Course: Cryptography and Network Security
Code: CS-34310
Branch: M.C.A - 4th Semester

Lecture – 1: Introduction

Faculty & Coordinator : Dr. J Sathish Kumar (JSK)

Department of Computer Science and Engineering

Motilal Nehru National Institute of Technology Allahabad,
Prayagraj-211004

Course Outline (To be covered in 30 lectures)

1. Introduction, Prime Number Generation, Shannon's Theory of Perfect Secrecy (5)
2. Asymmetric Key Cryptosystem and related issues (3)
3. Public Key Cryptography and related concepts/methodologies (4)
4. Cryptographic Hash Functions design and implementation issues. (4)
5. Digital Signatures and related issues (5)
6. E-Mail, IP and Web security (6)
7. Malicious Programs & Firewall(3)

Text Books

1. Modern Cryptography : Theory and Practice by W Mao
2. Applied cryptography by Bruce Schiener
3. “Cryptography: Theory & Practice” D R Stinson,
4. Introduction to cryptography by Johannes A Buchmann
5. Network Security and Cryptography by Bernard Menezes

Course Outcome(s):

After learning all the units of the course, the student can

1. Understand terms related to Cryptography, Attack types
2. Different Encryption Techniques to be used
3. Asymmetric key algorithm,
4. Public key cryptography
5. Mathematical foundation of cryptography,
6. Message integrity, message authentication and authentication protocols.
7. Digital Signature Mechanism
8. Advanced topics of Cryptography.

Program Outcome(s):

- PO1: Apply knowledge of mathematics, science and algorithm in solving complex Computer engineering problems.
- PO2: Generate solutions by programming and applying techniques to analyse and interpret data.
- PO3: Design component, or processes to meet the needs with in realistic constraints.
- PO4: Comprehend professional and ethical responsibility in computing profession.
- PO5: Express effective communication skills.
- PO6: Recognize the need for, and an ability to engage in life-long learning.
- PO7: Knowledge of contemporary issues and emerging developments in computing profession.
- PO 8: Design research problems and conduct research in computing environment.

Lets Get Started !!!!

History and Overview of Cryptography

- The Concise Oxford English Dictionary defines cryptography as “the art of writing or solving codes.”
- Cryptography: The Science of creating coded messages
- Cryptanalysis: The art of breaking coded messages
- Clear text/Plaintext: The original Message
- Cipher text: The encoded message
- Key: Input to the cryptographic algorithm
- “Cryptography: Practice of the enciphering and deciphering of messages in secret code in order to render them unintelligible to all but the intended receiver

History and Overview of Cryptography

- But cryptography nowadays encompasses much more than this: it deals with
  - mechanisms for ensuring integrity,
  - techniques for exchanging secret keys,
  - protocols for authenticating users,
  - electronic auctions and elections,
  - digital cash, and more.
- Modern cryptography involves the study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks.

Early Cryptography

- 3500 BC: Sumerians: Cuneiform writings

Source: Internet

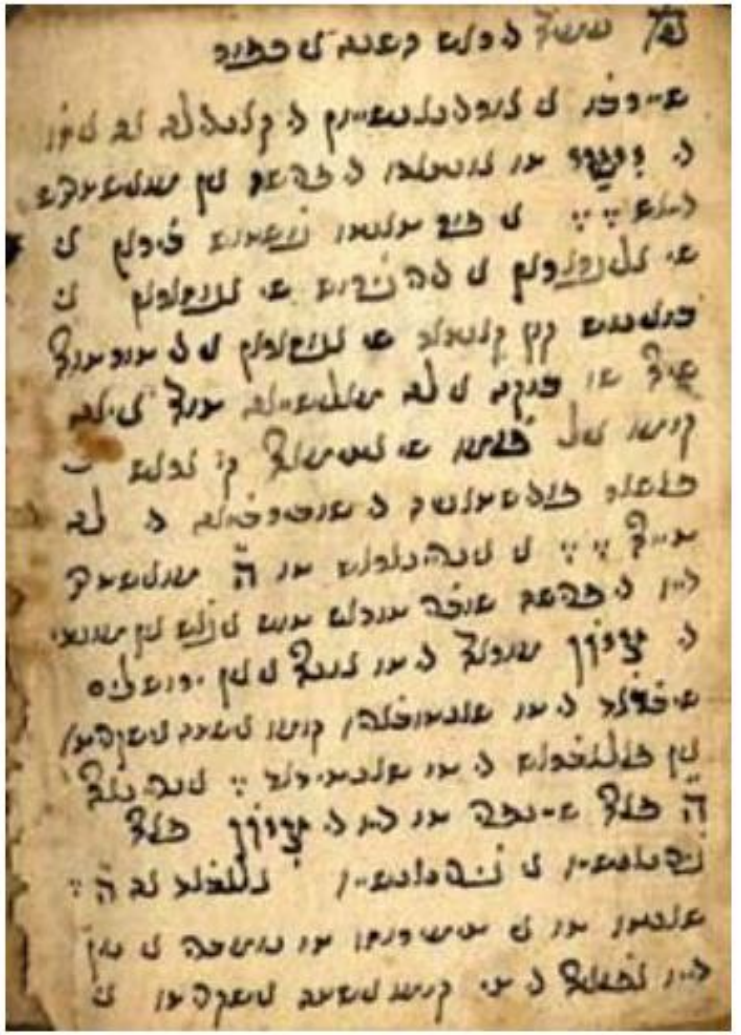
Early Cryptography

- 1900 BC: Egypt: First known use of cryptography

Source: Internet

Early Cryptography

- 500 – 600 BC: ATBASH Cipher
- Used by Hebrew scribes – Substitution cipher (reversed alphabet)



Source: Internet

Early Cryptography

- 486 BC: Greece
- σκυτάλη – skytale

Source: Internet

Early Cryptography

- 60 – 50 BC: Julius Caesar – substitution cipher – Shift letters by X positions:
- E.g. X = 3: A -> D, B -> E, C -> F,....
- Weakness?
  - Frequency analysis (1000 AD)

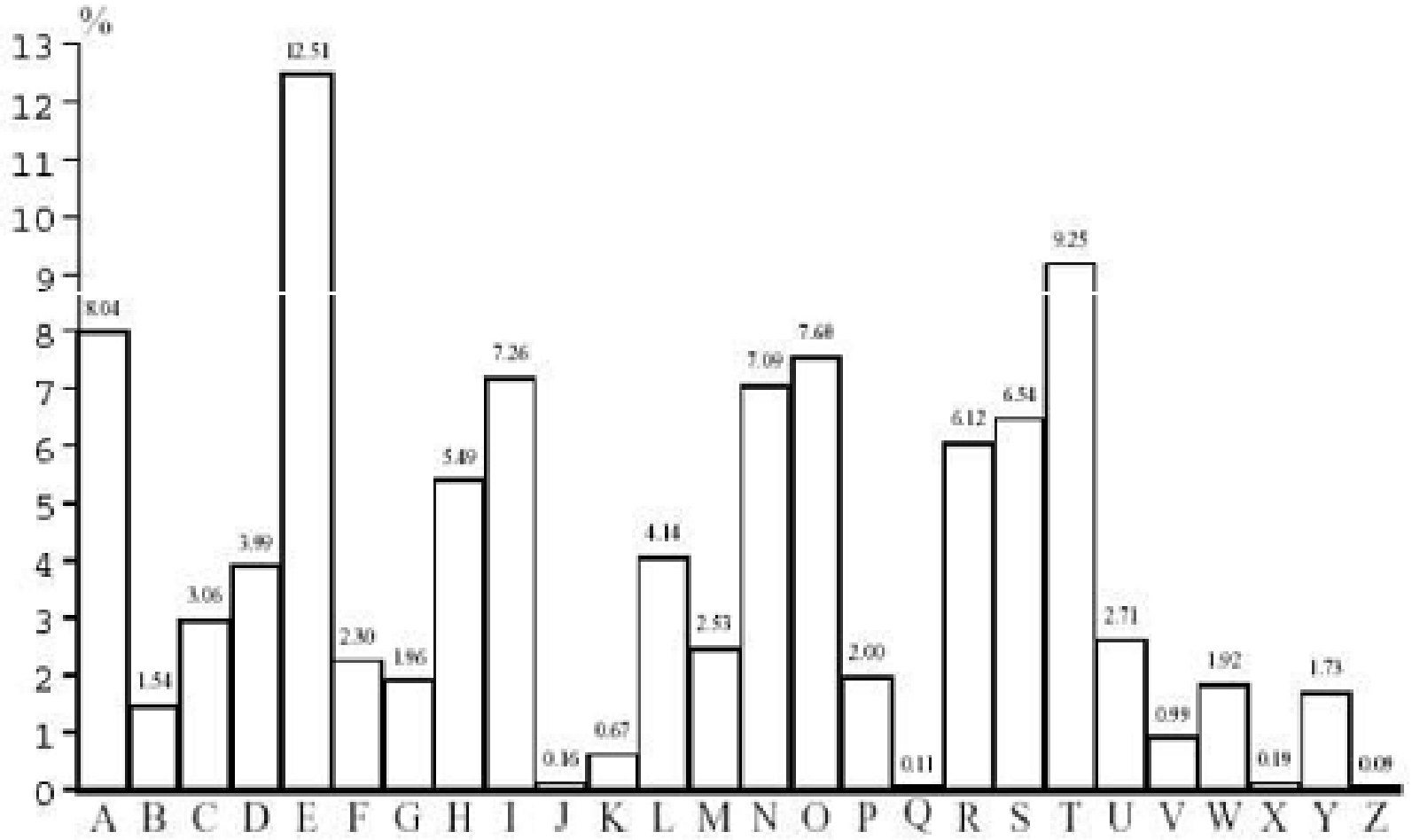
Source: Internet

Early Cryptography

- Mono-alphabetic substitution
  - letters of the plain text alphabet are mapped on to unique letters throughout the entire message text
  - cipher can be trivially broken because

    i. The language of the plain text is easily recognizable. (frequency distribution- unigram statistics- next slide)
    ii. There are only s= |A| keys (e.g. for Roman alphabet, only 25 keys – 1 to 25) to search exhaustively
    - Exhaustive key search is always possible <make it practically infeasible is the goal>

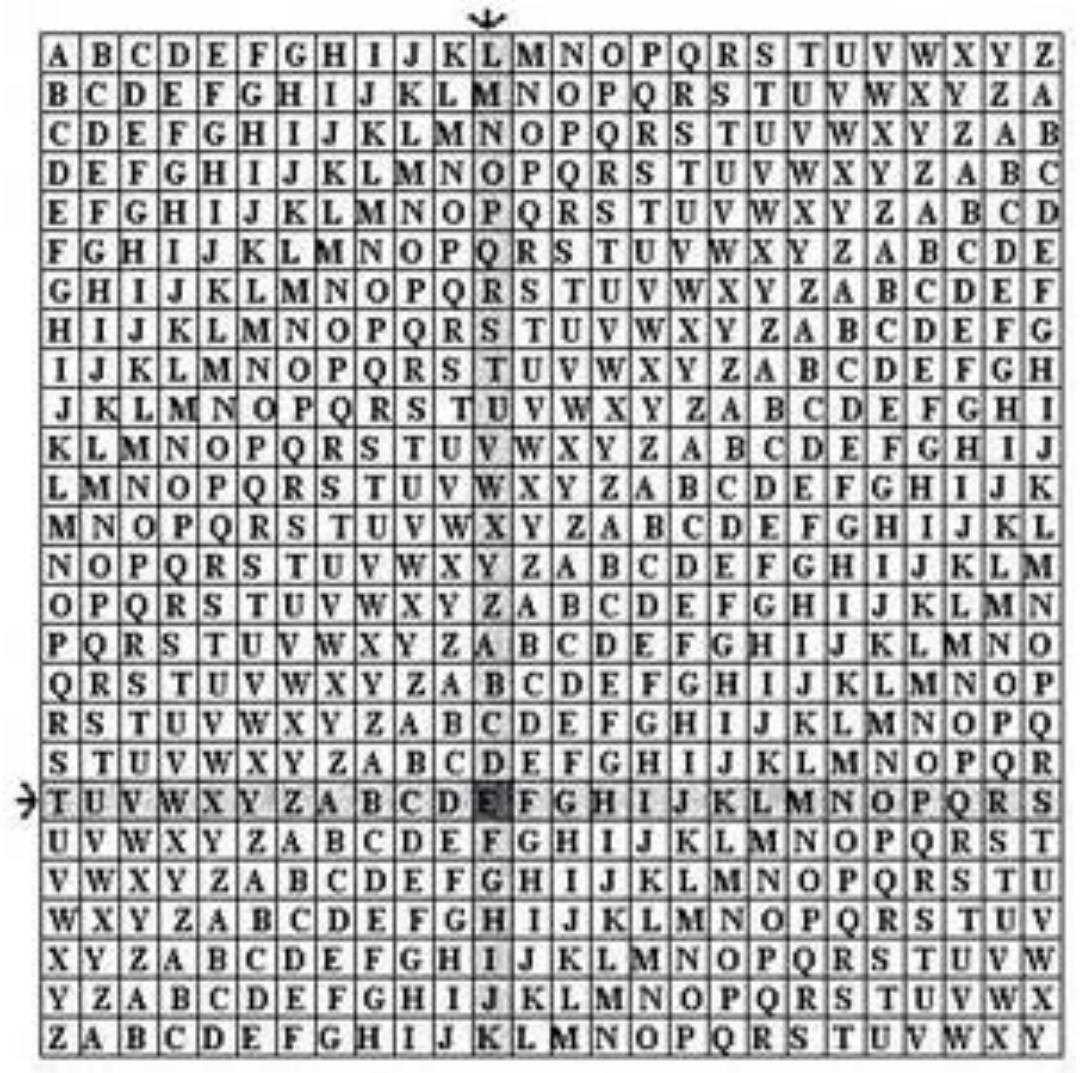
Frequency of single characters in English text



Medieval Cryptography

- 1587: Vigenère Cipher
- Polyalphabetic: one to many relationship
- Example

plaintext:	T	O	B	E	O	R	N	O	T	T	O	B	E
key:	L	T	O	B	E	O	R	N	O	T	T	O	B
ciphertext:	E	H	P	F	S	F	E	B	H	M	H	P	F



Medieval Cryptography
Vigenère Cipher

Example:
Message: "What fools these mortals be"

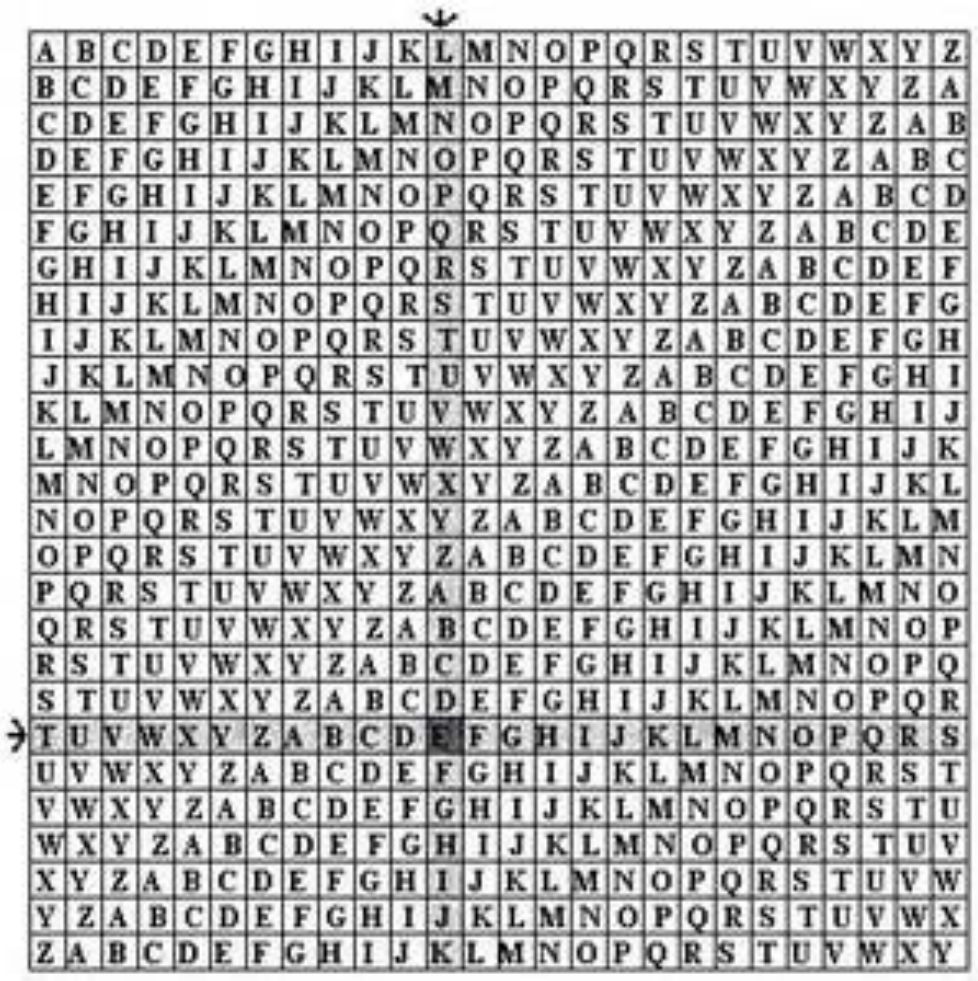
Keyword: Puck

plaintext:	W	H	A	T	F		O	O	L	S	T		H	E	S	E	M		O	R	T	A	L		S	B	E
key:	P	U	C	K	P		U	C	K	P	U		C	K	P	U	C		K	P	U	C	K		P	U	C
ciphertext:	L	B	C	D	U		I	Q	V	H	N		J	O	H	Y	O		Y	G	N	C	V		H	V	G

Example:
Message: LBCDU IQVHN JOHYO YGNCV HVG

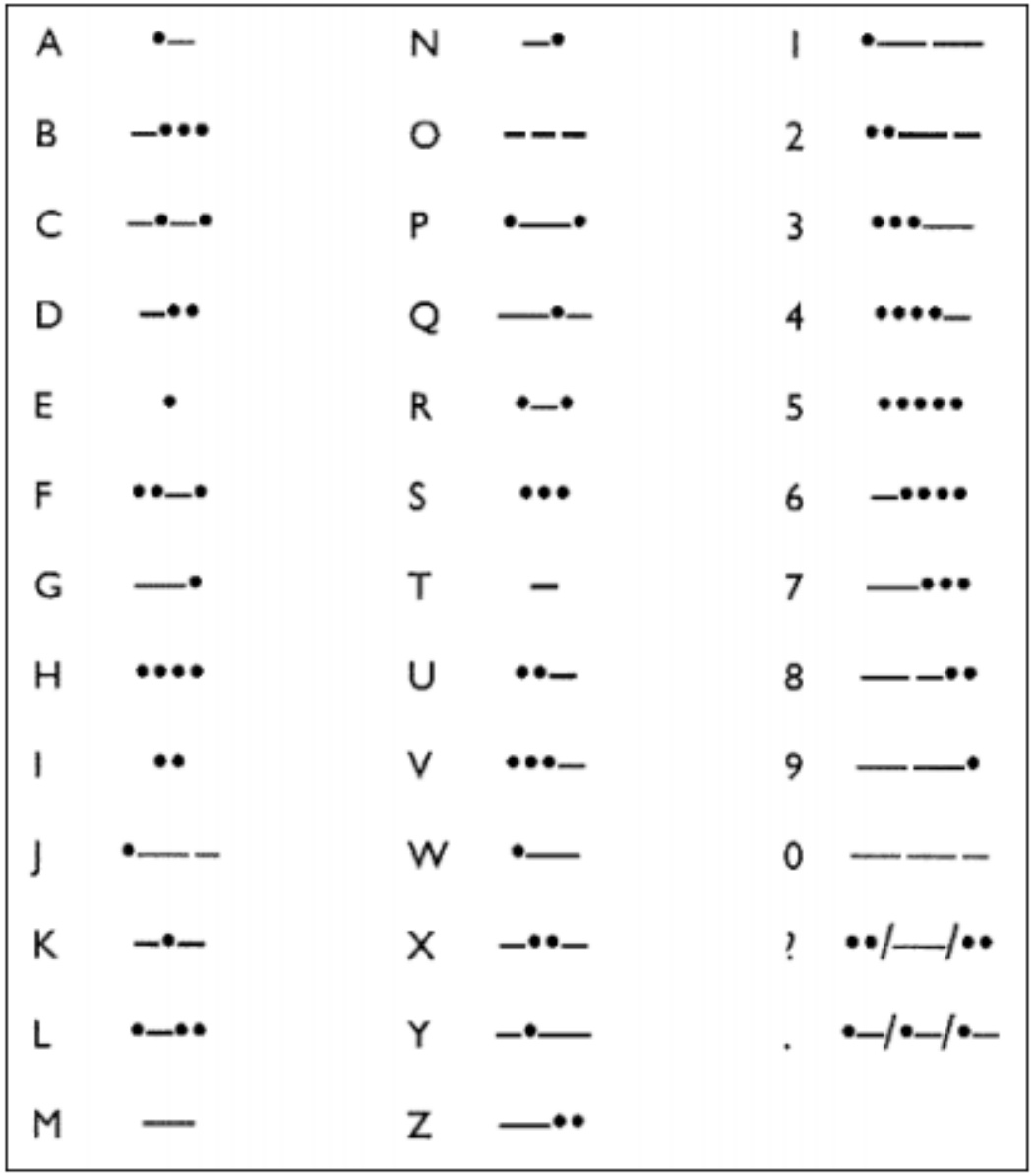
Keyword: Puck

key:	P	U	C	K	P		U	C	K	P	U		C	K	P	U	C		K	P	U	C	K		P	U	C
ciphertext:	L	B	C	D	U		I	Q	V	H	N		J	O	H	Y	O		Y	G	N	C	V		H	V	G
plaintext:	W	H	A	T	F		O	O	L	S	T		H	E	S	E	M		O	R	T	A	L		S	B	E



Modern Cryptography

- 1845: Morse Code –
- Representation by code signal
- States (on and off) composed into 5 symbols



A	•–	N	–•	1	•——
B	–•••	O	–––	2	••—–
C	–•–•	P	•––•	3	•••—–
D	–••	Q	––•–	4	••••–
E	•	R	•–•	5	•••••
F	••–•	S	•••	6	–••••
G	––•	T	–	7	––•••
H	••••	U	••–	8	––––••
I	••	V	•••–	9	––––•
J	•–––	W	•––	0	–––––
K	–•–	X	–••–	?	••/––/••
L	•–••	Y	–•––	.	•–/•–/•–
M	––	Z	––••		

Modern Cryptography

- 1863: Friedrich Kasiski breaks Vigenere: –
  - By examining repeated strings of characters in the cipher text, which could indicate the length of the secret key.
  - Find length of keyword
  - Once the length of the secret key is known, the cipher text is rewritten into a corresponding number of columns, with a column for each letter of the key.
  - Each column is then made up of plaintext that’s been encrypted by one Caesar cipher.
  - Use frequency analysis to solve these

Modern Cryptography

- 1918: ADFGVX Cipher – Used in the German army in WWI

Encrypt the plaintext "attack at 1200am"
using keywords *147 regiment* and *privacy*

	A	D	F	G	V	X
A	1	4	7	R	E	G
D	I	M	N	T	A	B
F	C	D	F	H	J	K
G	L	O	P	Q	S	U
V	V	W	X	Y	Z	0
X	2	3	5	6	8	9

a	t	t	a	c	k	a	t	1	2	0	0	a	m
DV	DG	DG	DV	FA	FX	DV	DG	AA	XA	VX	VX	DV	DD

P	R	I	V	A	C	Y
4	5	3	6	1	2	7
D	V	D	G	D	G	D
V	F	A	F	X	D	V
D	G	A	A	X	A	V
X	V	X	D	V	D	D

Cipher Text: "DXXV GDAD DAAX DVDX VFGV GFAD DVVD".

Modern Cryptography

- 1918: ADFGVX Cipher – Used in the German army in WWI

Decrypt the ciphertext "ADDDF DDAXF XAGGF DXXAX FGXFG G" which was encrypted using keywords *monkeys* and *zebras*

By reading off each row we get the intermediate text "GXFGAX XFDFDA FXDDDX GAAXDF GG".

Z	E	B	R	A	S
6	3	2	4	1	5
G	X	F	G	A	X
X	F	D	F	D	A
F	X	D	D	D	X
G	A	A	X	D	F
G	G				

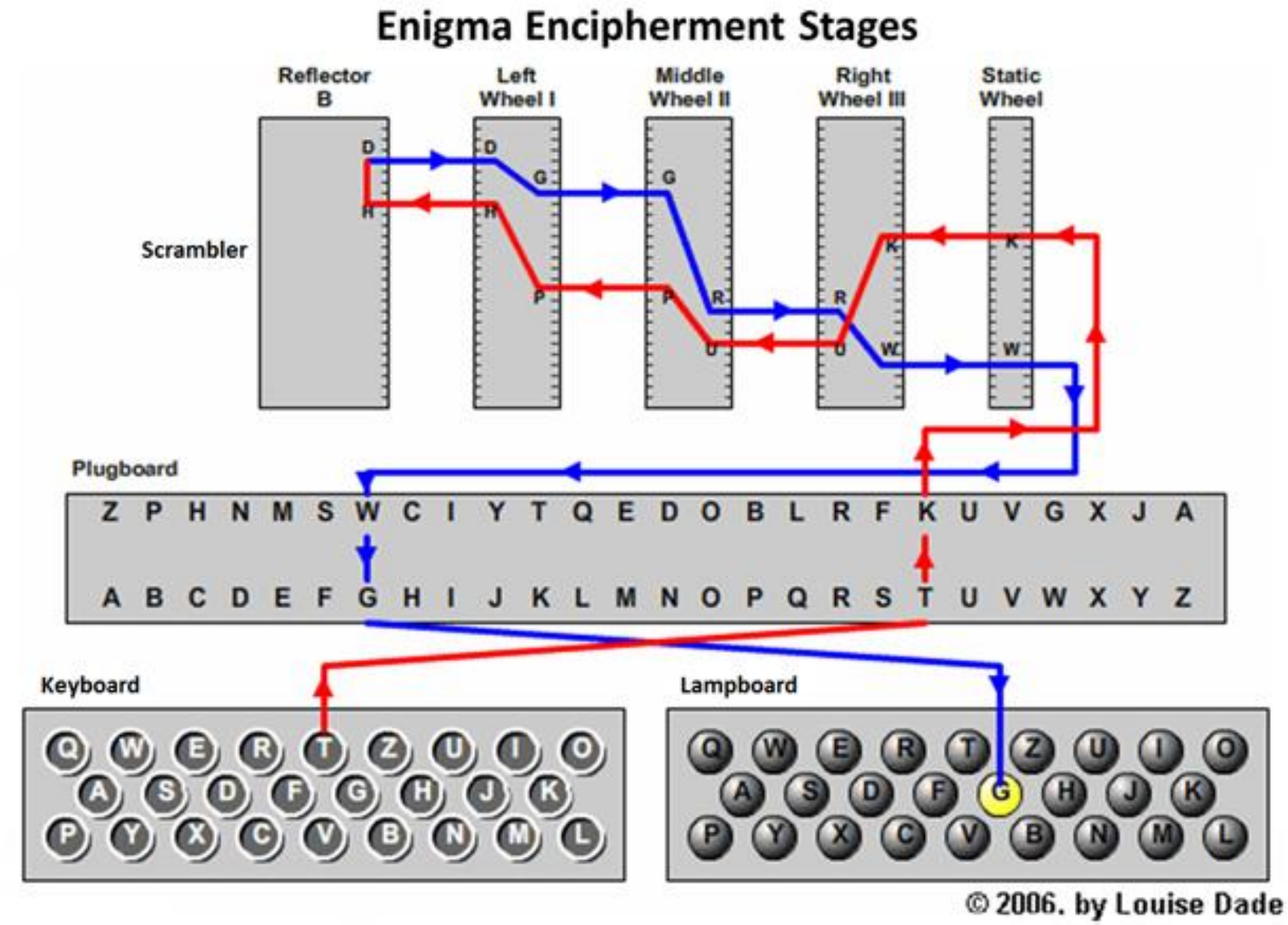
	A	D	F	G	X
A	M	O	N	K	E
D	Y	S	A	B	C
F	D	F	G	H	I
G	L	P	Q	R	T
X	U	V	W	X	Z

The plaintext is then retrieved as "the way is clear".

Modern Cryptography

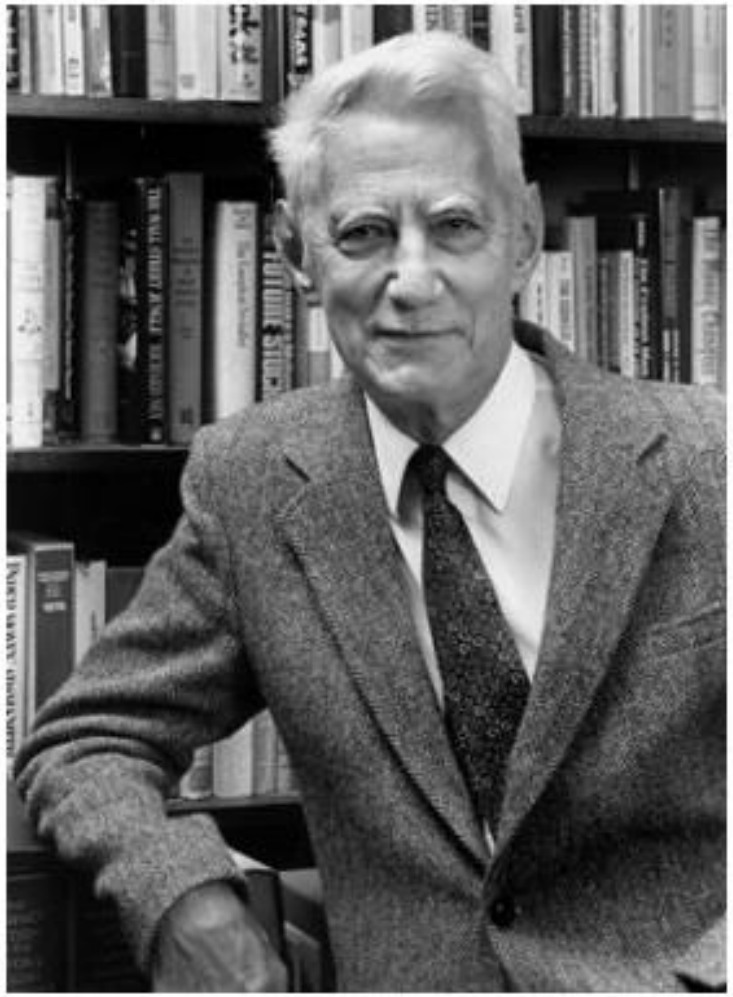
- 1918: The Enigma – Arthur Scherbius
- Business: confidential docs
- No codebooks
- Rotors -> multi substitution
- Wireing changes as-youtype
- German forces in WWII

Modern Cryptography: The Enigma



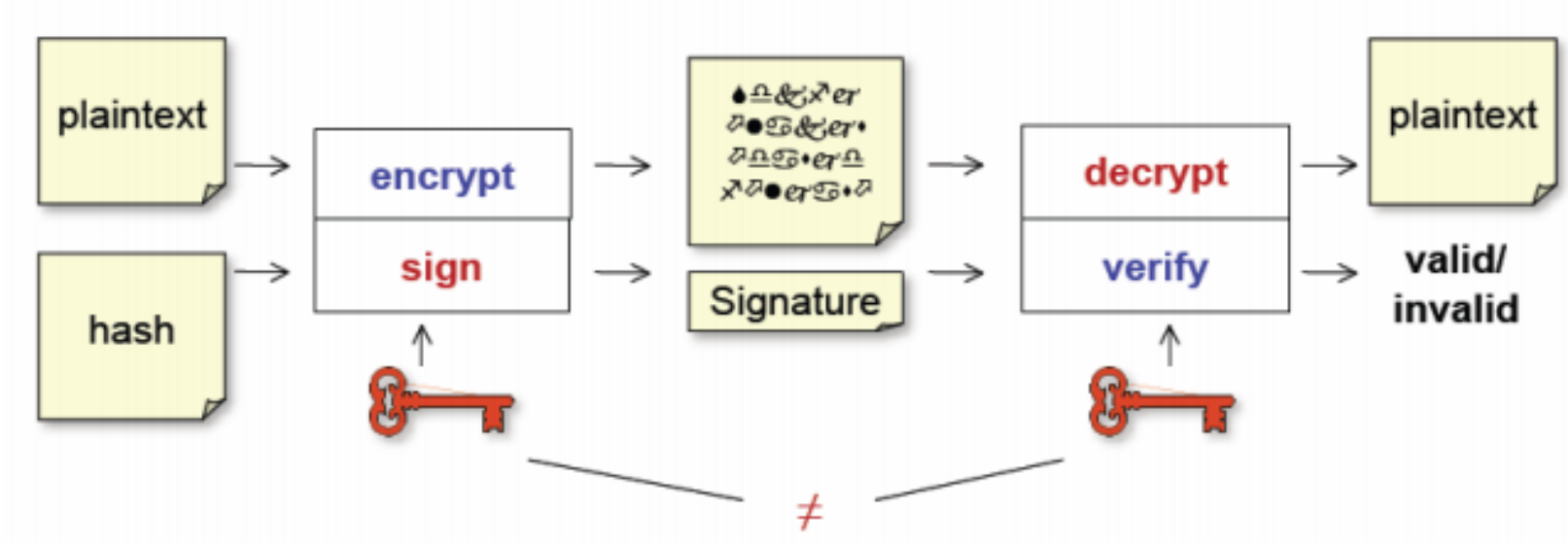
Modern Cryptography

- 1949: Shannon: –
- Communication Theory of Secret Systems
- Proved: One time pad unbreakable



Modern Cryptography

- 1976: Diffie – Hellman Key Exchange
- Public Key Crypto –
  - Key exchange problem –
  - Asymmetric key algorithm – E.g: RSA, MIT, 1977



Assignment #0

- Watch Movie “The Imitation Game”