بسم الله الرحمن الرحیم

درس مبانی رمزنگاری

الف) عناوین درس:

۱. مقدمه رمزنگاری و امنیت داده ها و نظریه اعداد (فصل اول و سایر مراجع)
۲. رمزهای جریانی(Stream Ciphers) (فصل دوم)
۳. رمزهای قالبی(Block Ciphers) (فصلهای سوم، چهارم و پنجم)
۴. رمزهای کلید عمومی(Public Key) (فصلهای ششم ،هفتم و هشتم)
۵. خمهای بیضوی(Elliptic Curve) (فصل نه)
۶. امضای دیجیتال(Digital Signature) (فصل ده)
۷. توابع چکیده ساز(Hash Functions) (فصل یازده و دوازده)
۸. پروتکلهای رمزنگاری(Protocols) (فصل ۱۳ و سایر مراجع)

ب)ارزیابی:

۱- امتحان اول : طبق برنامه دانشکده

۲- امتحان دوم :

۳-تکلیف و پروژه درسی:

د) گروه الکترونیکی درس

ه) مرجع اصلی:

-Christof Paar, Jan Pelzl,Understanding Cryptography, Springer-Verlag,2010

سایر مراجع :

- B.Schneier,” Applied Cryptography”, John Wiley& Sons,1996
-W.Stalling,” Cryptography and Network Security”, 6th ed.,2014
- J.Katz and Y.Lindell, ” Introduction to Modern Cryptography ”, CRC Press, 2007
-D.Stinson,” Cryptography Theory and Practice”, CRC Press, 2000
-J.Seberry&Pieper,” An Introduction to Computer Security “,Prentice Hall, -

Cryptography

- Greek kryptós (hidden) and gráphien (to write)
- The study of ways to hide or obscure information, making it unreadable without secret knowledge
- An interdisciplinary subject
- Before computers, linguistics dominated the crypto field. Today, it is mathematics, number theory, statistics, computational complexity, and finite mathematics.

Eras

- Two distinct eras of cryptography:
  - Pre-computer "classical"
  - Post-computer "modern"

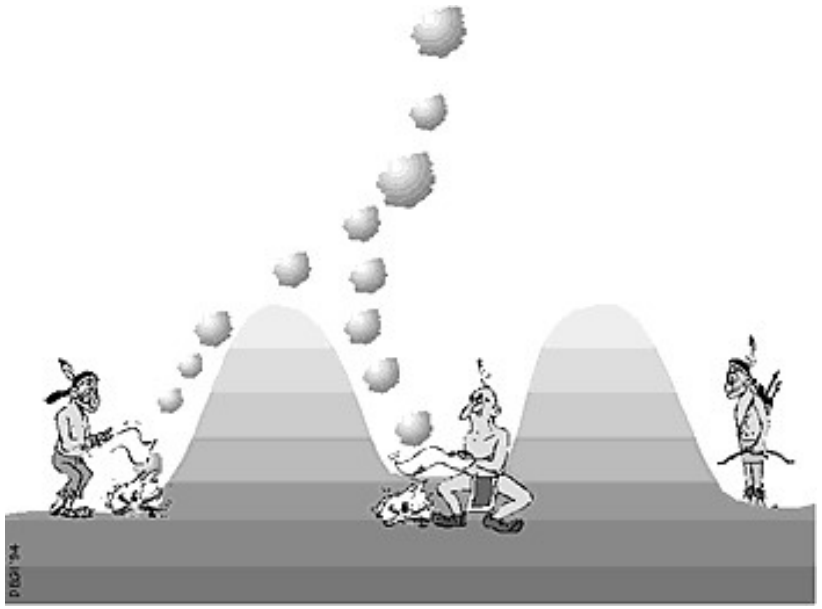
See the book:

"The Code Book", by: Simon Singh

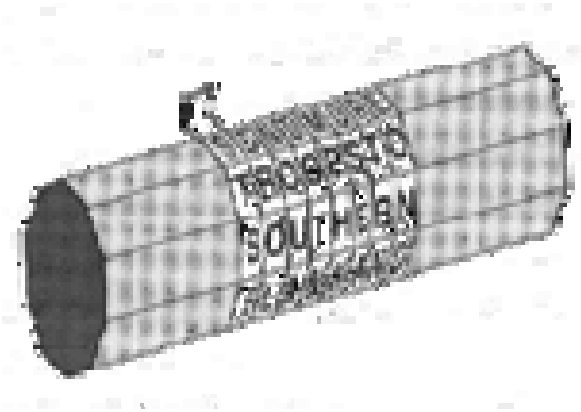
"Code Breakers", by : David Kahn

History

- **4000 years before ...(4000 B.C.)**



- **Spartans and Romans(500 B.C.)**



The Spartan's Skytale

Historical Example

- 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.

- **The Breakthrough of Frequency Analysis (1000)**

First page of al-Kindi's manuscript "On Deciphering Cryptographic Messages

- **Alberti's Cipher Disk (1467)**

Cipher Disk

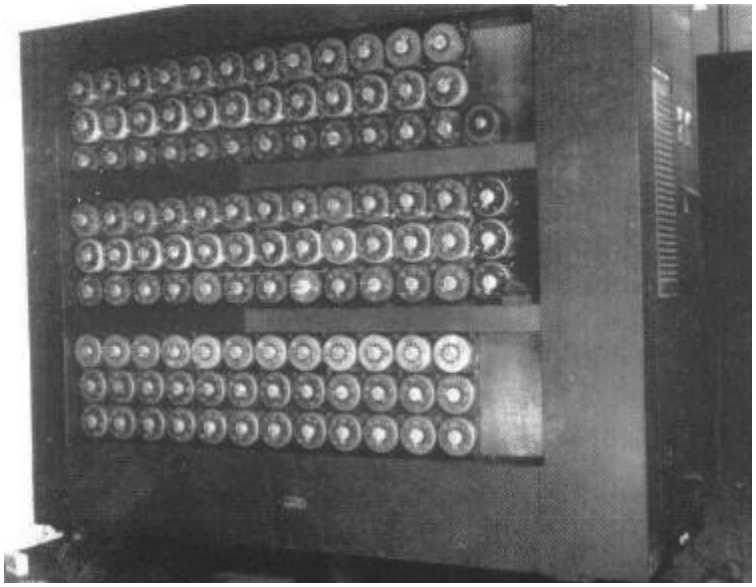
History

- **Scherbius' Enigma(1918)**

The Enigma machine looked

- Arthur Scherbius

- **Breaking the Enigma**



The British Bombe weighed
about 1 ton

- **Information Theory(1948-9)**

"A Mathematical Theory of Communication“

"Communication Theory of Secrecy Systems“

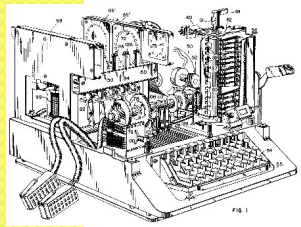
Claude Elwood Shannon

History of cryptography

Classical crypto: The earliest known use of cryptography is about 1900 BD

Medieval crypto: 800-1800 AD

Crypto from 1800 to WWII



Modern crypto

Crypto can be seen in everywhere

- **Advanced Encryption Standard(2001)**

V.Rijmen(right) and J.Daemen(left)

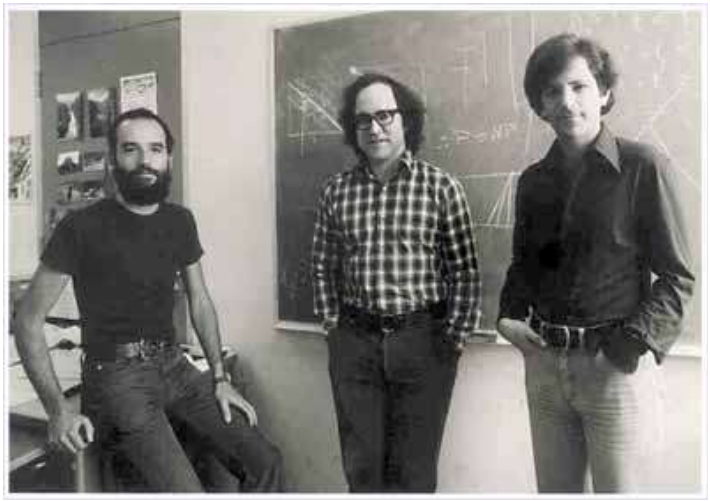
- **Public-Key Cryptography(1975)**

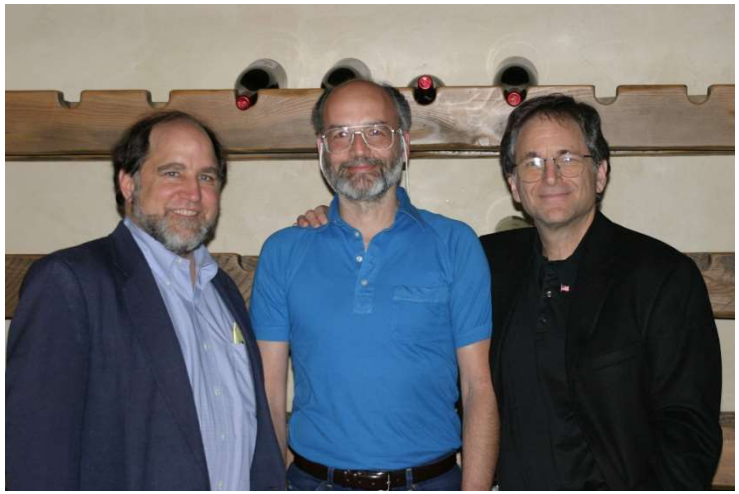
Whitfield Diffie, Martin Hellman and Ralph Merkle

Diffie ,Hellman and Mekle

(Merkle,Hellman and Diffie)

- **RSA (1977)**





Rivest, Shamir and Adleman

- **Quantum Cryptography_BB84(1984)**

Charles Bennett

- **Algorithms for Quantum Computers(1994)**

Peter Shor

- **Quantum Computing _First Successes(1998)**

Quantum Computer at IBM Almaden Research