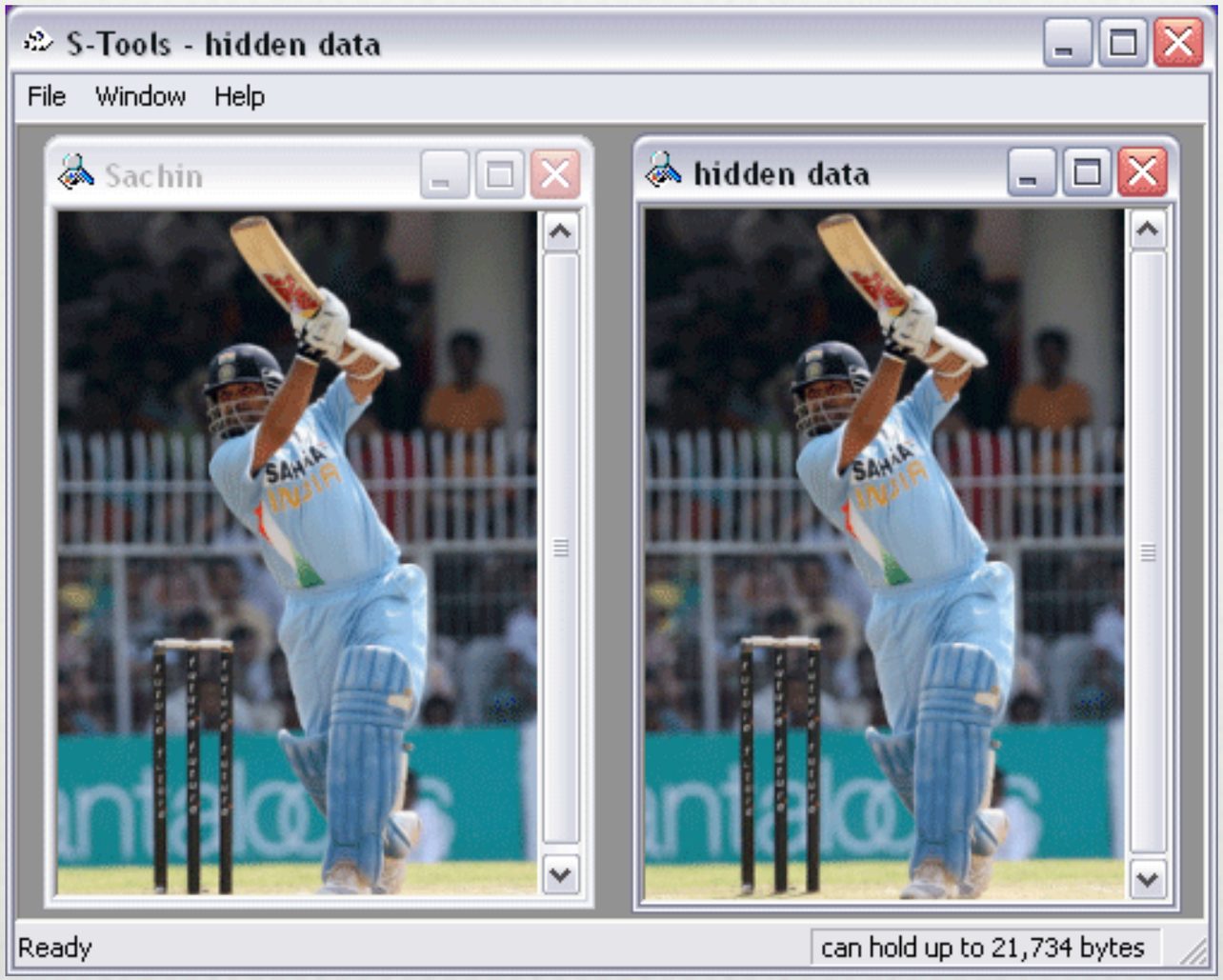
STEGANOGRAPHY

- [ ] HIDING MESSAGES IN OTHER MEDIA (MUSIC, IMAGES)
- [ ] "AFTER THE THEATRE, ALL CLIENTS KEEP A TAB DOWN AT WESLEY'S NOOK."
- [ ] "ATTACK AT DAWN"

(THANKS, ELONKA!) HTTP://ELONKA.COM/STEGO/STEGOLR.HTM

STEGANOGRAPHY

- HIDDEN IN IMAGES, MUSIC, TEXT, ETC



HTTP://WWW.INSECURE.IN/STEGANOGRAPHY.ASP

WRAPPING UP

- [ ] A GOOD CRYPTOSYSTEM IS SECURE IF ALL PARTS MINUS THE KEY ARE KNOWN

- [ ] MODERN CRYPTOGRAPHY CAN BE USED FOR BOTH ENCRYPTION AND VALIDATION

- [ ] SYMMETRIC CRYPTOGRAPHY USES ONE KEY, ASYMMETRIC USES TWO KEYS

FIN

- [ ] QUESTIONS?
- [ ] @AESTETIX