CS 557: Cryptography

S. Tripathy
IIT Patna

Cryptography!!!

- The word CRYPTOGRAPHY:
  - The science of codes, derived from the Greek words kryptos (secret) and graphos (writing).

- Codes and ciphers:
  - are methods for encrypting data and messages.
  - have been used since ancient times (1900 B.C.)

What cryptography is\ not?

Cryptography is:

- A tremendous tool
- The basis for many security mechanisms

Cryptography is not

- the solution to all security problems
- reliable unless implemented and used properly

many many examples of broken ad-hoc designs

Why Cryptography ?

Cryptography is everywhere!!!

Secure communication:

- web traffic: HTTPS
- wireless traffic: 802.11i WPA2 (and WEP), GSM, Bluetooth

Encrypting files on disk: EFS, TrueCrypt

Content protection (e.g. DVD, Blu-ray discs): CSS, APS

User **authentication**

… and much much more

Cryptography Application:HTTPS Connection

Secure Sockets Layer / TLS

Two main parts

1. Handshake Protocol: **Establish shared secret key using public-key cryptography** (2nd part of course)

2. Record Layer: **Transmit data using shared secret key**

   Ensure confidentiality and integrity (1st part of course)

Use Cases

Single use key: (one time key)

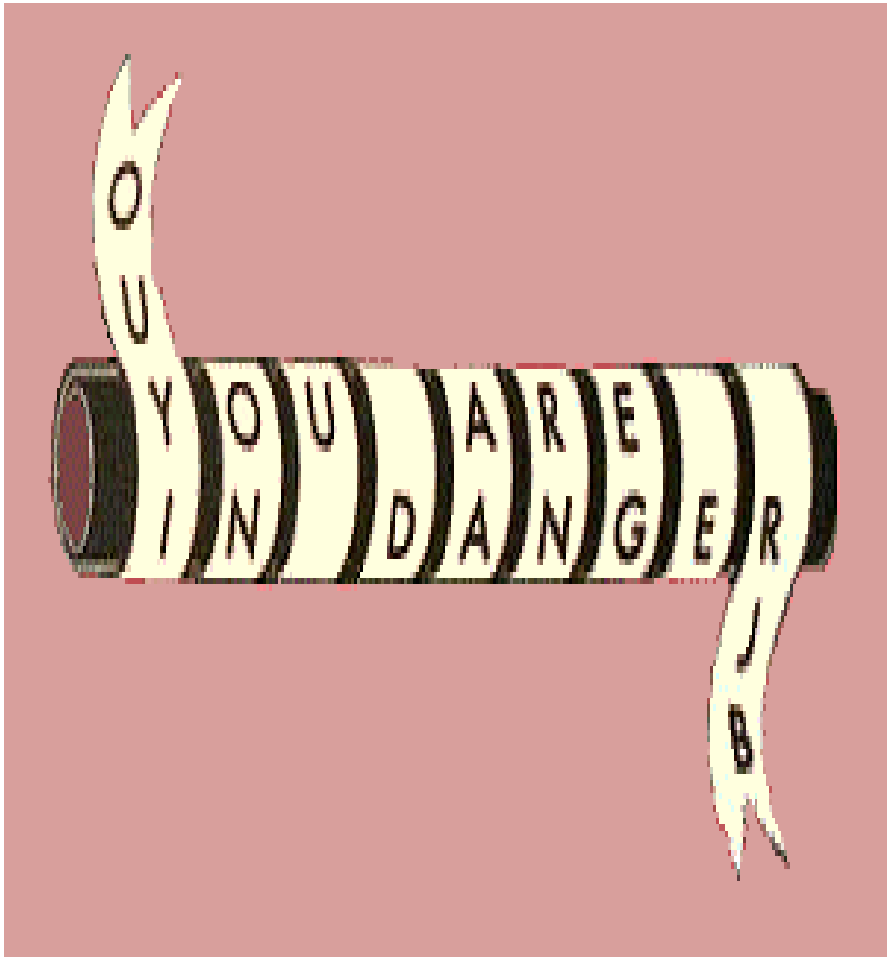
- Key is only used to encrypt one message
  - encrypted email: new key generated for every email

Multi use key: (many time key)

- Key used to encrypt multiple messages
  - encrypted files: same key used to encrypt many files
- Need more machinery than for one-time key

Historical Example 1

- In 405 BC the Greek general LYSANDER OF SPARTA was sent a coded message written on the inside of a servant's belt.



Historical Example 2

- The Greeks also invented a code which changed letters into numbers. A is written as 11, B is 12, and so on. So WAR would read 52 11 42. A form of this code was still being used two thousand years later during the First World War.

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

Historical Example 3

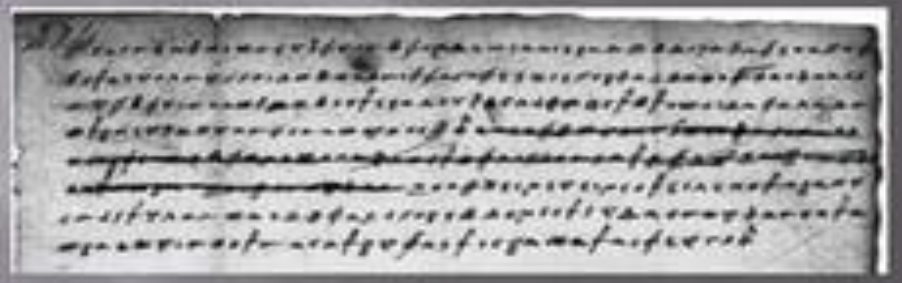
- The Roman Emperor JULIUS CAESAR invented his own simple code. He moved each letter of the alphabet along three places, so that A became D, B became E and so on. His famous phrase VENI, VIDI, VICI ("I came, I saw, I conquered") would have read YHQL YLGL YLFL.

Cryptanalysis

- Cryptanalysis is the study and process of analyzing and decrypting ciphers, codes, and encrypted text without using the real key
  - The science of code-breaking
- CRYPTANALYSIS - had begun
  - After the fall of the Roman Empire codes were not used much until the sixteenth century.
  - Then Italian and French scholars began to make up very complicated codes. .

Cryptanalysis: Example 1

A special type of code was used by Mary Queen of Scots when she was plotting against Elizabeth the First. Mary wanted to kill Elizabeth so that she herself could become Queen of England and was sending coded messages of this sort to her co-conspirator Anthony Babington. Unfortunately for Mary, there is a very simple way of cracking this code that doesn't involve trial and error, but which does involve, surprise, surprise, maths.



Letter sent by Mary Queen of Scots to her co-conspirator Anthony Babington. Every symbol stands for a letter of the alphabet.

- The messages were intercepted by the head of Elizabeth's secret service, Sir Francis Walsingham. He deciphered them and discovered the plot. Mary was executed for treason in 1587.

Enigma

ENIGMA:

- cipher device developed and used in the early- to mid-20th century
- looked like a typewriter in a wooden box. An electric current went from the keyboard through a set of rotors and a plugboard to light up the 'code' alphabet.

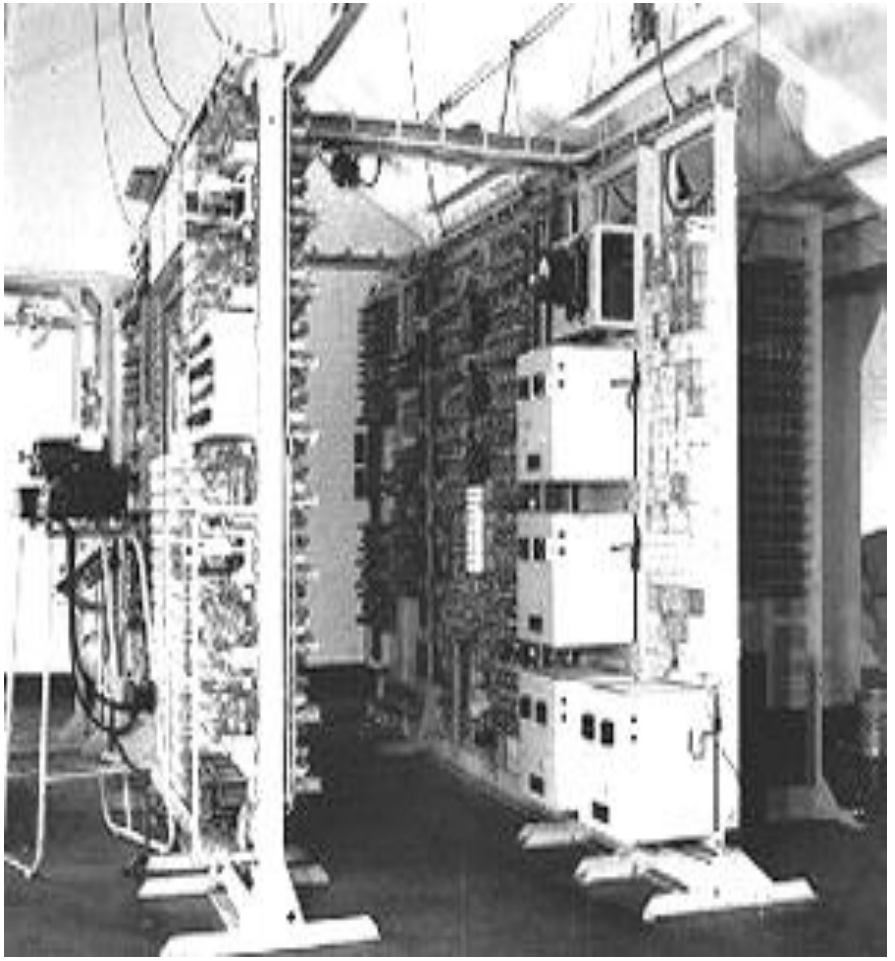
- Enigma could put a message into code in over 150 MILLION MILLION MILLION different ways.
  - At least once a day the Germans changed the order of the rotors, their starting positions and the plugboard connections. To decipher a message sent using Enigma, you had to work out exactly how all of these had been set.
  - In the 1930's Polish cipher experts secretly began to try to crack the code. Just before war broke out they managed to pass models and drawings of Enigma to British and French code-breakers.
  - Later Enigma was broken.

Some older Crypto machines

- Sigaba: Used by U.S. for high-level communications.
  - It was the only machine system used by any participant to remain completely unbroken by an enemy during World War II.
- BC38: Boris Hagelin of Sweden developed a long line of cipher systems, beginning with the B-21, B-211, C-35, C-36, C-38 (which later became America's M-209).
- BID 590: British built crypto machine used by Canada's foreign service communicators at various diplomatic missions to communicate with various government departments.
- The KY-28 was an analog, voice encryption device based on transistor circuitry
- The Racal-Milgo 64-1027C Datacryptor was used to send and receive secure data via computer. This is the commercial version of the KG-84,

Computer and Code Breaking

- Colossus was built for the code-breakers at Bletchley Park by post office engineers in 1943.
- One of the earliest computers.
- The computer was as big as a room - 5 metres long, 3 metres deep and 2.5 metres high - and was made mainly from parts used for post office telephone and telegraph systems.



Cipher Machines and Software Somulation

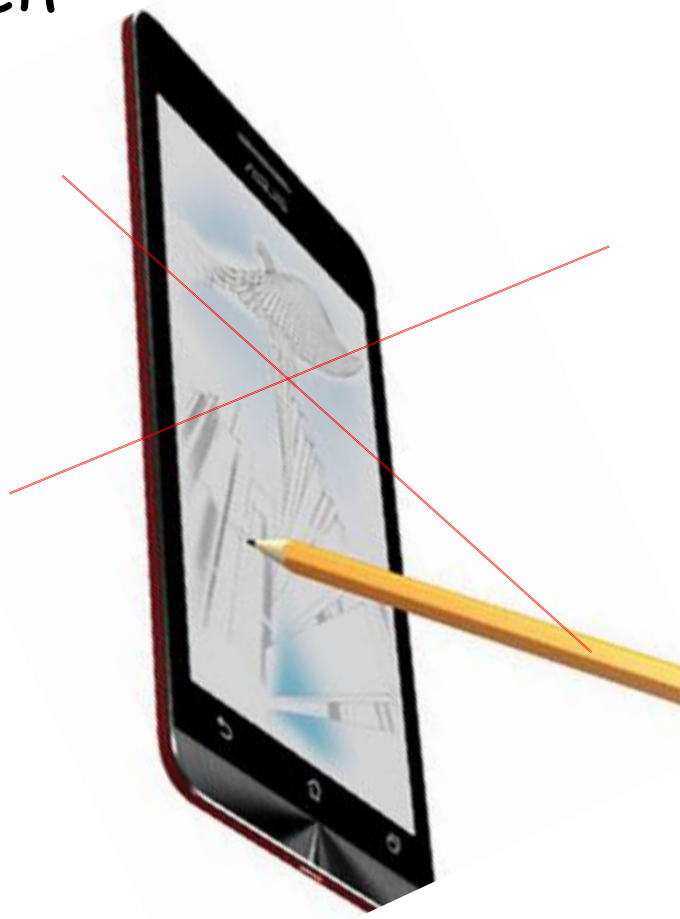
- http://frode.home.cern.ch/frode/crypto/

An appeal

- Please keep your mobile in silent/ switch off mode

- Please Keep your mobile(s)
  - inside your bag/ pocket

- Punctuality!!



Course Objective

- Goal:
  - This course aims to provide a solid foundation in cryptography.
  - It deals with the study of modern cryptography from a theoretical perspective and
  - the Students will build on these ideas by investigating practical implementation of cryptographic techniques
  - Various cryptographic constructs and their analysis

Course Outline

- Mathematical Background:
- Symmetric Key Encryption:
- Key Management,
- Hash Functions and Message Authentication Codes
- Public Key Encryption:
- Digital Signatures
- Public key based infra structure.
- Key Exchange:
- Zero knowledge based protocols.
- Text:
- Doug Stinson, Cryptography: Theory and Practice, Third Edition or later, Publisher: Chapman and Hall/CRC, 2005
- References:
- Hand book of applied cryptography by A. Menezes, CRC press: available online source: www.cacr.math.uwaterloo.ca/hac
- W. Mao, Modern Cryptography : Theory and Practice. Pearson Education, 2003 or later

Course mechanics

- Course pre-requsite
  - knowledge of any programming language (like c) is desirable.
- Evaluation
  - Assignments, Quiz-tests / Term Paper (30%)
  - Midterm (30%)
  - Final (40%)
- Your participation in the class has major value
- Attendance:
  - 75% is mandatory as per Ordinance

Thanks