SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

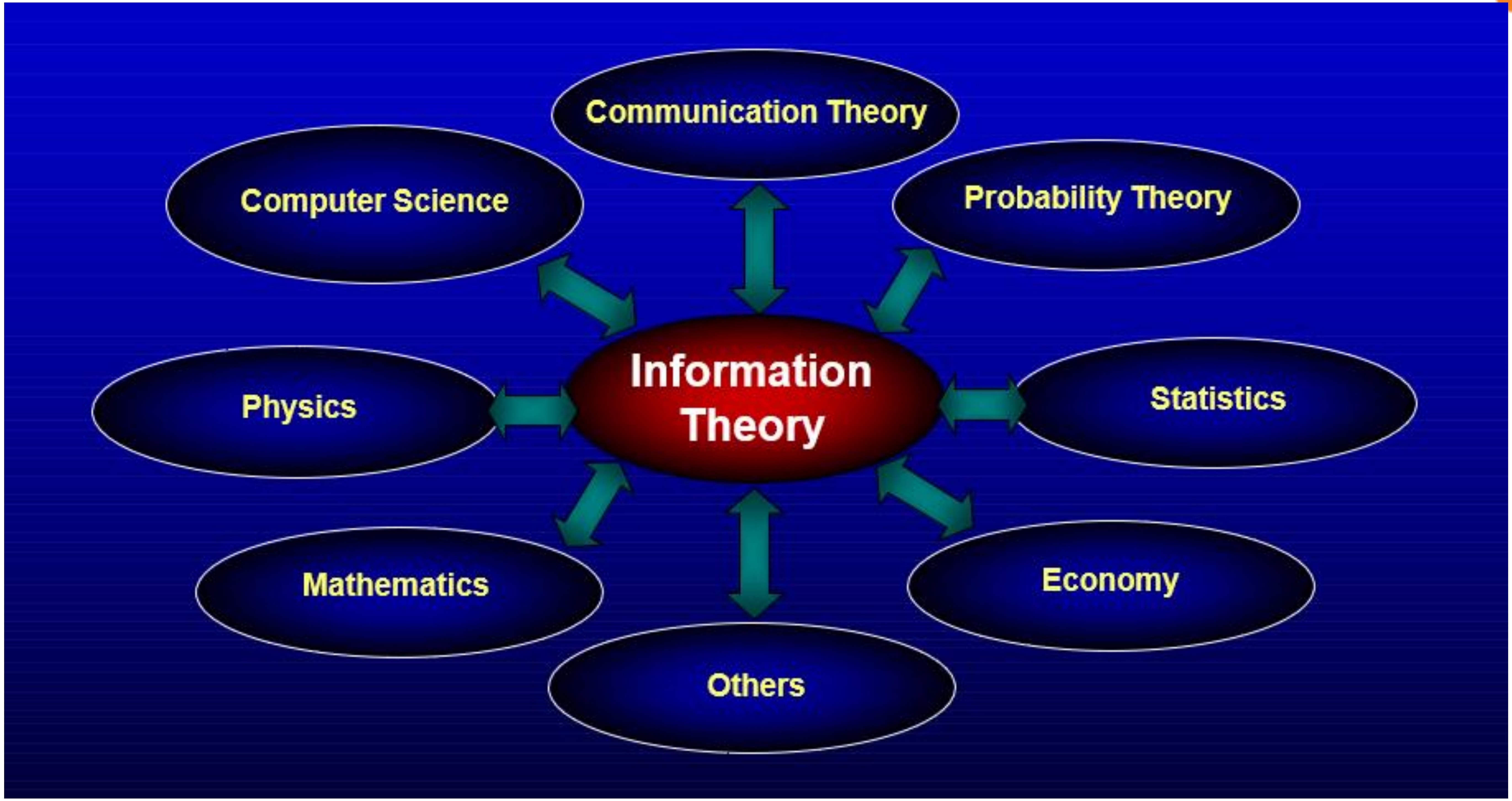
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE NAME : 19CS503 Cryptography and Network Security

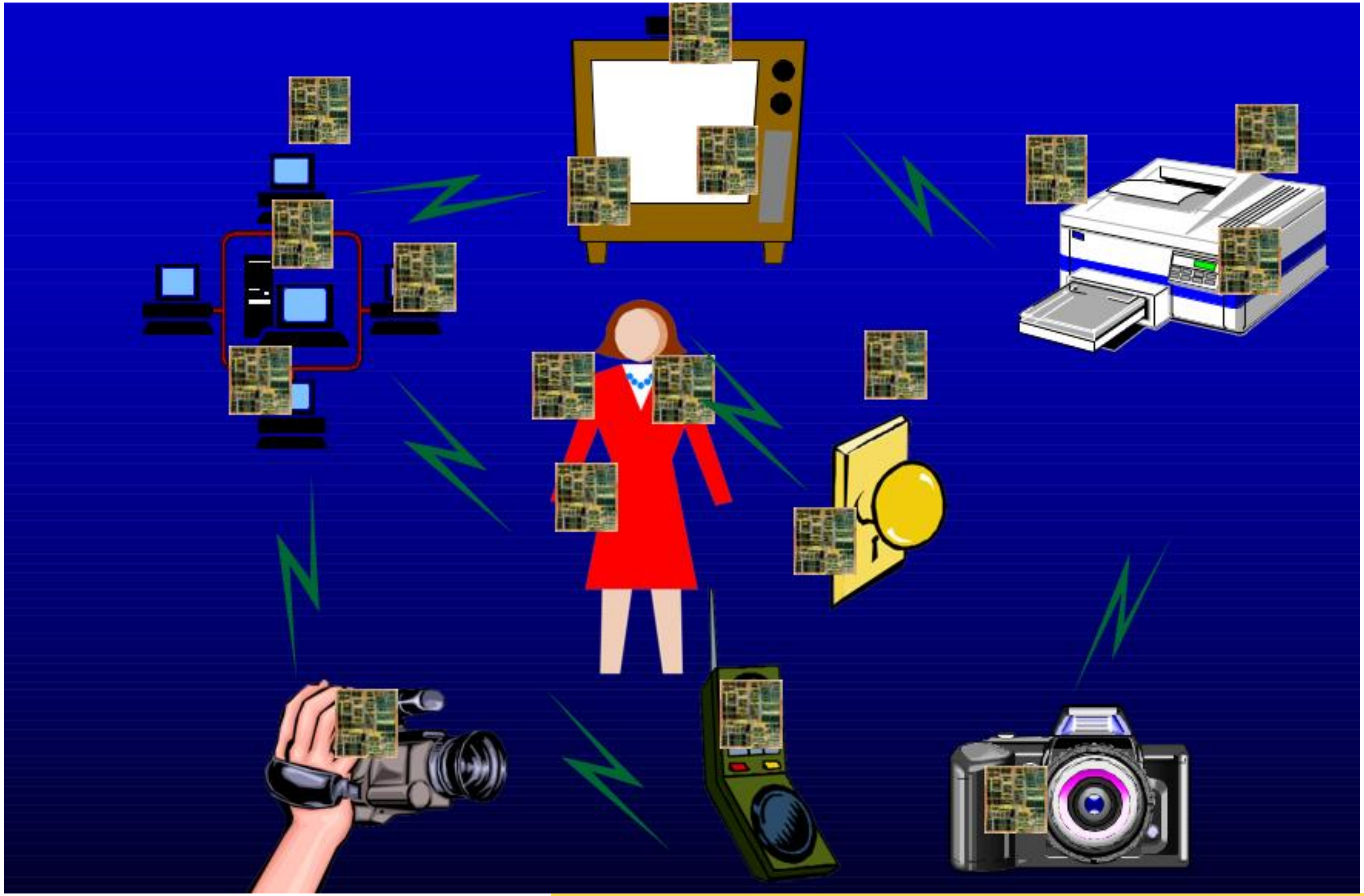
III YEAR /V SEMESTER

Unit 1- Introduction

Topic : Perfect security – Information theory – Product cryptosystem

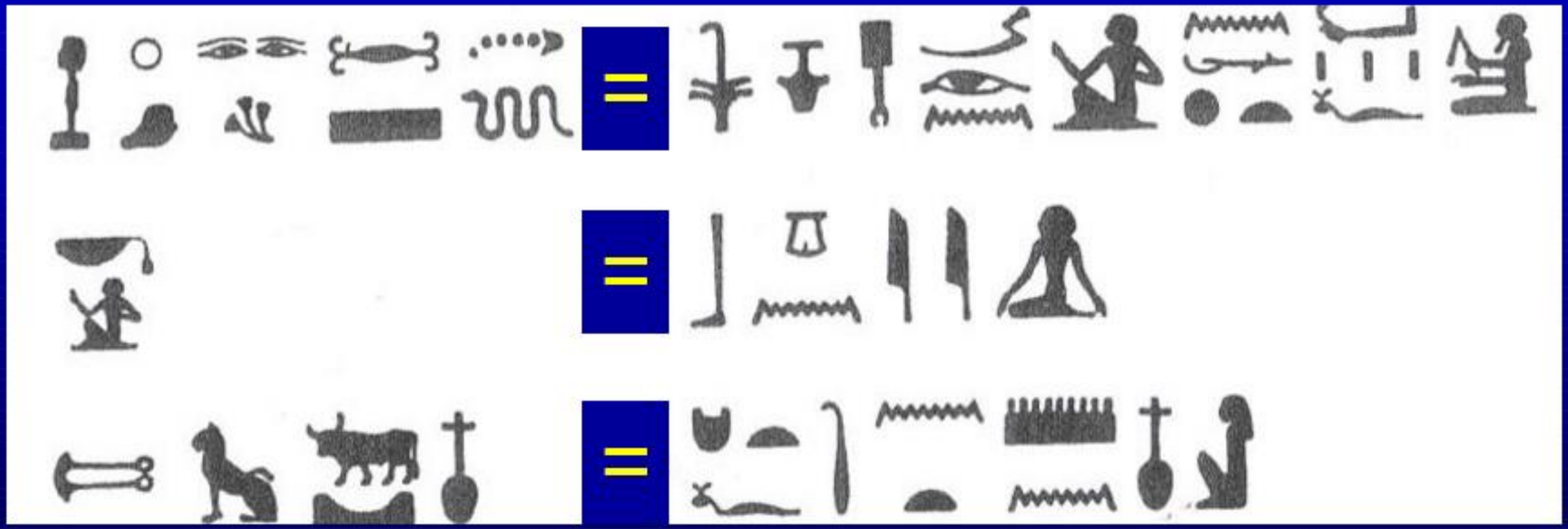

Communication Theory
Computer Science
Probability Theory
Information Theory
Physics
Statistics
Mathematics
Economy
Others

DIGITAL COMMUNICATION



EGYPTIAN

Cryptography, ca. 1900BC

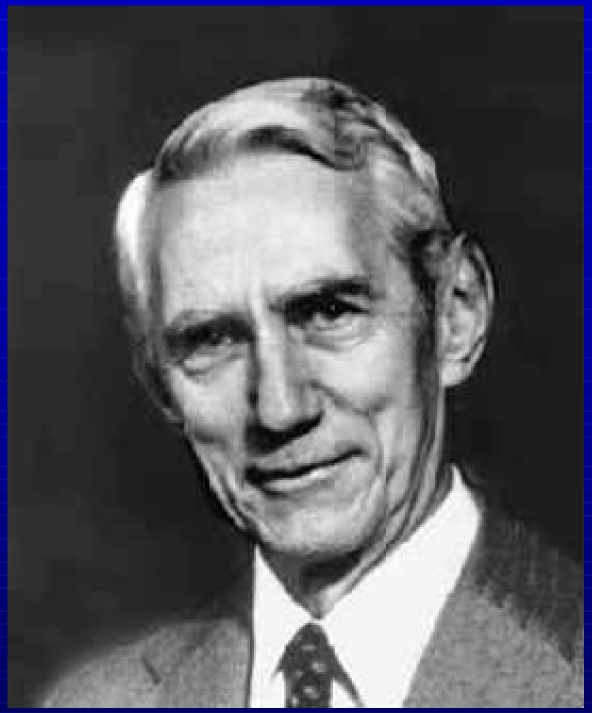


OVERVIEW OF INFORMATION THEORY HISTORY

"Claude Shannon's creation in the 1940's of the subject of information theory is arguably one of the great intellectual achievements of the twentieth century"

Bell Labs
Computing and Mathematical Sciences Research

http://cm.bell - labs.com/cm/ms/what/shannonday/work.html

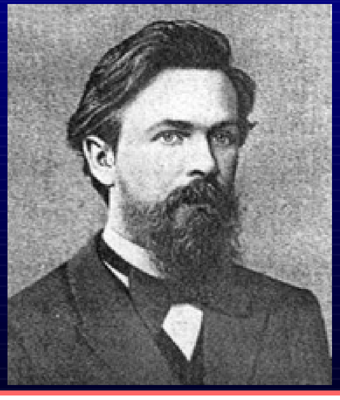


Claude Shannon

Father of Digital Communications

Andrei Andreyevich Markov

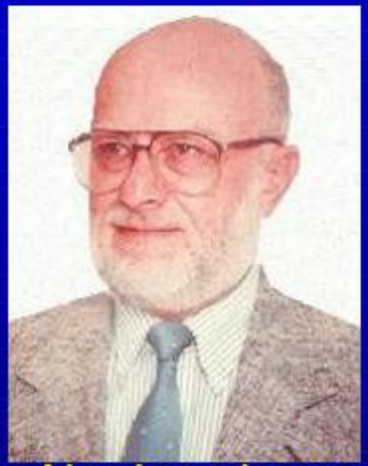
Markov is particularly remembered for his study of Markov chains, sequences of random variables in which the future variable is determined by the present variable but is independent of the way in which the present state arose from its predecessors. This work launched the theory of stochastic processes.



Born: 14 June 1856 in Ryazan, Russia
Died: 20 July 1922 in Petrograd (now St Petersburg), Russia

OVERVIEW OF INFORMATION THEORY HISTORY

The inventors


Abraham Lempel


Jacob Ziv

LZW (Lempel-Ziv-Welch) is an implementation of a lossless data compression algorithm created by Lempel and Ziv. It was published by Terry Welch in 1984 as an improved version of the LZ78 dictionary coding algorithm developed by Abraham Lempel and Jacob Ziv.

Fano

Shannon showed that it is possible to compress information. He produced examples of such codes which are now known as Shannon-Fano codes.

Robert Fano was an electrical engineer at MIT (the son of G. Fano, the Italian mathematician who pioneered the development of finite geometries and for whom the Fano Plane is named).

What is Information theory about ?

Information: knowledge that can be used

Communication: exchange of Information

Our goal: efficient; reliable; secure

Express everything in

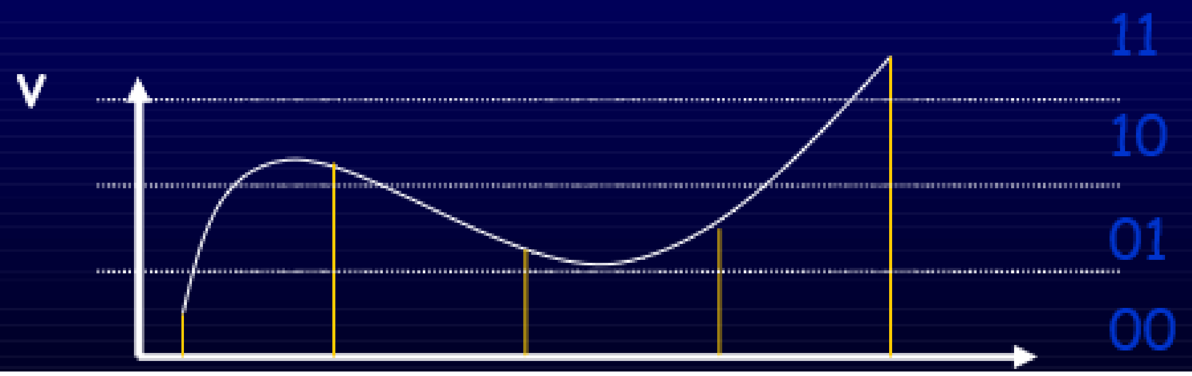
Discrete ensemble:

a,b,c,d $\Rightarrow$ 00, 01, 10, 11

in general: k binary digits specify 2^k messages

Analogue signal:

1) sample and 2) represent sample value binary



Output

00, 10, 01, 01, 11

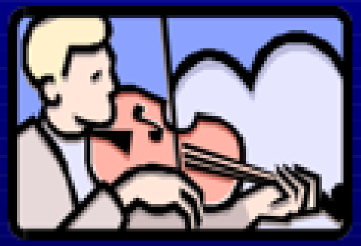
Efficient

text:

→ 1 book storage: = 4 Mbit 1 book

speech:

→ 45 minutes lecture = 45*60*64k =180Mbit 45 books



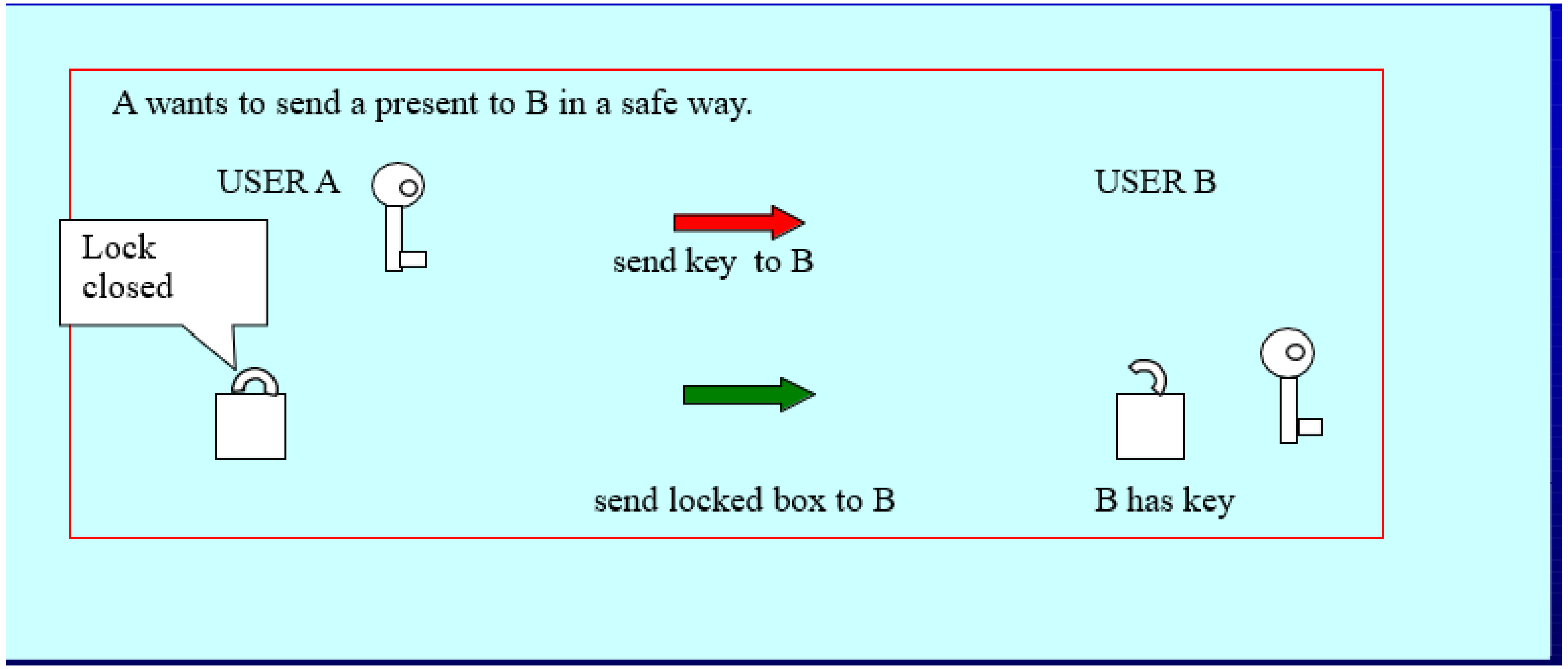
CD music:

→ storage capacity for one hour stereo: 5 Gbit 1250 books

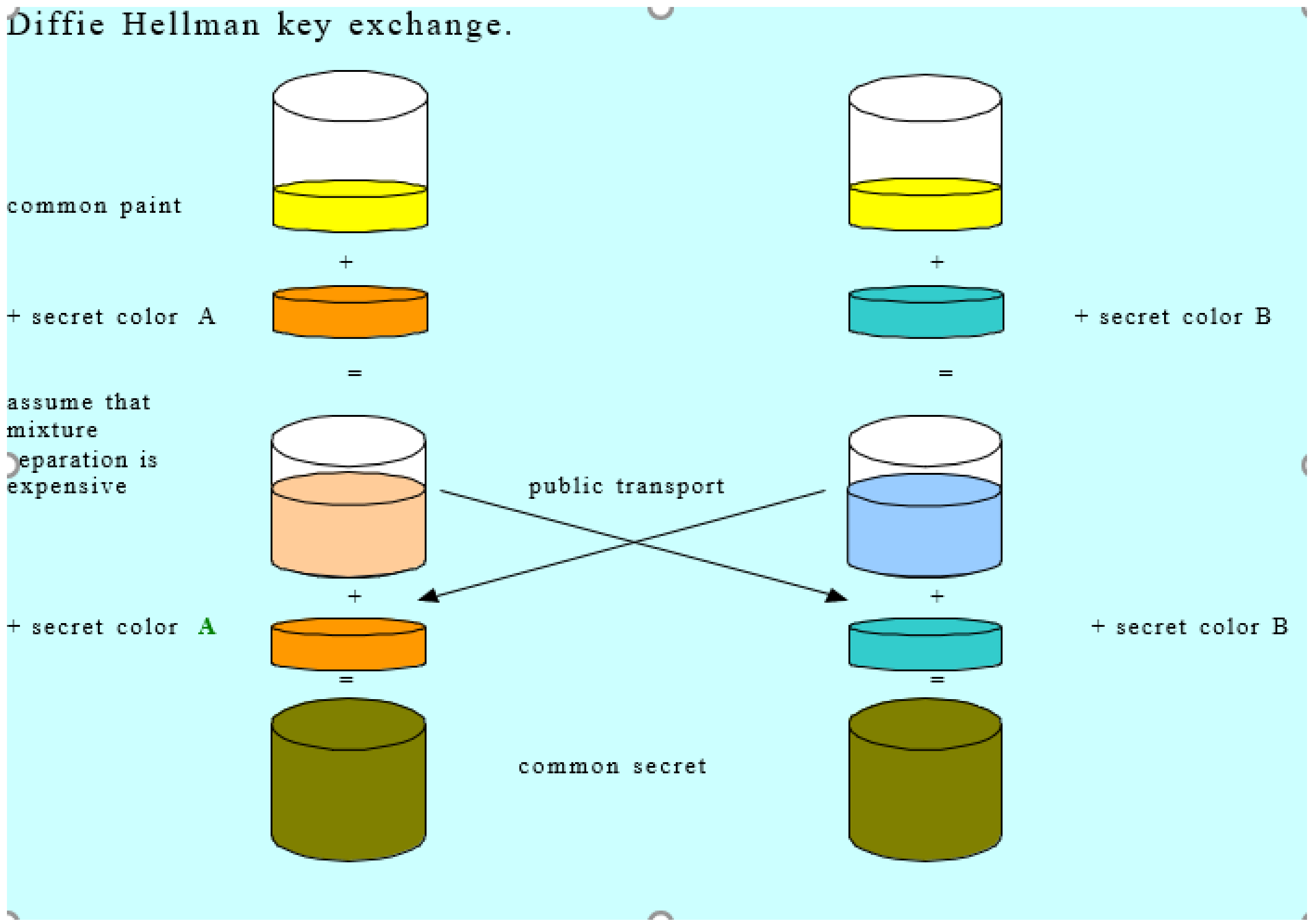
digital pictures:

→ 2 hour pictures need 540 Gbit 130.000 books

Secure

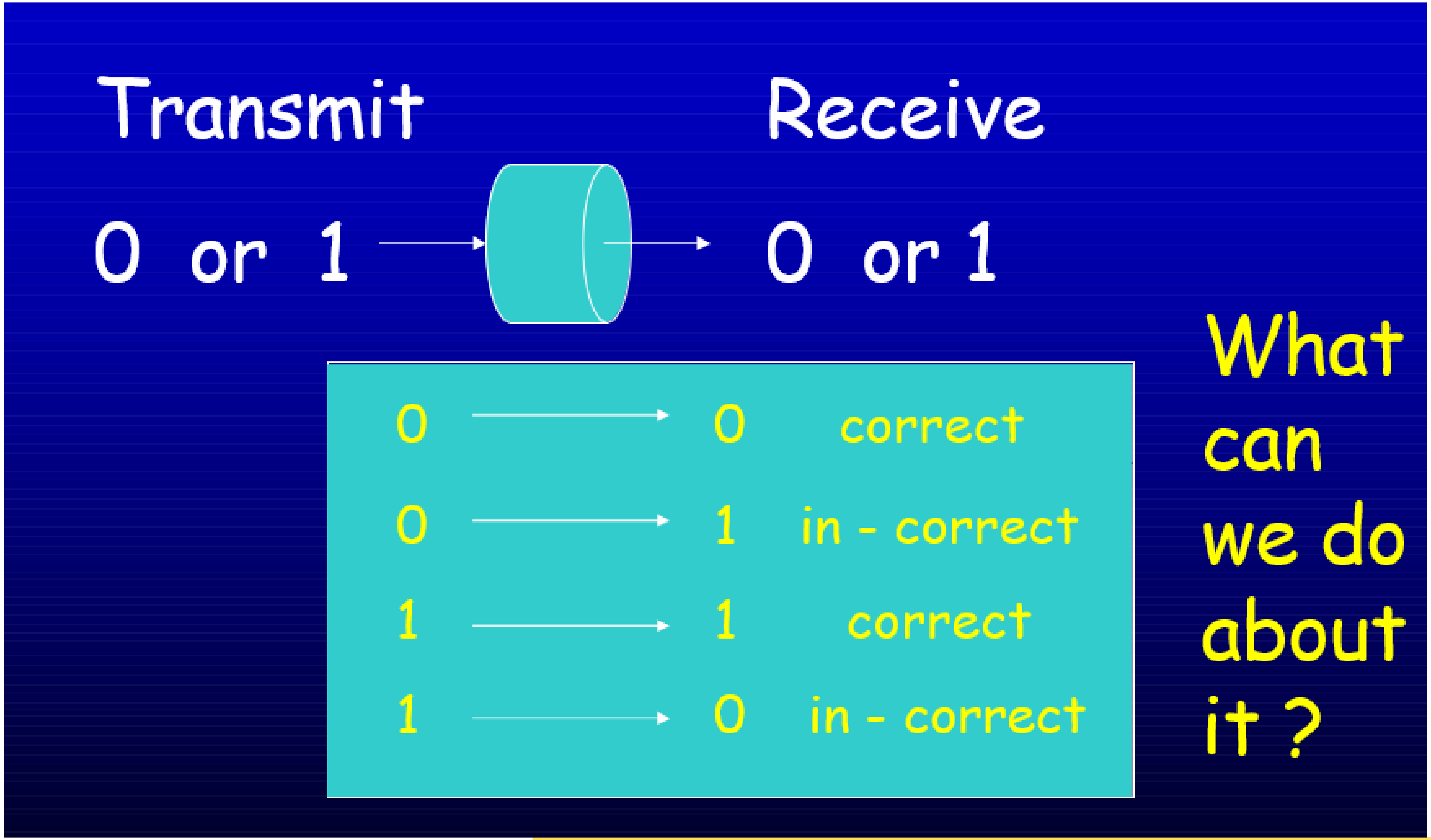


A wants to send a present to B in a safe way.
USER A
USER B
Lock
closed
send key to B
send locked box to B
B has key



Diffie Hellman key exchange.
common paint
+
+ secret color A
+ secret color B
=
assume that
mixture
separation is
expensive
public transport
+ secret color A
+ secret color B
=
common secret

Reliable


Transmit
Receive
0 or 1
0 or 1
0 → 0 correct
0 → 1 in - correct
1 → 1 correct
1 → 0 in - correct
What can we do about it ?

Perfect security -Cryptosystem

Cryptosystem

- The traditional main goal of cryptography is to preserve secrecy of the message, i.e. to transform it in the way that no unauthorized person can read the message while it is easily readable by authorized persons.
- First applications of message secrecy are known from ancient times and served to keep secret military and diplomatic secrets, craftsmanship methods and also love letters.
- Craftsmanship secrets on earthen tablets in Ancient Summer.
- Spartian Scytale.
- Secrets hidden in a wax table or under hair of a slave.
- Caesar cipher.

Cryptosystem

Definition

A encryption system (cipher) is a five-tuple $(\mathbf{P}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$, where

1. $\mathbf{P}$ is a finite set of possible plaintexts
2. $\mathbf{C}$ is a finite set of possible ciphertexts
3. $\mathbf{K}$ is a finite set of possible keys
4. For each $k \in \mathbf{K}$ there is an encryption rule $e_k \in \mathbf{E}$ and a corresponding decryption rule $d_k \in \mathbf{D}$. Each $e_k : \mathbf{P} \to \mathbf{C}$ and $d_k : \mathbf{C} \to \mathbf{P}$ are functions such that $d_k(e_k(x)) = x$ for every $x \in \mathbf{P}$.

Cryptosystem

Example

Example is e.g. the **shift cryptosystem**, sometimes known as the Caesar cipher. In this case $\mathbf{P} = \mathbf{C} = \mathbf{K} = \mathbb{Z}_{26}$. For $0 \le k \le 25$ we define

$$e_k(x) = (x + k) \bmod 26 \tag{1}$$

and

$$d_k(y) = (y - k) \bmod 26 \tag{2}$$

for $x, y \in \mathbb{Z}_{26}$.

Perfect Secrecy

To derive a definition of perfect secret we assume that there is some a priori distribution on plaintexts described by the random variable X with distribution $P(X = x)$. The key is chosen independently from the plaintext and described by the random variable K. Finally, ciphertext is described by the random variable Y that will be derived from X and K. Also, for $k \in \mathbf{K}$ we define $\mathbf{C}_k = \{e_k(x) | x \in \mathbf{X}\}$ as the set of all ciphertexts provided k is the key.

Now we can explicitly calculate the probability distribution of Y as

$$P(Y = y) = \sum_{k : y \in \mathbf{C}_k} P(K = k) P(X = d_k(y)). \tag{3}$$

Another quantity of interest is the probability of a particular ciphertext given a particular plaintex, easily derived as

$$P(Y = y | X = x) = \sum_{k : x = d_k(y)} P(K = k). \tag{4}$$

Perfect Secrecy

Definition

We say that the cryptosystem $(\mathbf{P}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ achieves **perfect (unconditional) secrecy** if and only if for every $x \in \mathbf{X}$ and $y \in \mathbf{Y}$ it holds that

$$P(X = x|Y = y) = P(X = x). \tag{5}$$

In words, the a posteriori probability distribution of plaintext given the knowledge of ciphertext is the same as the a priori probability distribution of the plaintext.

Following our previous analysis we calculate the conditional probability of a (possibly insecure) cryptosystem as

$$P(X = x|Y = y) = \frac{P(X = x) \sum_{k: x = d_k(y)} P(K = k)}{\sum_{k: y \in \mathbf{C}_k} P(K = k) P(X = d_k(y))}. \tag{6}$$

Perfect Secrecy

Theorem

Suppose the 26 keys in the Shift cipher are used with equal probability 1/26. Then for any plaintext distribution the Shift cipher achieves perfect secrecy.

Proof.

Recall that **P** = **C** = **K** = $\mathbb{Z}_{26}$. First we compute the distribution of ciphertexts as

$$
\begin{aligned}
P(Y = y) &= \sum_{k \in \mathbb{Z}_{26}} P(K = k) P(X = d_k(y)) \\
&= \sum_{k \in \mathbb{Z}_{26}} \frac{1}{26} P(X = y - k) \\
&= \frac{1}{26} \sum_{k \in \mathbb{Z}_{26}} P(X = y - k).
\end{aligned} \tag{7}
$$

Perfect Secrecy

Proof.

For fixed y the values $(y - k) \bmod 26$ are a permutation of $\mathbb{Z}_{26}$ and we have that

$$\sum_{k \in \mathbb{Z}_{26}} P(X = y - k) = \sum_{x \in \mathbb{Z}_{26}} P(X = x) = 1. \tag{8}$$

Thus for any $y \in \mathbf{Y}$ we have

$$P(Y = y) = \frac{1}{26}.$$

Next, we have that

$$P(Y = y | X = x) = P(K \equiv (y - x) \pmod{26}) = \frac{1}{26}$$

for every x and y. $\square$

Perfect Secrecy

Proof.

Using the Bayes' theorem we have

$$P(X = x|Y = y) = \frac{P(X = x)P(Y = y|X = x)}{P(Y = y)} = \frac{P(X = x)\frac{1}{26}}{\frac{1}{26}} \qquad (9)$$

$$= p(X = x)$$

what completes the proof. □

The previous result shows that the shift cipher is unbreakable provided we use an independent key for each plaintext character.

Perfect Secrecy

- If $P(X = x0) = 0$ for some $x0 \in P$, then we trivially obtain
- $P(X = x0|Y = y) = P(X = x0)$. Therefore we consider only elements such that $P(X = x) > 0$.
- For such plaintexts we observe that $P(X = x|Y = y) = P(X = x)$ is equivalent to $P(Y = y|X = x) = P(Y = y)$.
- Let us suppose that $P(Y = y) > 0$ for all $y \in C$. Otherwise y can be excluded from C since it is useless.
- Fix $x \in P$. For each $y \in C$ we have
- $P(Y = y|X = x) = P(Y = y) > 0$. Therefore for each $y \in C$ there must be some key $k \in K$ such that $y = ek(x)$. It follows that
- $|K| \geq |C|$.
- The encryption is injective giving $|C| \geq |P|$.

Perfect Secrecy

- If $P(X = x0) = 0$ for some $x0 \in P$, then we trivially obtain
- $P(X = x0|Y = y) = P(X = x0)$. Therefore we consider only elements such that $P(X = x) > 0$.
- For such plaintexts we observe that $P(X = x|Y = y) = P(X = x)$ is equivalent to $P(Y = y|X = x) = P(Y = y)$.
- Let us suppose that $P(Y = y) > 0$ for all $y \in C$. Otherwise y can be excluded from C since it is useless.
- Fix $x \in P$. For each $y \in C$ we have
- $P(Y = y|X = x) = P(Y = y) > 0$. Therefore for each $y \in C$ there must be some key $k \in K$ such that $y = ek(x)$. It follows that
- $|K| \geq |C|$.
- The encryption is injective giving $|C| \geq |P|$.

Perfect Secrecy

Theorem (Shannon)

Let $(\mathbf{P}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ *be a cryptosystem such that* $|\mathbf{P}| = |\mathbf{C}| = |\mathbf{K}|$. *Then the cryptosystem provides perfect secrecy if and only if every key is used with equal probability* $1/|\mathbf{K}|$, *and for every* $x \in \mathbf{P}$ *and every* $y \in \mathbf{C}$, *there is a unique key* k *such that* $e_k(x) = y$.

Proof.

Let us suppose the given cryptosystem achieves a perfect secrecy. As argued above for each x and y there must be at least one key such that $e_k(x) = y$. We have the inequalities

$$|\mathbf{C}| = |\{e_k(x) : k \in \mathbf{K}\}| \leq |\mathbf{K}|. \tag{10}$$

Perfect Secrecy

Proof.

We assume that $|\mathbf{C}| = |\mathbf{K}|$ and therefore

$$|\{e_k(x) : k \in \mathbf{K}\}| = |\mathbf{K}|$$

giving there do not exist two different keys $k_1, k_2 \in \mathbf{K}$ such that $e_{k_1}(x) = e_{k_2}(x) = y$. hence, for every x and y there is exactly one k such that $e_k(x) = y$.

Denote $n = |\mathbf{K}|$, let $\mathbf{P} = \{x_i \mid 1 \leq i \leq n\}$ and fix a ciphertext element y.

We can name keys $k_1, k_2, \ldots, k_n$ in the way that $e_{k_i}(x_i) = y$. Using Bayes' theorem we have

$$\begin{aligned} P(X = x_i \mid Y = y) &= \frac{P(Y = y \mid X = x_i) P(X = x_i)}{P(Y = y)} \\ &= \frac{P(K = k_i) P(X = x_i)}{P(Y = y)}. \end{aligned} \tag{11}$$

Perfect Secrecy

Proof.

The perfect secrecy condition gives $P(X = x_i \mid Y = y) = P(X = x_i)$ and we have $P(K = k_i) = P(Y = y)$. This gives that all keys are used with the same probability. Since there are $|\mathbf{K}|$ keys, the probability is $1/|\mathbf{K}|$. Conversely, suppose the conditions are satisfied and we want to show perfect secrecy. The proof is analogous to the proof of perfect secrecy of the Shift cipher.

Assessment

Let (P, C, K, E, D) be a cryptosystem such that |P| = |C| = |K|. Then the cryptosystem provides perfect secrecy if and only if every key is used with equal probability 1/|K|, and for every x ∈ P and every y ∈ C, there is a unique key k such that ek (x) = y.

REFERENCES

1. William Stallings, Cryptography and Network Security, 6 th Edition, Pearson Education, March 2713.

THANK YOU