CSCI971/471
Modern Cryptography

Subject Introduction

Jiageng Chen

Central China Normal University Wollongong Joint Institute

Contact details

- Associate Professor Jiageng Chen (陈嘉耕)
  - jiageng.chen@ccnu.edu.cn
  - QQ: 939288955
  - Office: 南湖综合楼 7080

- Lecture time:
  - Tuesday: 14:00 – 16:00, N319
- Tutorial time:
  - Thusday: 16:00 – 18:00 , N204 (two time slots)

Subject contact hours

- This subject is worth 6 credit points. Each week we will have a 2-hour lecture and a 1-hour workshop.

- According to University policy, 1 credit point is equivalent to 2 hours of work including class attendance, per week.

- So you should be doing about 9 hours of work a week on this subject outside of class attendance.

(Google and then learn the meaning of each concept)

The Moodle site

- The subject materials are available in Moodle

- Check the Moodle site for this subject regularly!
  - Any change to the subject will be announced on the Moodle site.
  - Any information posted to the Moodle site is deemed to have been notified to all students.

- Check SOLS mail too, since urgent updates are likely to be sent there.

What is this subject about

- Modern cryptography foundations and Their applications
  - Basic security concepts
  - Cryptographic primitives
  - Security definitions and models
  - Design and analysis of modern cryptographic systems
  - Applications of modern cryptosystems

Try my best to avoid mathematics! :)

Cryptography can be somewhat explained with a function *f(x)*

The objectives of this subject

1. Understand modern cryptographic techniques.
2. Undertake basic cryptanalysis on cryptographic schemes.
3. Apply appropriate techniques to design cryptographic schemes satisfying specific conditions.
4. Evaluate the design of modern cryptographic schemes.

No coding

No complex computation

But abstracted notions.

Subject contents

Week 1	Introduction
Week 2	Computational Complexity and Cryptographic Notions (1)
Week 3	Computational Complexity and Cryptographic Notions (2)
Week 4	Symmetric-Key Encryption
Week 5	Hash Function and MAC
Week 6	Public-key Encryption
Week 7	Digital signatures
Week 8	Identity-based cryptography
Week 9	Zero-knowledge Proof
Week 10	Secure Multi-Party Computation
Week 11	Modern Cryptography Applications I
Week 12	Modern Cryptography Applications II
Week 13	Revision

Recommended readings (No need to buy)

- A Graduate Course in Applied Cryptography version 0.6, D. Boneh and V. Shoup, 2023, http://toc.cryptobook.us
- Introduction to Modern Cryptography (3rd edition), Jonathan Katz, Yehuda Lindell, 2020
- Arora, Sanjeev, and Boaz Barak. Computational complexity: a modern approach. 2009
- Fuchun Guo, Willy Susilo, Yi Mu, Introduction to Security Reduction, Springer, 2018

Assessment tasks

- Two individual assignments (25% each)
  - Due in Week 5 & 12
  - problem solving, cryptographic algorithm/protocol design, cryptanalysis

- Final exam (50%)

Assignment submission

- Assignments must be submitted via the submission links in Moodle
- No email submission
- Penalties apply to all late work, except if student academic consideration has been granted.
- Late submissions will attract a penalty of 25% of the assessment mark per day including weekends.
- Work more than three (3) days late will be awarded a mark of zero.

Plagiarism

- There are two primary concerns for us:
  - Students copying each other.
    - You can discuss ideas but need to write down your solution independently!
    - With mathematical solutions you need to work fairly independently.
  - Students copying directly without appropriate referencing.

How do you pass this subject

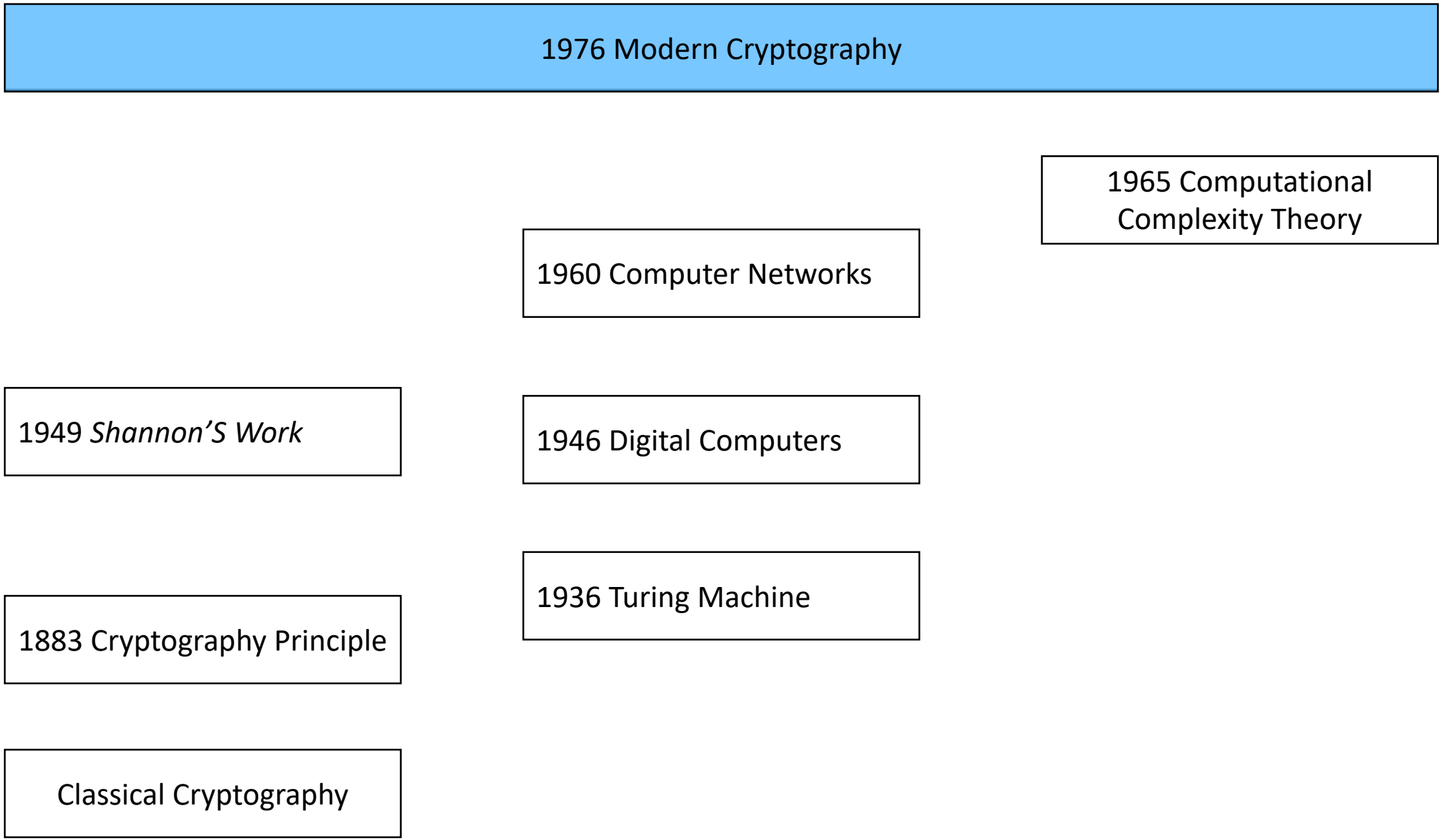
- You need to get at least 20/50 in the final exam.

AND

- Overall you need to get at least 50.

Questions?

Modern Cryptography Overview


1976 Modern Cryptography
1965 Computational Complexity Theory
1960 Computer Networks
1949 *Shannon'S Work*
1946 Digital Computers
1936 Turing Machine
1883 Cryptography Principle
Classical Cryptography

Steganography vs Cryptography

- Steganography
  - Also known as secret/covered writing
  - Hiding secret messages in public ones
  - Focused on hiding the presence of secret information, or communication channel
- Cryptography (before 1976)
  - The communication channel is public
  - Focused on transforming cleartext (plaintext) to ciphertext

• Steganography vs Cryptography

The HR manager received the following appraisal report one day:

"Bob, my assistant programmer, can always be found working hard at his desk. He works independently, without wasting company time talking to colleagues. Bob never thinks twice about helping fellow employees, and always finishes given assignments on time. Often he takes extended measures to complete his work, sometimes skipping coffee breaks. Bob is a dedicated individual who has absolutely no vanity in spite of his high accomplishments and profound knowledge in his field. I firmly believe that Bob can be classed as a valuable employee, the type which cannot be dispensed with. Consequently, I duly recommend that Bob be promoted to executive management, and a proposal will be executed as soon as possible."

The HR manager received the following appraisal report one day:

```
1  "Bob, my assistant programmer, can always be found
2  working hard at his desk. He works independently, without
3  wasting company time talking to colleagues. Bob never
4  thinks twice about helping fellow employees, and always
5  finishes given assignments on time. Often he takes extended
6  measures to complete his work, sometimes skipping coffee
7  breaks. Bob is a dedicated individual who has absolutely no
8  vanity in spite of his high accomplishments and profound
9  knowledge in his field. I firmly believe that Bob can be
10 classed as a valuable employee, the type which cannot be
11 dispensed with. Consequently, I duly recommend that Bob be
12 promoted to executive management, and a proposal will be
13 executed as soon as possible."
```

Later that day, the HR manager received the following addendum:

Addendum:

"Bob was standing over my shoulder while I wrote the report sent to you earlier today. Kindly *re-read* ONLY the odd numbered lines."

3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told, by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours,

Classical Cryptography

Cryptography

Cryptography (before 1883)

Cryptography = Encryption + Decryption

Encryption= Encryption Algorithm

Decryption=Decryption Algorithm

Cryptography (1883-1976)

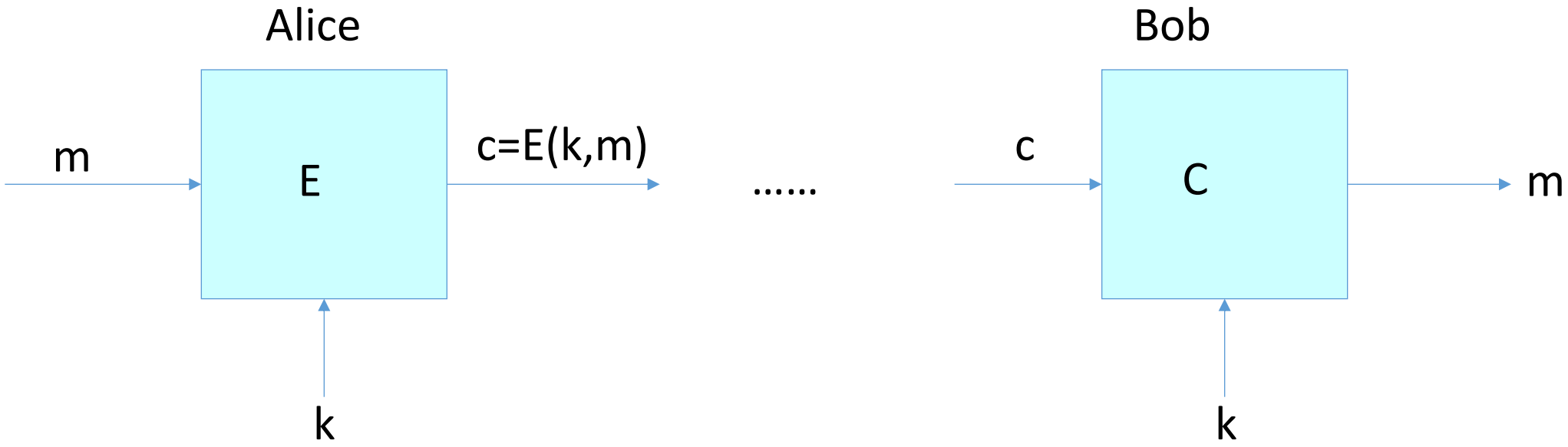
Cryptography = Encryption + Decryption

Encryption= Encryption Algorithm + Secret Key

Decryption=Decryption Algorithm + Secret Key

1. The system should be, if not theoretically unbreakable, unbreakable in practice.
2. The design of a system should not require secrecy, and compromise of the system should not inconvenience the correspondents (Kerckhoffs's principle).
3. The key should be memorable without notes and should be easily changeable.
4. The cryptograms should be transmittable by telegraph.
5. The apparatus or documents should be portable and operable by a s
6. The system should be easy, neither requiring knowledge of a long list

Symmetric Ciphers



Alice and Bob have the same key.

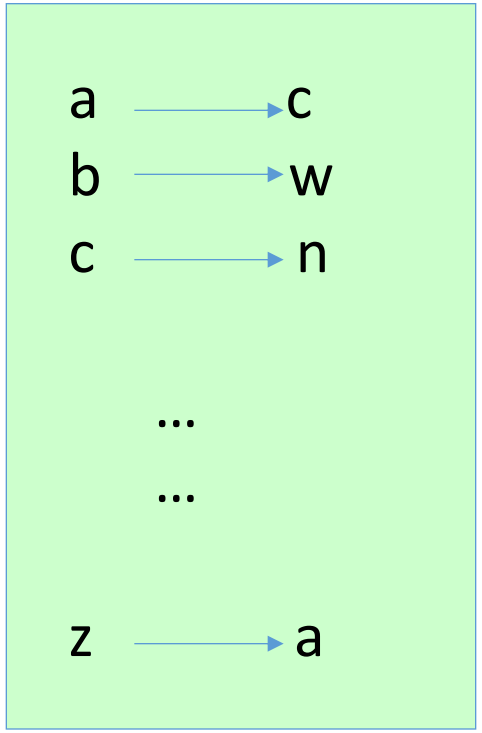
Few Historic Examples (all badly broken)

1. Substitution cipher

C =E(k, “bcza”)=“wnac”

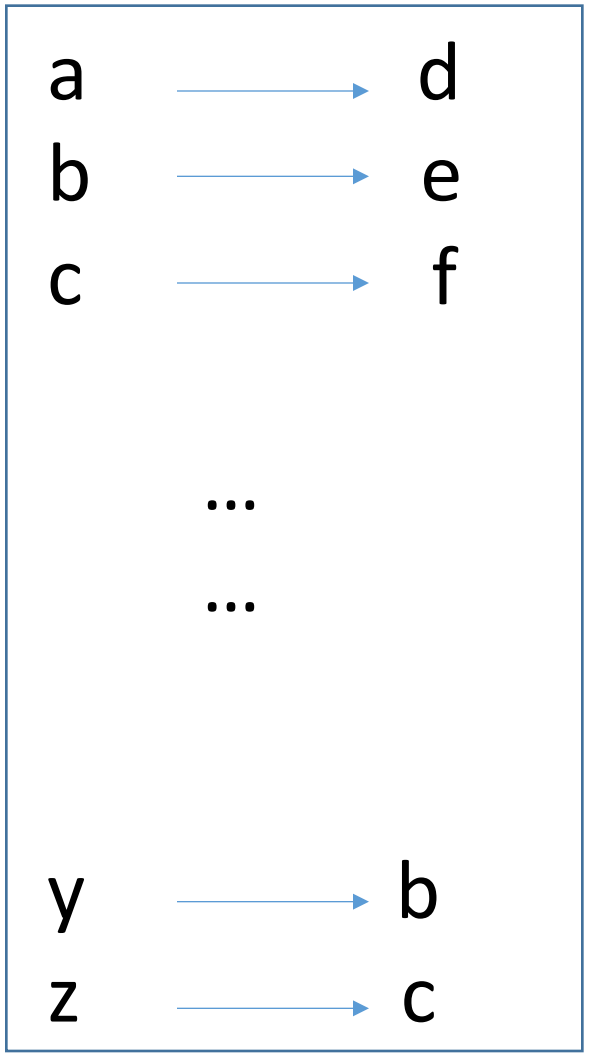
D(k,C)=“bcza”

k =



Caesar Cipher (no key)

Shift by 3:



What is the size of key space in the substitution cipher assuming 26 letters?

$$|\mathcal{K}| = 26$$

$$|\mathcal{K}| = 26!$$

$$|\mathcal{K}| = 2^{26}$$

$$|\mathcal{K}| = 26^2$$

How to break a substitution cipher?

What is the most common letter in English text?

“X”

“L”

“E” 

“H”

How to break a substitution cipher?

(1) Use frequency of English letters

“e”:12.7%, ”t”:9.1%, “a”:8.1%

(2) Use frequency of pairs of letters (digrams)

“he”, ”an”, “in”, “th”

⟹ CT only attack!

An Example

UKBYBIPOUZBCUFEEBORUKBYBHOBBRFESPVKBWFOFERVNBCVBZPRUBOFERVNBCVBPCYYFVUFOF
EIKNWFRFIKJNUPWRFIPOUNVNIPUBRNCUKBEFWWFDNCHXCYBOHOPYXPUBNCUBOYNRVNIWNC
POJIOFHOPZRVFZIXUBORJRUBZRBCHNCBBONCHRJZSFWNVRJRUBZRPCYZPUKBZPUNVPWPCYVFZI
XUPUNFCPWRVNBCVBRPYYNUNFCPWWJUKBYBIPOUZBCUIPOUNVNIPUBRNCHOPYXPUBNCUBOY
NRVNIWNCPOJIOFHOPZRNCRVNBCUNENVVFZIXUNCHPCYVFZIXUPUNFCPWZPUKBZPUNVR

B	36
N	34
U	33
P	32
C	26

➔ E

➔ T

➔ A

NC	11
PU	10
UB	10
UN	9

digrams

➔ IN

➔ AT

UKB	6
RVN	6
FZI	4

trigrams

➔ THE

2. Vigener cipher (16'th century, Rome)

k = **C R Y P T O C R Y P T O C R Y P T**

(+ mod 26)

m = **W H A T A N I C E D A Y T O D A Y**

---

c = **Z Z Z J U C L U D T U N W G C Q S**

suppose most common = "H" ⟶ first letter of key = "H" – "E" = "C"

3. Data Encryption Standard (1974)

DES: # keys = 2^{56} , block size = 64 bits

Today: AES (2001), Salsa20 (2008) (and many others)

1949 *Shannon'S Work*

Claude Shannon

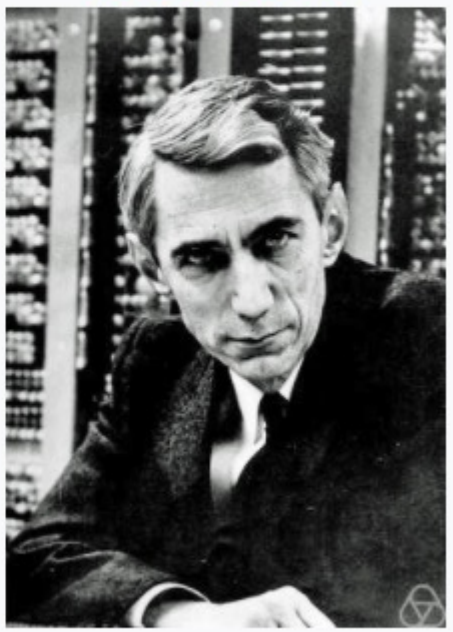
From Wikipedia, the free encyclopedia
(Redirected from Claude E. Shannon)

Claude Elwood Shannon (April 30, 1916 – February 24, 2001) was an American mathematician, electrical engineer, and cryptographer known as "the father of information theory".[1][2] Shannon founded information theory with a landmark paper, "A Mathematical Theory of Communication", which he published in 1948.

He also founded digital circuit design theory in 1937, when—as a 21-year-old master's degree student at the Massachusetts Institute of Technology (MIT)—he wrote his thesis demonstrating that electrical applications of Boolean algebra could construct any logical numerical relationship.[3] Shannon contributed to the field of cryptanalysis for national defense during World War II, including his fundamental work on codebreaking and secure telecommunications.

Contents [hide]

Claude Shannon



Born	April 30, 1916 Petoskey, Michigan, U.S.

Shannon'S Work

- Shannon joined Bell Labs to work on fire-control systems and cryptography during World War II
- At the close of the war, he prepared a classified report for Bell Telephone Labs entitled "A Mathematical Theory of Cryptography"
- In 1948, he published the paper "A Mathematical Theory of Communication" (Information Theory)
- In 1949, a declassified version of paper was published in 1949 as "Communication Theory of Secrecy Systems" in the Bell System Technical Journal. (Study Cryptography with Mathematics)

Shannon'S Work

- What kinds of cryptosystem can be broken.
  (Didn't consider the time cost. Hence called Theory research)

- What kinds of cryptosystem cannot be broken.
  (One-Time Pad)

X	Y	X ⊕ Y
0	0	0
0	1	1
1	0	1
1	1	0

One-Time Pad： K ⊕M

- Secret key is as long as messages to be encrypted
- Each secret key will be used once only
- Choose secret key randomly.

An important property of XOR

Thm: Y a rand. var. over $\{0,1\}^n$, X an indep. uniform var. on $\{0,1\}^n$

Then $Z := Y \oplus X$ is uniform var. on $\{0,1\}^n$

Proof: (for n=1)

$\Pr[Z=0] = \Pr[(X,Y)=(0,0) \text{ or } (X,Y)=(1,1)]$

$= \Pr[(X,Y)=(0,0)] + \Pr[(X,Y)=(1,1)]$

$= P_0/2 + P_1/2 = 1/2$

Y	Pr
0	P_0
1	P_1

X	Pr
0	½
1	½

X	Y	Pr
0	0	$P_0/2$
0	1	$P_1/2$
1	0	$P_0/2$
1	1	$P_1/2$

Independence

Def: events A and B are **independent** if $\Pr[A \text{ and } B] = \Pr[A] \cdot \Pr[B]$

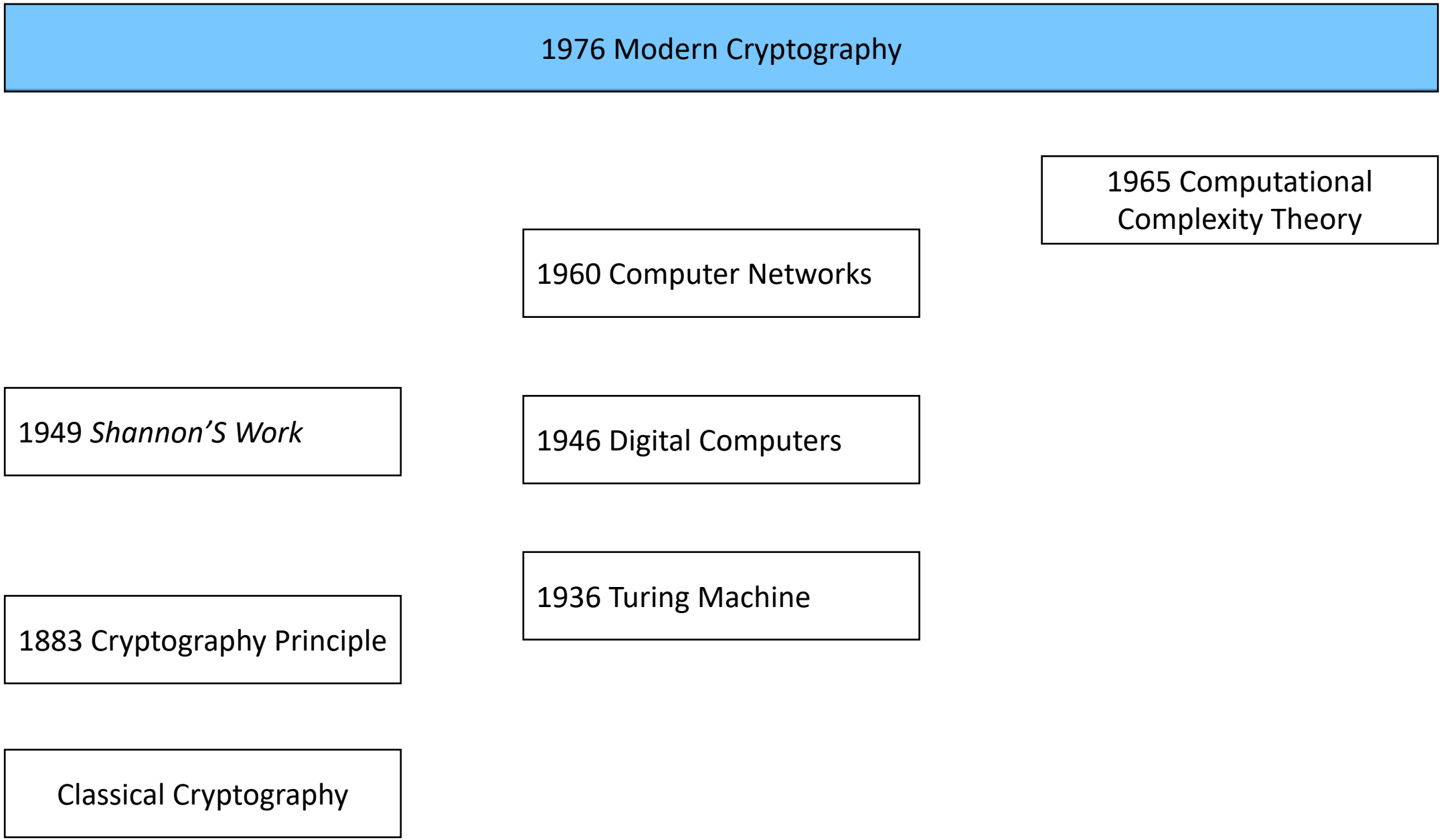
random variables X,Y taking values in V are **independent** if

$\forall a,b \in V$: $\Pr[X=a \text{ and } Y=b] = \Pr[X=a] \cdot \Pr[Y=b]$

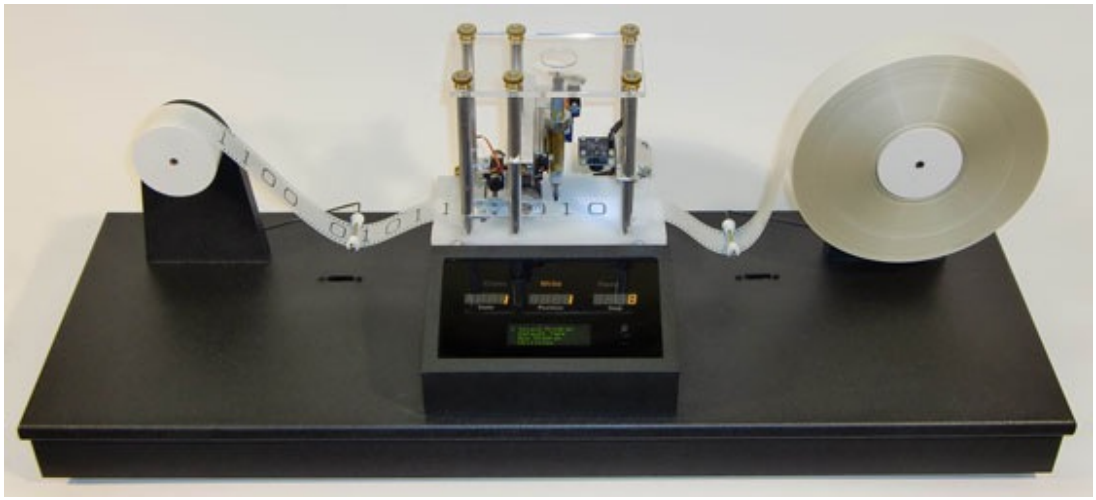
Example: $U = \{0,1\}^2 = \{00, 01, 10, 11\}$ and $r \xleftarrow{R} U$

Define r.v. X and Y as: $X = \text{lsb}(r)$, $Y = \text{msb}(r)$

$\Pr[X=0 \text{ and } Y=0] = \Pr[r=00] = ¼ = \Pr[X=0] \cdot \Pr[Y=0]$


1976 Modern Cryptography
1965 Computational Complexity Theory
1960 Computer Networks
1949 *Shannon'S Work*
1946 Digital Computers
1936 Turing Machine
1883 Cryptography Principle
Classical Cryptography

Alan Turing and Turing Machine



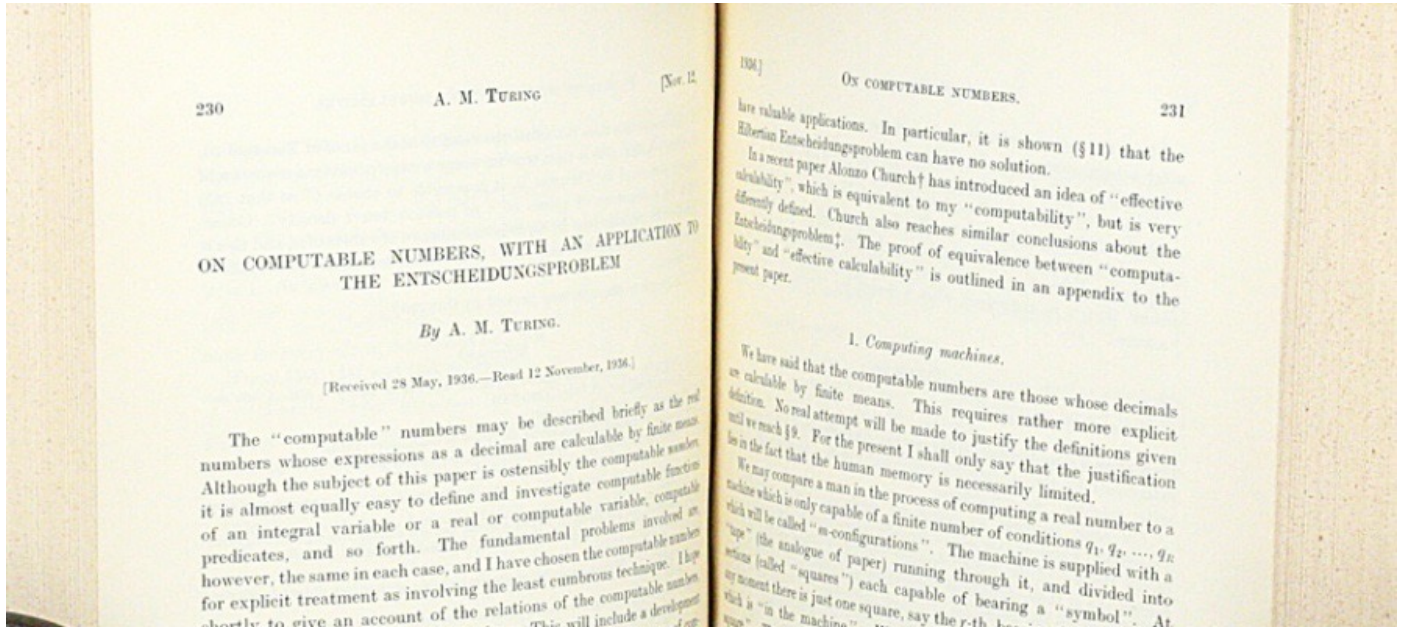
David Hilbert (1912)

Born	23 January 1862 Königsberg or Wehlau, Prussia
Died	14 February 1943 (aged 81) Göttingen, Nazi Germany

- One of the most influential mathematicians of the 19th and early 20th centuries.
- He proposed 32 open problems in mathematics in 1900
- In 1928, Hilbert Asked: Is Mathematics Complete, is it Consistent, and is it Decidable?

Decision Problem: Entscheidungsproblem

Can any problem be decidable with True or false?
Can any mathematic theorem be proved to be true or false?



230 A. M. TURING [Nov. 12,

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means. Although the subject of this paper is ostensibly the computable numbers, it is almost equally easy to define and investigate computable functions of an integral variable or a real or computable variable, computable predicates, and so forth. The fundamental problems involved are, however, the same in each case, and I have chosen the computable numbers for explicit treatment as involving the least cumbrous technique. I hope shortly to give an account of the relations of the computable numbers

1936.] ON COMPUTABLE NUMBERS. 231

have valuable applications. In particular, it is shown (§ 11) that the Hilbertian Entscheidungsproblem can have no solution.

In a recent paper Alonzo Church† has introduced an idea of "effective calculability", which is equivalent to my "computability", but is very differently defined. Church also reaches similar conclusions about the Entscheidungsproblem‡. The proof of equivalence between "computability" and "effective calculability" is outlined in an appendix to the present paper.

1. *Computing machines.*

We have said that the computable numbers are those whose decimals are calculable by finite means. This requires rather more explicit definition. No real attempt will be made to justify the definitions given until we reach § 9. For the present I shall only say that the justification lies in the fact that the human memory is necessarily limited.

We may compare a man in the process of computing a real number to a machine which is only capable of a finite number of conditions $q_1, q_2, \ldots, q_R$ which will be called "m-configurations". The machine is supplied with a "tape" (the analogue of paper) running through it, and divided into sections (called "squares") each capable of bearing a "symbol". At any moment there is just one square, say the r-th, bearing the symbol $\mathfrak{S}(r)$ which is "in the machine". At

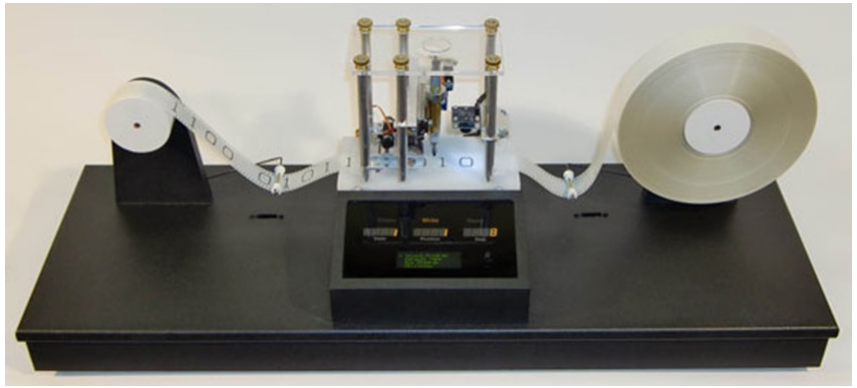
In 1936, Turing published his paper "On Computable Numbers, with an Application to the Entscheidungsproblem"

Some problems must be undecidable!

↓

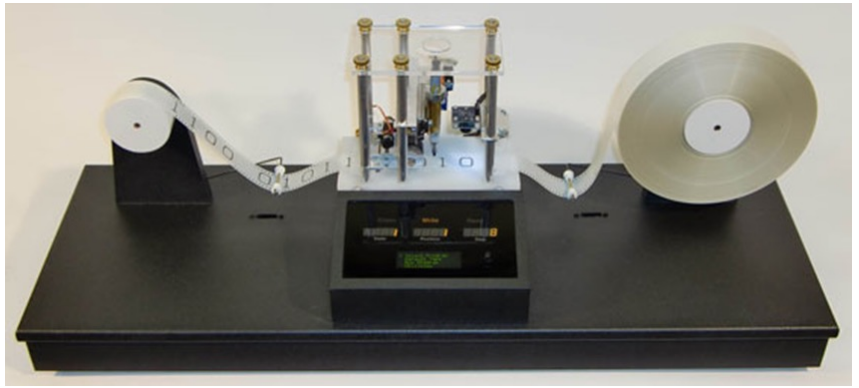
Turing Machine

Turing Machine



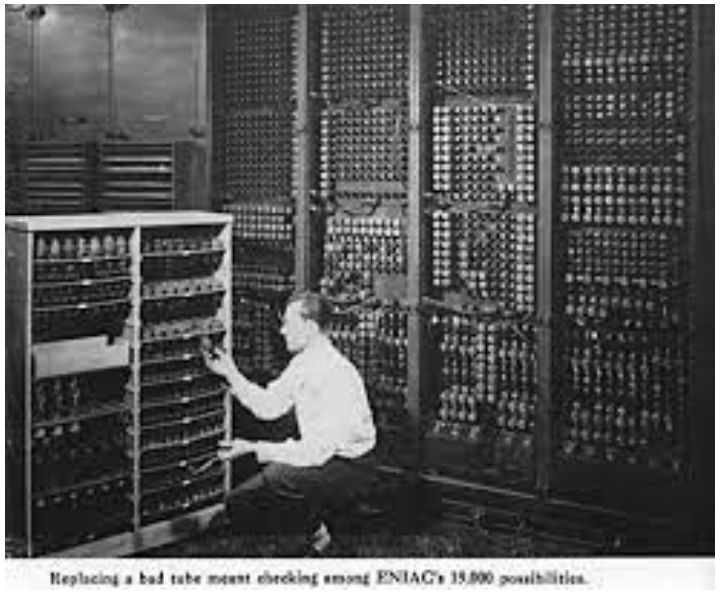
- Turing machine is not a computer but a computation model.
- The computation model can capture all computations by humans.
- If a computing device meets the computation model, it can perform computations as smart as humans. (theory only)

Turing Machine



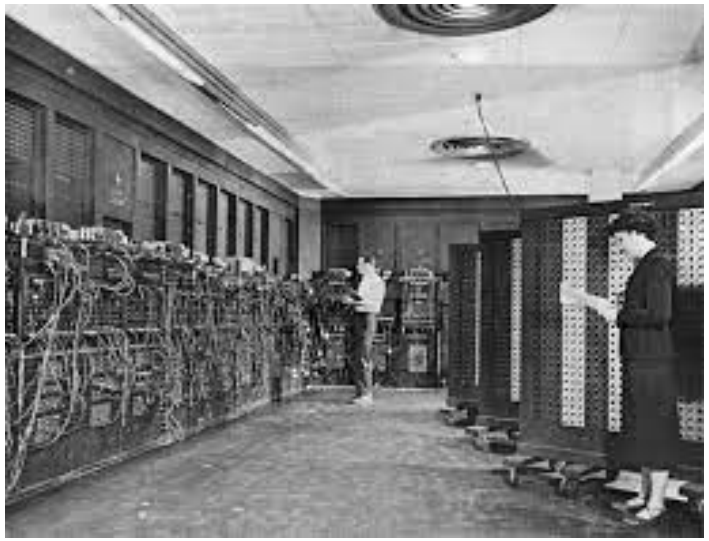
- A digital computer must provide computing ability captured by Turing machine. (We have computers 10 years later)
- A turning machine was later applied in studying computational complexity theory.

Computers and Network

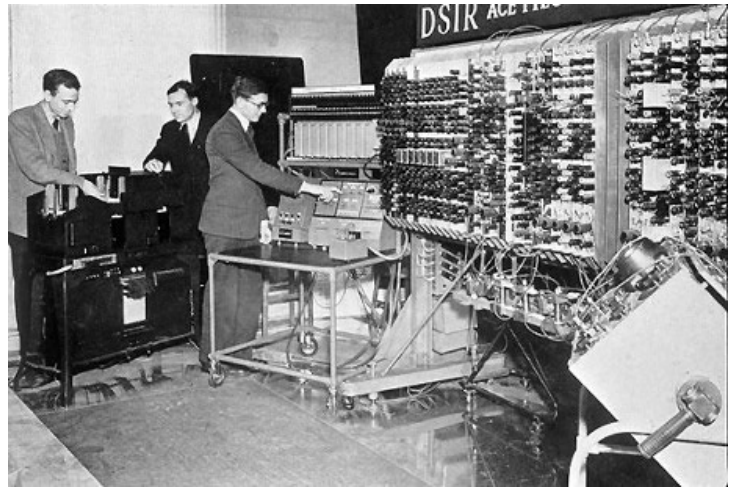


Replacing a bad tube meant checking among ENIAC's 19,000 possibilities.

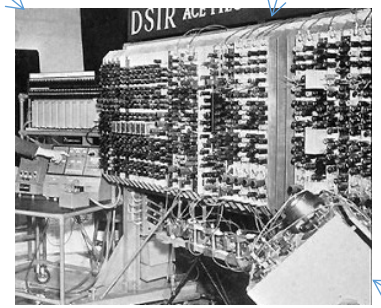
1.Computers
1940s



2.Networks
1960s



3. ATM



Bank Sever

How to keep our money safe?

- Computer Networks need protection with cryptography (encryption and decryption)
- Computers run encryption and decryption
- Need to design cryptography for business applications
- Cryptography should be strong against very powerful computers
- The first cryptography called Modern cryptography is **DES** in 1970s

1976 Public-Key Cryptography

New Directions in Cryptography
W.Diffie & M.E.Hellman

Hellman

Diffie

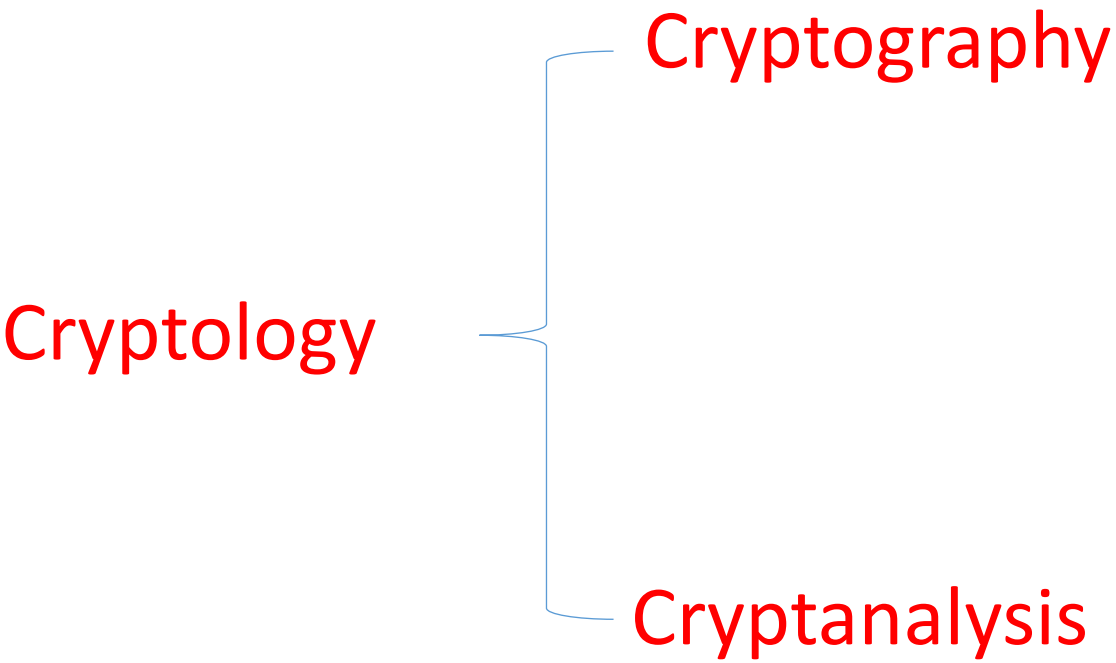
"We stand today on the brink of a revolution in cryptography"

After 1976

- Symmetric-Key Encryption
- Asymmetric-Key Encryption

- Message Authentication Code
- Digital Signatures
- Hash Function

- Security Protocols
  - ❑ Zero-Knowledge Proof
  - ❑ Identification Protocol
  - ❑ MPC
  - ❑ Commitment



Modern Cryptography

Formal study with mathematics. You can understand the meaning of each word but is hard to understand what it says.

Definition 3.8. An encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ had *indistinguishable encryption in the presence of an eavesdropper* if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there exists a negligible function negl such that

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n),$$

where the probability is taken over the random coins used by $\mathcal{A}$, as well as the random coins used by the experiment (for choosing the key, the random bit b, and any random coins used in the encryption process).

What we are NOT going to learn

- How to compute

$$= 12 + 7 \int_0^2 \left(-\frac{1}{4} \left(e^{-4t_1} + e^{4t_1 - 8} \right) \right) dt_1$$

What we are going to apply

- Given x and a function *f()*, You simply say: **compute *f(x)***

Like calling API during coding.

No need to understand how each API is generated.

Need to build a “software” with APIs.

END