



# The History of Cryptography

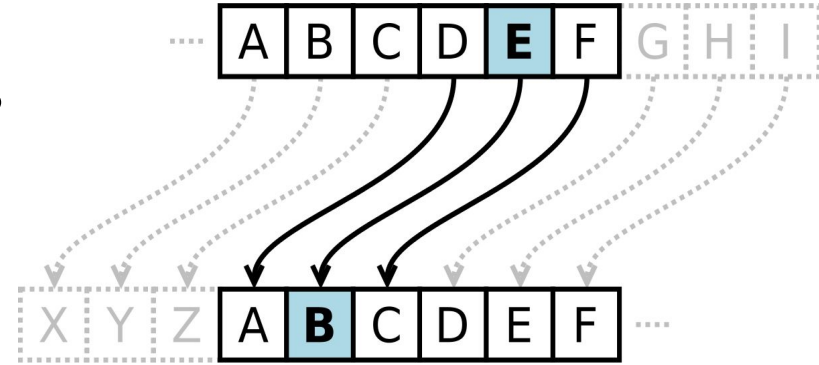
March 15, 2018

Jack Dell, Peter Regas

# The Beginnings



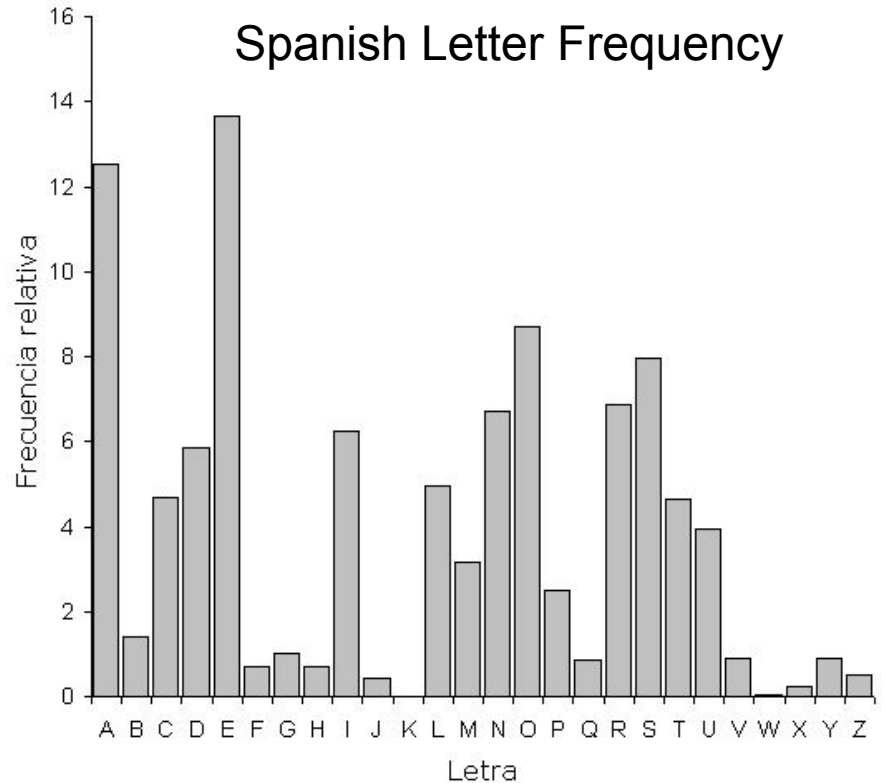
Julius Caesar  
Caesar Ciphers  
50BC



# First form of Encryption Cracking



**“Al-Kindi”**  
Arabic  
Polymath  
First discovered  
Frequency Analysis  
Method  
850



# Combating Frequency Analysis

a b c d e f g h i k l m n o p q r s t u x y z  
 0 † ‡ § ¶ · ¸ 9 10 11 12 13 14 15 16 17 18 19

Nulles ff. — . — d.

Dowbleth σ

and for with that if but where as of the from by  
 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

so not when there this in wich is what say me my wyrt  
 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40

send lre receive bearer I pray you Mte your name myne  
 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60

	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z		
1	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s		1
2	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g		2
3	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n		3
4	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l		4
5	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z		5
6	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r		6
7	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a		7
8	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a		8
9	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q		9
10	y	z	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x		10
11	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z		11
12	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	l	m		12

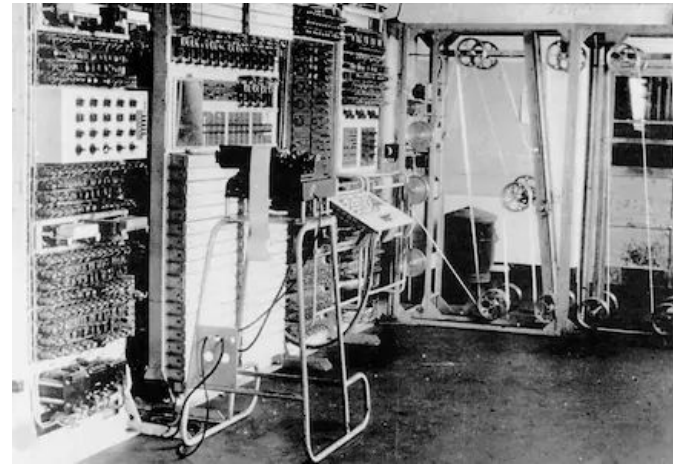
1. Still involved a basic cipher
2. Distribution and updating of nomenclators was challenging
3. Hard to have lots of people using same nomenclator

# WWII

Bombe

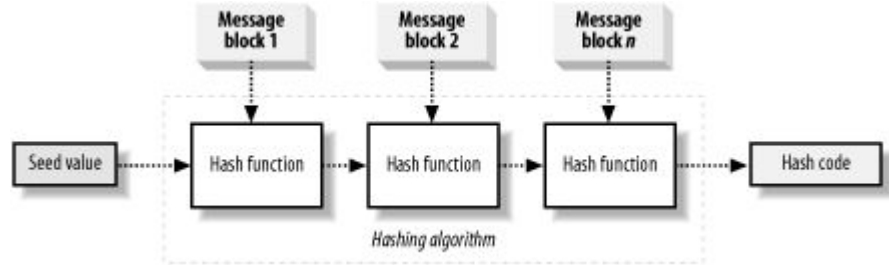
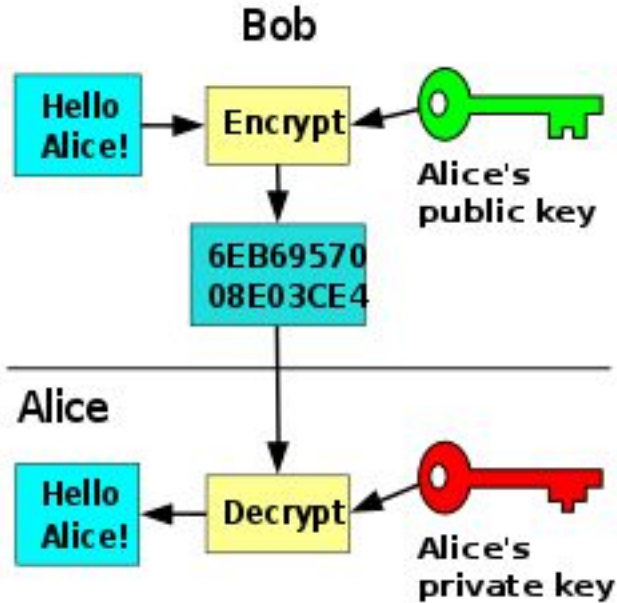


Colossus



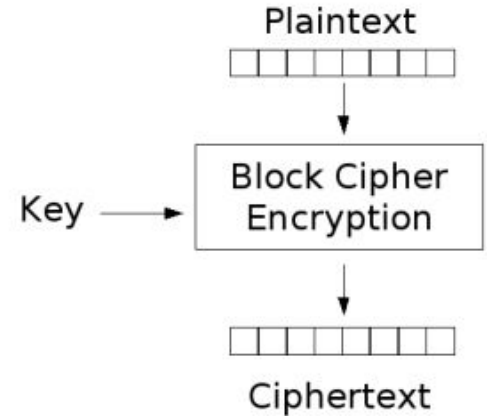
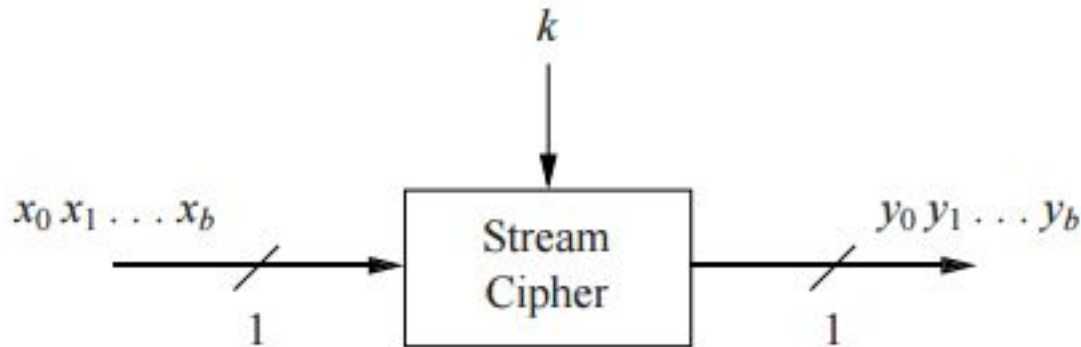
# Public Keys

Solved the problem of encrypting two way communication



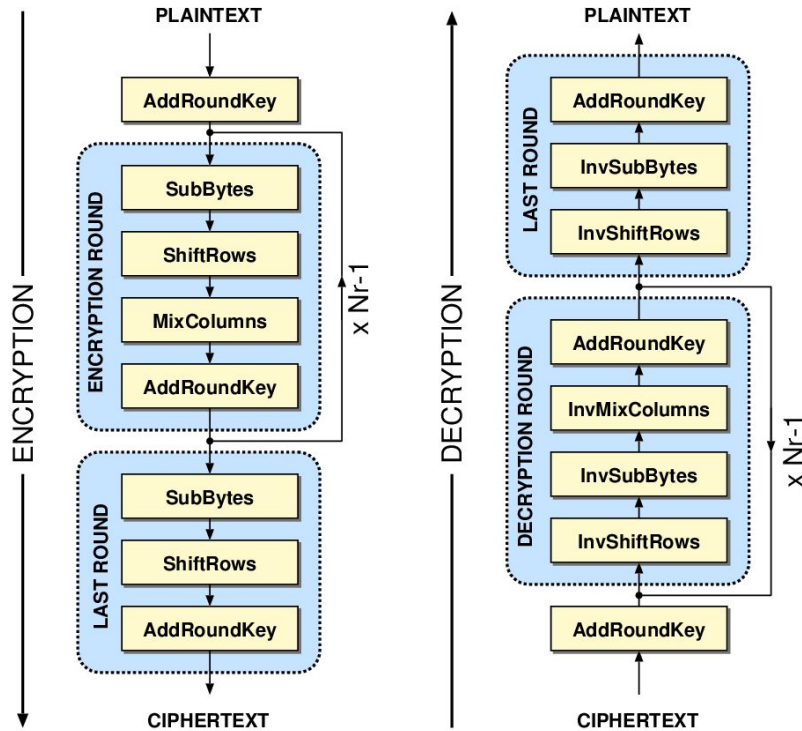
# Stream & Block Ciphers

- Stream ciphers consist of long continuous data stream
- Data stream is plain text bits
- The bits are encoded using a cryptographic key and some chosen algorithm

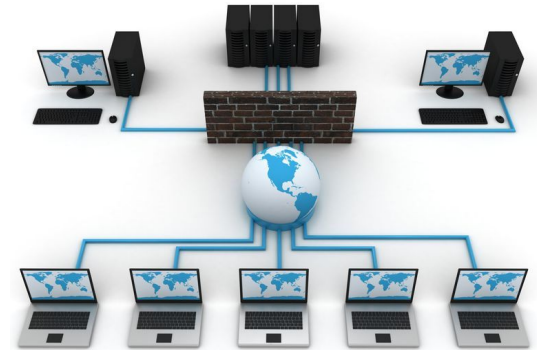


- Block ciphers are very similar to stream ciphers
- Instead of individually encoding each bit, block ciphers will encode blocks of data of a specified size

# Modern Encryption Security



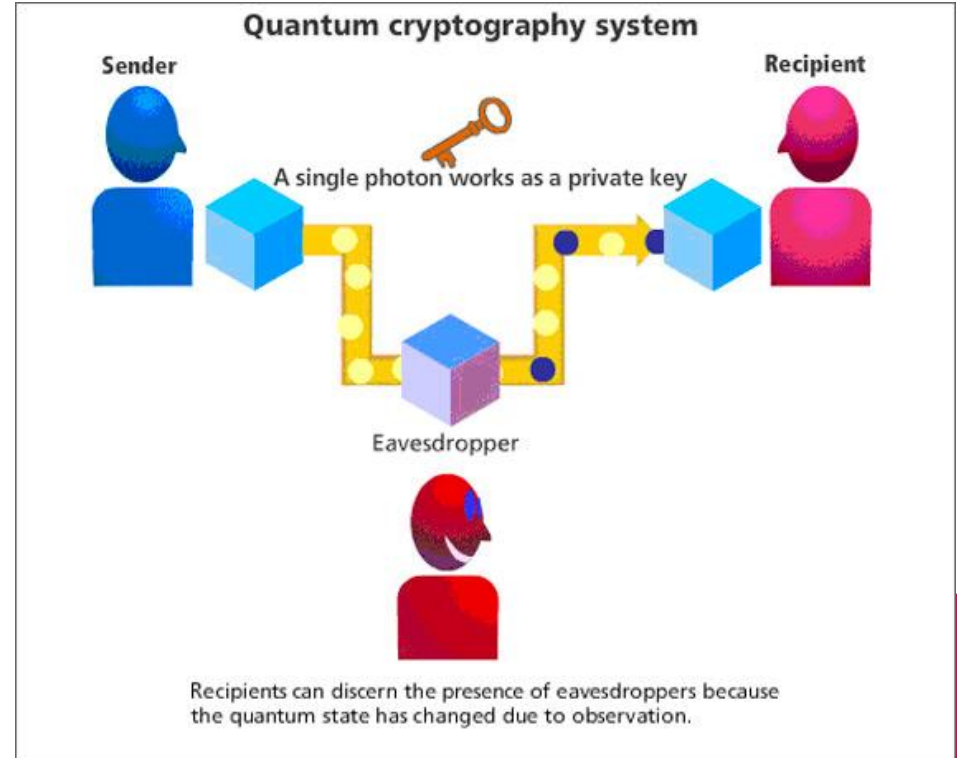
- Many modern Encryptions could be trivially decrypted with future advances
- Mathematics and computing technology is constantly advancing





# Quantum Encryption

“Quantum cryptography makes use of the quantum-mechanical behavior of nature for the design and analysis of cryptographic schemes. Optimally (but not always), quantum cryptography allows for the design of cryptographic schemes whose security is guaranteed solely by the laws of nature” (Fehr, 2010, pg 494).



# Conclusion

- Cryptography is a field that continues to reinvent itself over time.
- Is there a better solution with current technology?
- Is Quantum Cryptography the final step in this progression?

