EWSCS'06

Palmse, Estonia
5-10 March 2006

Lecture 1: Shannon's Theory of Secrecy and its Extension to Authenticity

James L. Massey

Prof.-em. ETH Zürich, Adjunct Prof., Lund Univ., Sweden, and Tech. Univ. of Denmark
Trondhjemsgade 3, 2TH
DK-2100 Copenhagen East

JamesMassey@compuserve.com

Cryptology

("hidden word")

Cryptography

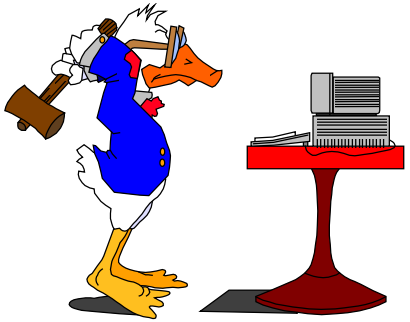
(code making)

The "good guys"

Cryptanalysis

(code breaking)

The "bad guys"

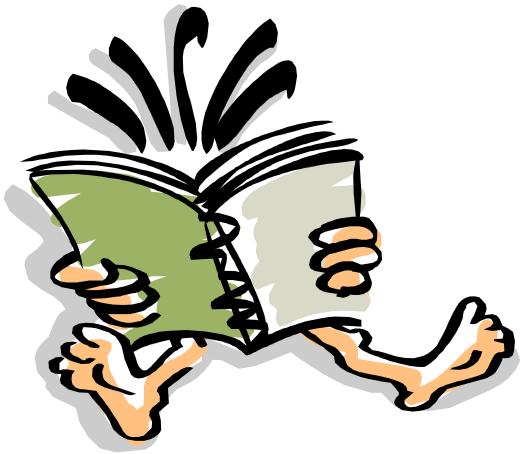


Goals of cryptography

Secrecy **Authenticity**

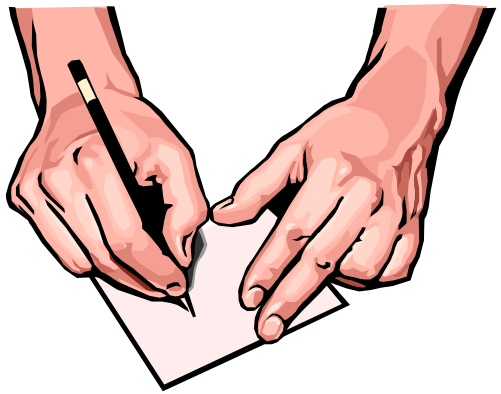
Xuejia Lai has given a useful **razor** for deciding whether something is a matter of secrecy or a matter of authenticity.

Secrecy - concerned with who has **access** to (or can **read**) a legitimate message.



Secrecy deals with **safeguarding the future** by ensuring that **only authorized recipients will be able to gain access** to (or read) a legitimate message.

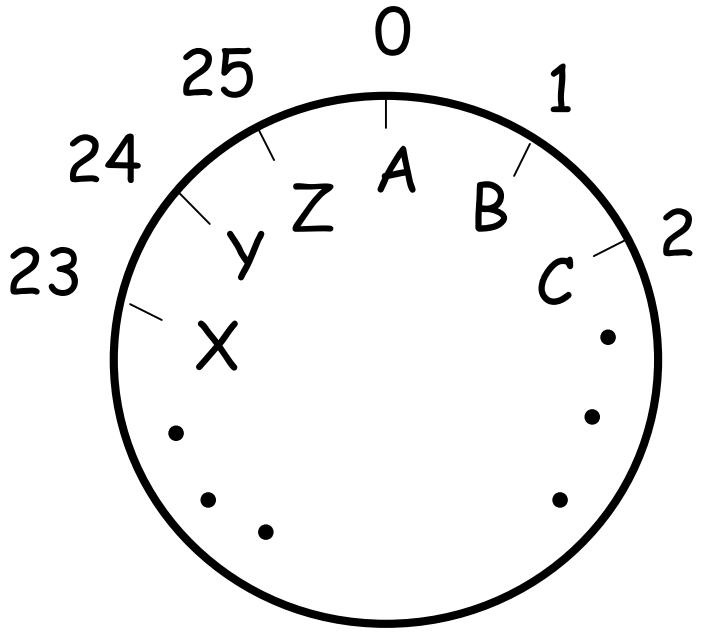
Authenticity - concerned with who can **create** (or **write**) a legitimate message.



Authenticity deals with **protecting the past** by

- ensuring that the creator (or author) was **entitled to create** (or write) the message
- ensuring that the **contents** of the message **have not been altered**

A secrecy scheme: The Caesar Cipher



Arithmetic on a CIRCLE
(Modulo 26 arithmetic)

Encrypt = Add 3
(move **clockwise 3** places)

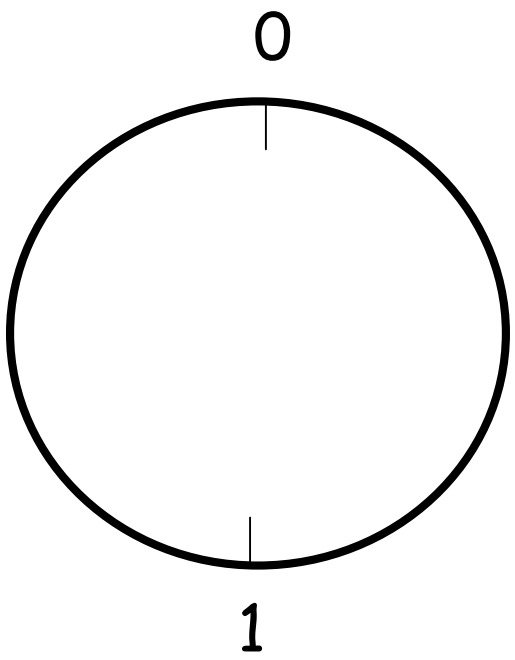
Decrypt = Subtract 3
(move **counterclockwise 3** places)

SECRET KEY = 3

C A E S A R ← plaintext
F D H V D U ← ciphertext

M A S S E Y ← plaintext
P D V V H B ← ciphertext

Today we use a **SMALLER CIRCLE**!



Arithmetic on this CIRCLE
(**Modulo 2** arithmetic)

Encrypt = **Add**
(move **clockwise**)

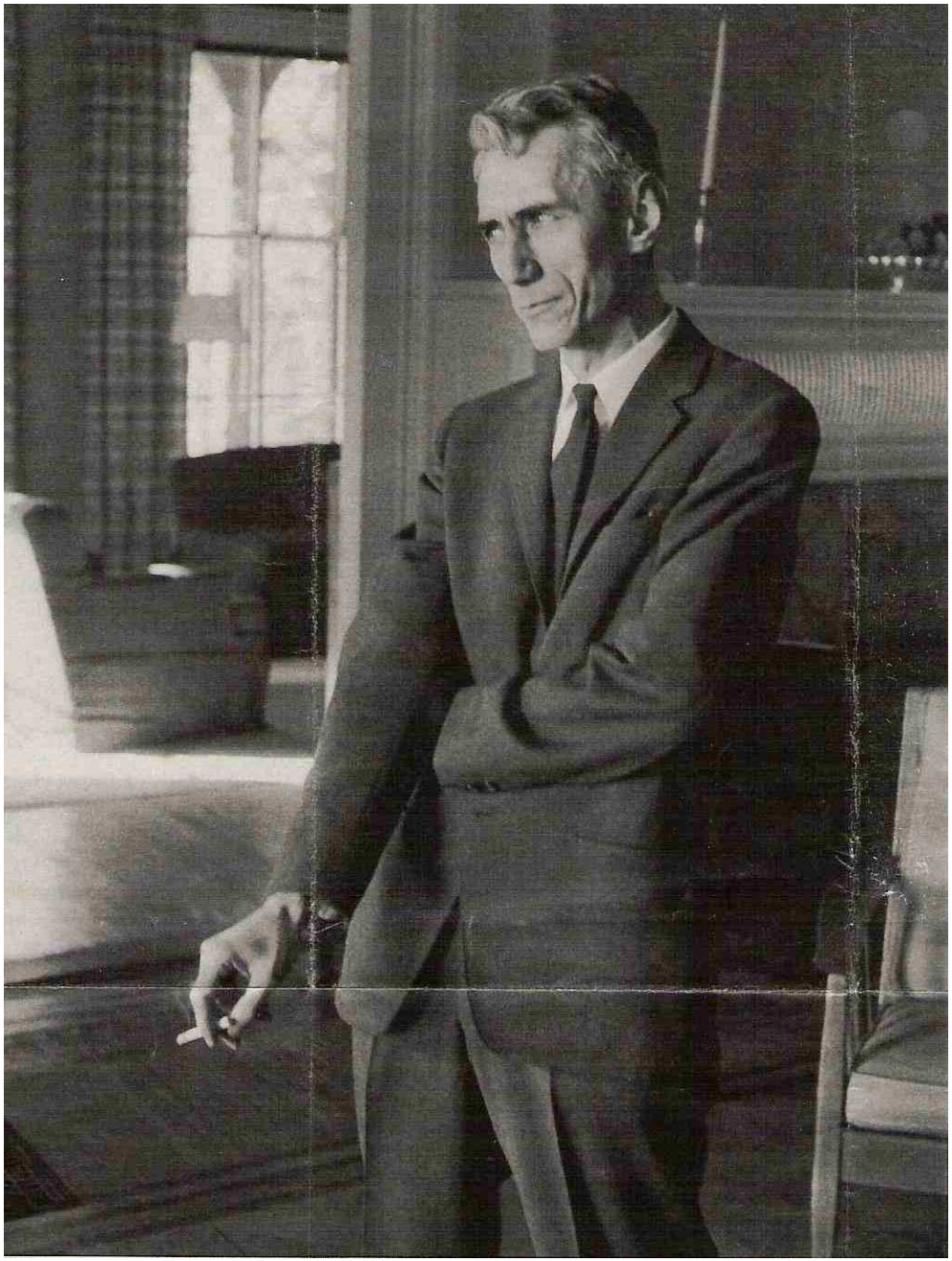
Decrypt = **Subtract**
(move counterclockwise)
= (move **clockwise**)

⇒ **Decrypt** = **Encrypt**

and a **LONGER SECRET KEY**!

1	0	0	1	1	1	0	1	← plaintext
0	1	1	0	0	1	1	1	← secret key
1	1	1	1	1	0	1	0	← ciphertext

Everybody likes to make secret codes!



Photograph of Shannon at home in 1962. (from the *New York Times Magazine*, 30 December 2001)

"As a first step in the mathematical analysis of cryptography, it is necessary to idealize the situation suitably, and to define in a mathematically acceptable way what we shall mean by a secrecy system."

C.E. Shannon, "Communication Theory of Secrecy Systems", *Bell System Tech. J.*, vol. 28, pp. 656-715, Oct., 1949.

This was a radical departure from previous papers in cryptography where (as in Steen and Stoffer) conjecture and imprecision reigned.

Just how did Shannon define a secrecy system in "a mathematically acceptable way"?

He drew a picture!

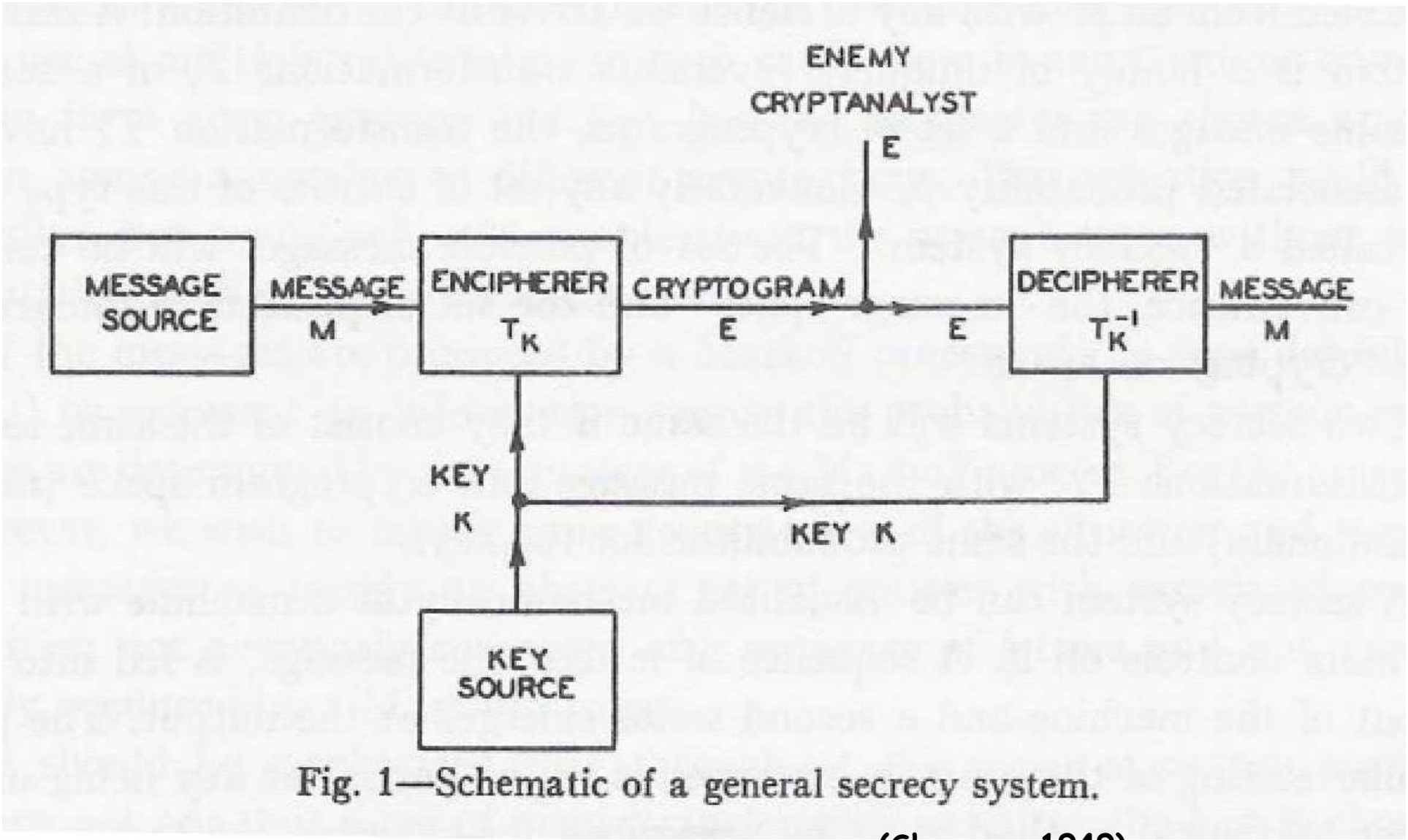
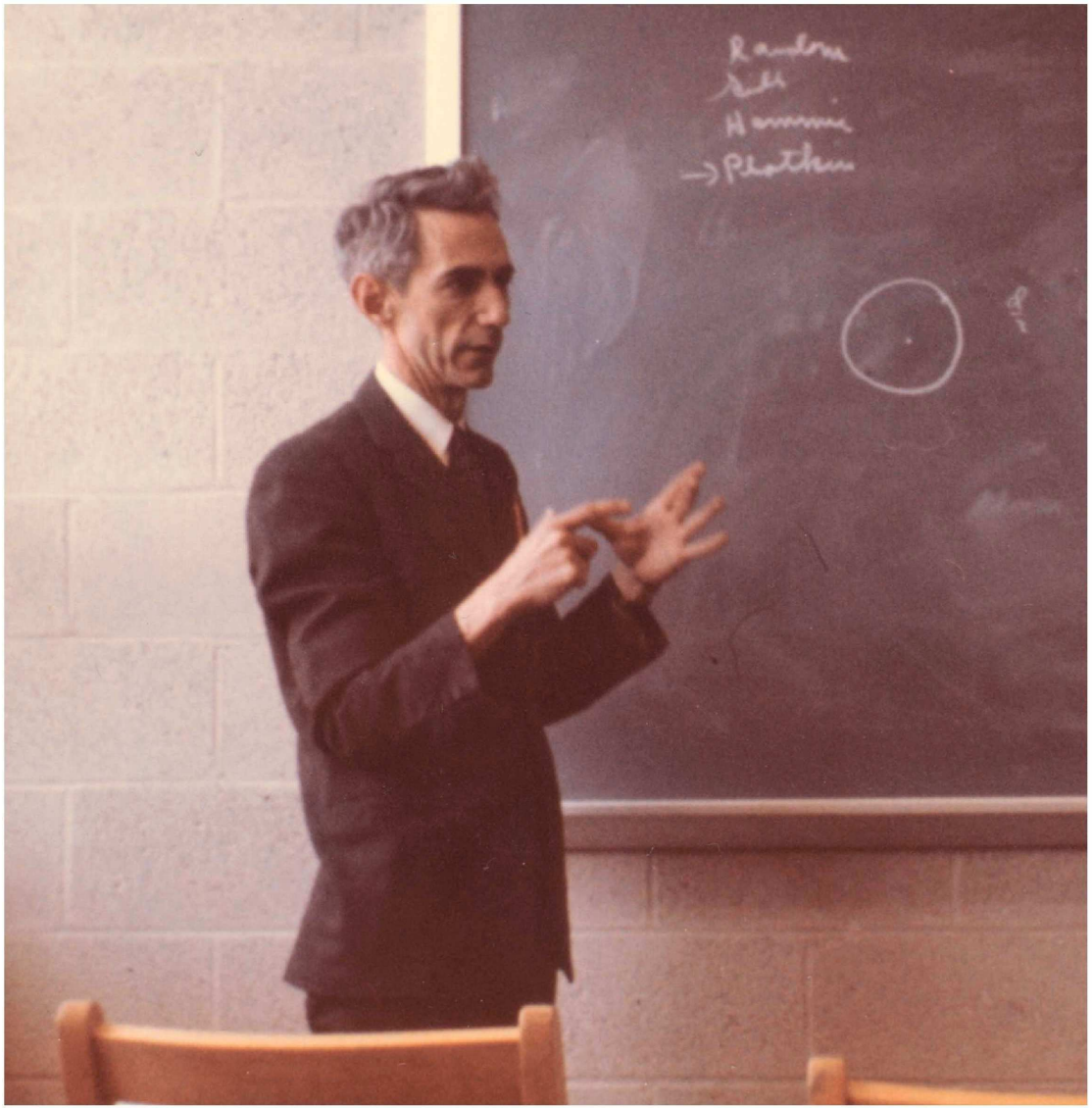


Fig. 1—Schematic of a general secrecy system.

(Shannon, 1949)



Claude Elwood Shannon (1916-2001)
(photographed 17 April 1961 by Göran Einarsson)

Shannon's

Fig. 1—Schematic of a general secrecy system

makes the following assumptions crystal clear:

- The **message M** and the **key K** are **independent** random variables.
- The **sender** and **receiver** both **know** the **key**.
- The **attacker knows only** the **cryptogram E** (i.e., a ciphertext-only attack is assumed).
- The **receiver** is able to **recover** the **message M** from knowledge of the cryptogram **E** and key **K**.
- No assumption is made about who generates the key.

You don't need a lot of words and/or equations to make yourself mathematically precise!

Kerckhoffs' Principle

A cipher should be **secure** when the enemy **cryptanalyst knows all details of the enciphering process and deciphering process except** for the value of the secret **key**.

This principle was first stated in 1881 by the Dutchman Auguste Kerckhoffs (1835 - 1903).

When evaluating security, one assumes that the enemy cryptanalyst knows everything (including the source statistics and key statistics) except the secret key.

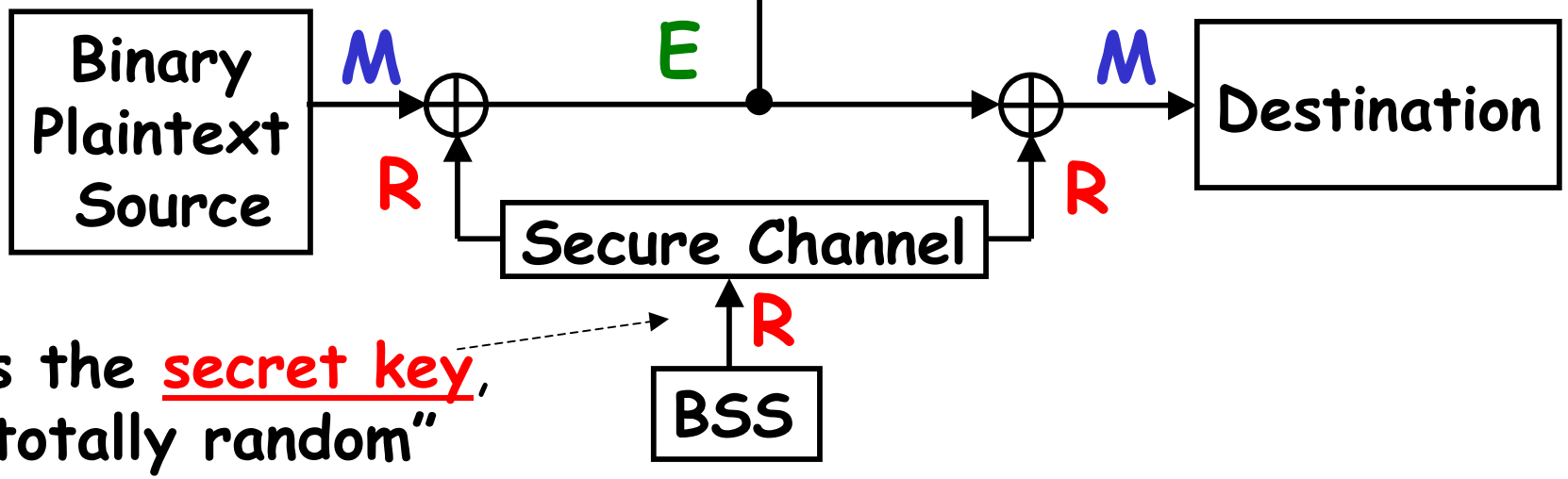
What does "unbreakable" mean?

To Shannon, a cipher is unbreakable in a ciphertext-only attack if it provides unconditional security, i.e., no matter how hard or how long the attacker works, he/she can do no better than to guess the plaintext by the best guessing rule that he/she would use without having seen the ciphertext.

Shannon 's 1949 definition: A cipher provides **perfect secrecy against a ciphertext-only attack** if the plaintext and the ciphertext, considered as random variables, are independent.

Vernam's 1926 Cipher:

Enemy cryptanalyst in a ciphertext-only attack.



R is the secret key, a "totally random" sequence.

Binary Symmetric Source

Vernam claimed that his cipher was unbreakable!

Vernam not only claimed that his cipher was **unbreakable**, but also stated that he had **confirmed** this in **"field trials with the U. S. Army Signal Corps"**.

Was Vernam right? Was his cipher the first unbreakable cipher in the many thousands of years of cryptographic history?

The **Binary Symmetric Source** (**BSS**) of information theory is a **monkey with a fair binary coin** (0 on one side and 1 on the other).

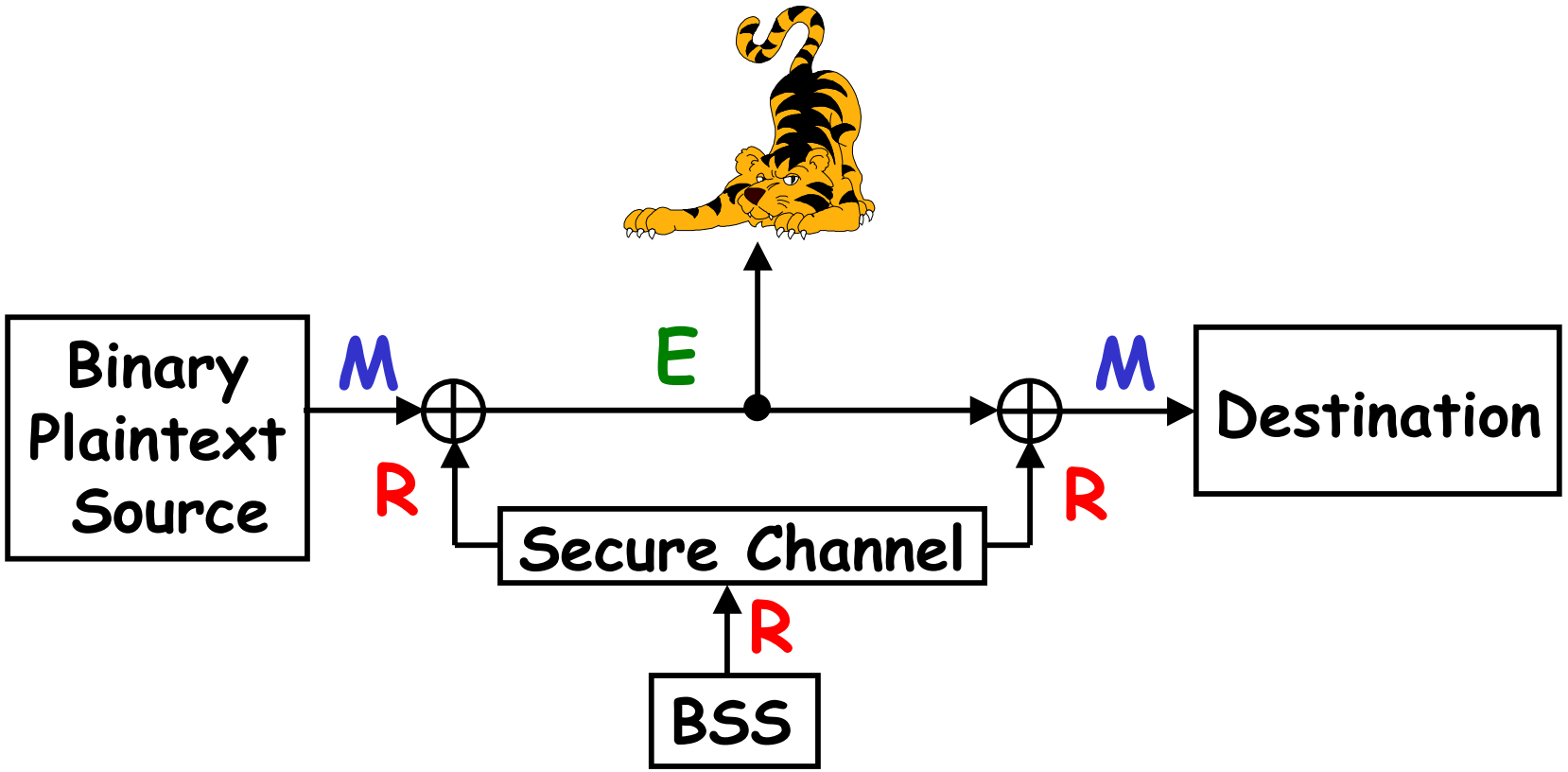
Cryptographic property of the BSS:

The modulo-two sum of a BSS output and an arbitrary random sequence is another BSS output that is INDEPENDENT of the arbitrary random sequence.

Example:

BSS output:	0	1	0	0	1	0	1	0	1	1	1	0	1 . . .
Arb. Ran. Seq.	1	1	1	1	1	1	1	1	1	1	1	1	1 . . .
Modulo-2 sum	1	0	1	1	0	1	0	1	0	0	0	1	0 . . .

Vernam's cipher provides perfect secrecy against a ciphertext-only attack!



The **cryptogram E** that the enemy cryptanalyst sees is **independent** of the **plaintext message M.** This simple **proof of unbreakability** of Vernam's 1926 cipher was first given by Shannon in **1949**!

Vernam's cipher is usually today called the "**one-time pad**" to emphasize that the key is to be used for only one message . It was used by spies on both sides in World War II and is still the cipher of choice for extremely important secret communications.

(What Shannon called the **plaintext** is the **total data** that will be encrypted before the key is changed, i.e., Shannon specified a "**one-time key**" in his theory of secrecy systems.)

Vernam's cipher needs **as many binary digits of secret key as there are bits of plaintext** to be encrypted.

Vernam was right about his cipher being unbreakable, **but does an unbreakable cipher really need this huge amount of secret key???**

Shannon's 1949 Lower Bound on Key Length:

For perfect secrecy, the number of different keys must be AT LEAST AS GREAT as the number of different plaintexts.

Proof:

- For any fixed key **k**, the number of different ciphertexts **e** equals the number of different plaintexts **m**.
- **Perfect secrecy** $\Rightarrow$ for all possible **e** and any fixed **m**,

$$P(E=e|M=m) = P(E=e) \neq 0$$

- $\Rightarrow$ For a fixed **m**, the number of different ciphertexts **e** must equal at least the number of different plaintexts **m**.
- But all **keys** from a **fixed m** to **different e**'s **must be different**.

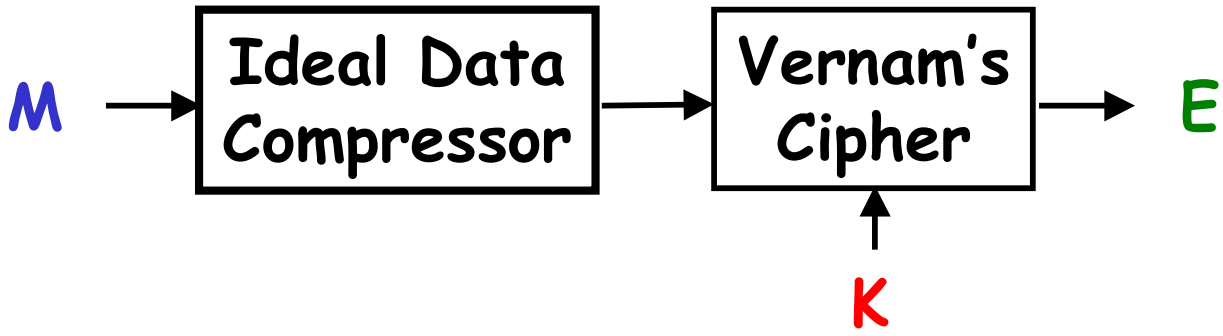
Shannon later gave the following proof of a slightly weaker lower bound on key length, namely

$$\boxed{H(\mathbf{K}) \geq H(\mathbf{E}).}$$

$$\begin{aligned}
\text{Perfect secrecy} \Rightarrow H(\mathbf{E}) &= H(\mathbf{M}|\mathbf{E}) \\
&\leq H(\mathbf{M}\mathbf{K}|\mathbf{E}) \\
&= H(\mathbf{K}|\mathbf{E}) + \underbrace{H(\mathbf{M}|\mathbf{E}\mathbf{K})}_{=0} \\
&= H(\mathbf{K}|\mathbf{E}) \\
&\leq H(\mathbf{K})
\end{aligned}$$

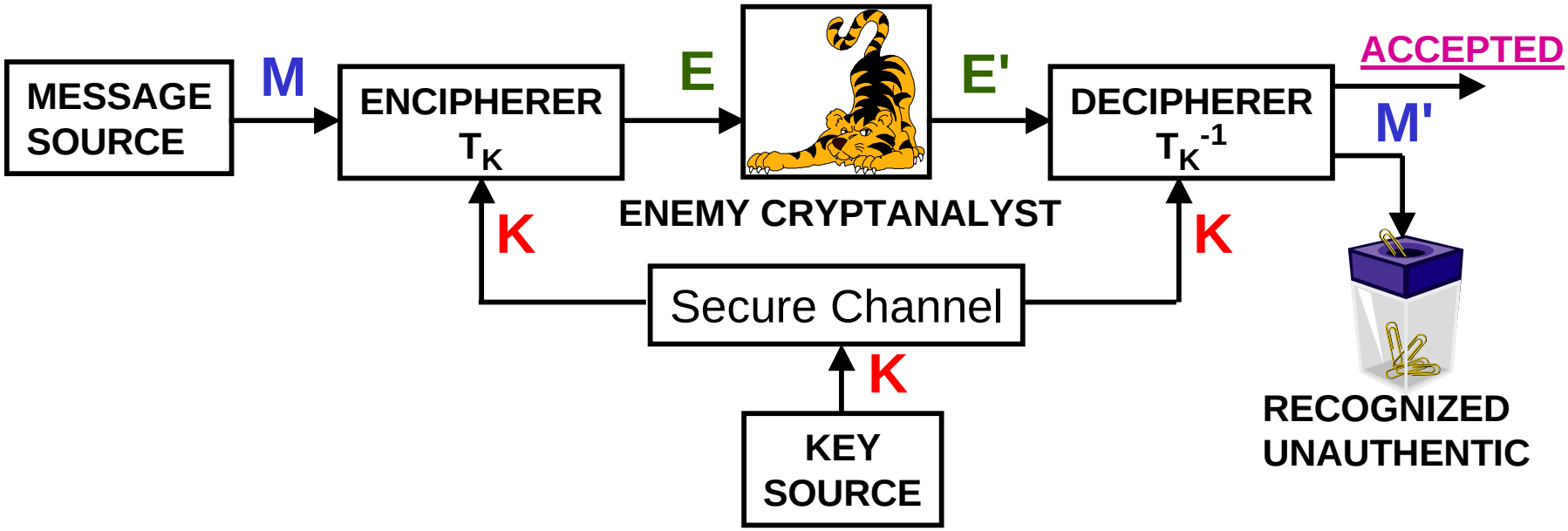
Thus, if the cipher is to give perfect secrecy regardless of the source statistics, it must also give perfect secrecy for the BSS for which $H(\mathbf{M}) = N$ bits. Thus $H(\mathbf{K}) \geq N$ so that the key must be at least N binary digits long.

The number of different plaintext messages is about $2^{H(M)}$ where **H(M)** is the **entropy** of the **plaintext** message. Equivalently, one says that **H(M)** is the number of bits of information in the plaintext message. An ideal data compressor will compress **M** to about **H(M)** binary digits. Consider the system:



Achieves perfect secrecy and the number of binary digits of the key **K** is **H(M)**, which **satisfies Shannon's lower bound with equality**.

Simmons' Model of a **Substitution Attack** on an Authenticity System



E' can be the legitimate cryptogram **E** or a phony cryptogram **E'** (**E'** ≠ **E**) inserted by the attacker.

E' is **accepted** if and only if it is a valid cryptogram for the key **K**.

In an **impersonation attack**, the attacker forms **E'** without seeing a legitimate cryptogram **E** and wins if his cryptogram is accepted.

P_I = Probability of **successful impersonation** when the attacker uses an optimum attack.

P_S = Probability of **successful substitution** when the attacker uses an optimum attack.

P_d = Probability of **deception** = $\max(P_I, P_S)$

Simmons' 1984 bound on the probability of deception:

$$P_d \geq 2^{-I(E;\,K)}$$

where $I(E;\,K) = H(K) - H(K|E)$ is the **mutual information** between **E** and **K**.

The only way to get unconditionally secure authenticity is to let the cryptogram give information about the key!

Example of an authenticity system meeting Simmon's lower bound on P_I with equality:

Plaintext is sent in the clear and the key is added as a signature: $E = [M : K]$

If the key has length **n** binary digits, then

$$P_I = 2^{-n}$$

because the attacker can only make a random guess at the secret key in an impersonation attack. **I(E; K) = n** bits so that **Simmons' bound on P_I holds with equality!**

This authenticity system gives no secrecy!

In a **substitution attack**, the attacker can achieve

$$P_S = 1.$$

Example of an authenticity system meeting Simmon's lower bound on P_s and P_d with equality:

1-bit messages with individual signatures.

K = $(K_1, K_2, \ldots K_\nu, K_{\nu+1}, \ldots K_{2\nu})$ [n = 2ν-bit key] assumed generated by a BSS.

M is 0 or 1.

M = 0 $\Rightarrow$ **E** = $(0, K_1, K_2, \ldots K_\nu)$

M = 1 $\Rightarrow$ **E** = $(1, K_{\nu+1}, K_{\nu+2}, \ldots K_{2\nu})$

Note that again there is **no secrecy!**

Whether the attacker observes **E** or not, he must guess ν bits of key to produce a cryptogram **E'** that will be accepted as authentic.

$\Rightarrow$ $P_I = P_S = P_d = 2^{-\nu}$.

But **I(E; K)** = ν bits so that **Simmons' bound on P_d holds with equality!**

This example shows that we can have unconditionally secure authenticity with no secrecy.

Vernam's cipher gives perfect secrecy against a ciphertext-only attack but no protection against an impersonation attack, i.e., $P_I = 1$.

The important conclusion to make is that **secrecy and authenticity are independent attributes** of a cryptographic system.

The **informational divergence** (or the "**Kullbach-Leibler distance**" or the "**relative entropy**" or the "**discrimination**") from **P** to **Q**, two probability distributions on the same alphabet, is the quantity

$$D(P \| Q) = -\sum_{x \in \mathrm{supp}(P)} P(x) \log \frac{Q(x)}{P(x)}.$$

Fundamental property of informational divergence:

$$D(P \| Q) \geq 0 \text{ with equality if and only if } P = Q.$$

Let H_0 and H_1 be the two possible **hypotheses** and let Y be the **observation** used to determine which hypothesis is true. Let D_0 and D_1 be the regions of Y values in which one decides for H_0 or H_1, respectively. Let α or β be the **error probabilities** when H_0 or H_1 is true, respectively.

Let V (0 or 1) be the **decision** as to which hypothesis is true so that

$$\alpha = P_{V|H_0}(1) \quad \text{and} \quad \beta = P_{V|H_1}(0).$$

Direct calculation gives

$$D(P_{V|H_0} \,\|\, P_{V|H_1}) = -\alpha \log \frac{1-\beta}{\alpha} - (1-\alpha) \log \frac{\beta}{1-\alpha}.$$

Information-theoretic bound for hypothesis testing:

$$D(P_{Y|H_0} \,\|\, P_{Y|H_1}) \geq -\alpha \log \frac{1-\beta}{\alpha} - (1-\alpha) \log \frac{\beta}{1-\alpha}$$

with equality if and only if $\dfrac{P_{Y|H_0}(y)}{P_{Y|H_1}(y)}$ has the same value for all $y \in D_0$ and has the same value for all $y \in D_1$.

For the important special case where $\alpha = 0$, i.e., where **we never err when H_0 is true**, the previous bound gives

$$\beta \geq 2^{-D(P_{Y|H_0} \| P_{Y|H_1})} .$$

Now suppose that H_0 is the **hypothesis that the observation $Y = E'$ is the legitimate cryptogram E** for the key $K = k$, i.e.,

$P_{Y|H_0}(y) = P_{E|K=k}(y)$, and that H_1 is the **hypothesis that $Y = E'$ is formed by the attacker** according to

$$P_{Y|H_1}(y) = P_E(y) = \sum_k P_{K=k}(k) P_{E|K=k}(y),$$

which **may not** be the optimum attacking strategy.
Let β_k be the **error probability when $K = k$** so that

$$\beta_k \geq 2^{-D(P_{E|K=k} \| P_E)} .$$

$$D(P_{E|K=k} \parallel P_E) = -\sum_y P_{E|K=k}(y) \log \frac{P_E(y)}{P_{E|K=k}(y)}$$

$$\beta = \sum_k P_K(k)\beta_k \geq \sum_k P_K(k) 2^{-\sum_k D(P_{E|K=k} \| P_E)}$$

$$\geq 2^{-\sum_k P_K(k) D(P_{E|K=k} \| P_E)}$$

where we have used **Jensen's inequality**. But

$$\sum_k P_K(k) D(P_{E|K=k} \parallel P_E) = H(E) - H(E \mid K) = I(E;K).$$

Moreover, β **is just the probability** P_I **of successful impersonation**, so the information-theoretic bound becomes

$$P_I \geq 2^{-I(K;E)}.$$

This completes the proof of Simmons' lower bound.

Simmons' proof of his bound on the probability of deception (or impersonation) appears in

G. J. Simmons, "Authentication Theory/Coding Theory," pp. 411-431 in *Advances in Cryptology - CRYPTO '84* (Eds. G. R. Blakey and D. Chaum), Lecture Notes in Computer Science No. 196. Heidelberg and New York: Springer, 1985.

Several simplifications of his derivation have since been given. The most insightful one, which we have followed, is by **Maurer**, cf.

U. M. Maurer, "Information Theoretic Bounds in Authentication Theory," p.12 in *Proc. IEEE Inst. Symp. Info. Th.*, Whistler, Canada, Sept. 17-22, 1995.

U.M. Maurer, "A Unified and Generalized Treatment of Authentication Theory, pp. 387-398 in *Proc. 13th Symp. on Theoretical Aspects of Computer Science (STACS'96)*, Lecture Notes in Computer Science No. 1046, New York: Springer, 1996.

Maurer based his treatment on **Blahut's** information-theoretic approach to hypothesis testing, cf.

R. E. Blahut, "Hypothesis testing and information theory", *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 405-417, July 1974