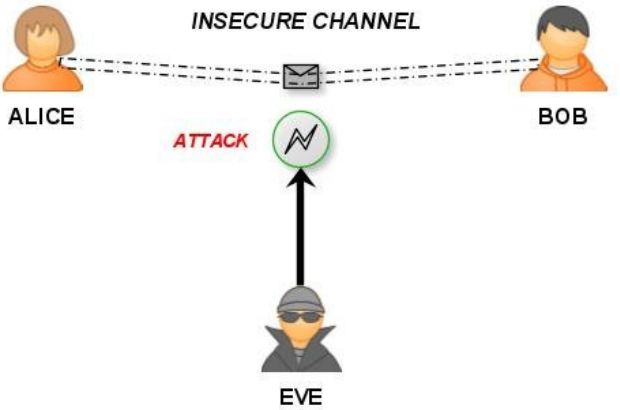
Classical cryptography
Quantum cryptography

Ivan Murashko

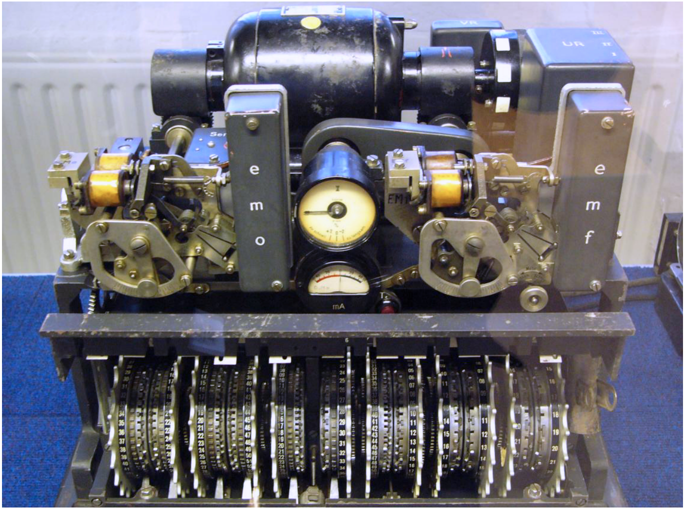
Introduction

- Classic cryptography
  - Caesar cipher
  - Vernam cipher (one-time pad)
  - Key distribution (Diffie-Hellman)
- Quantum cryptography
  - Einstein–Podolsky–Rosen paradox
  - No-cloning theorem
  - Quantum key distribution algorithm

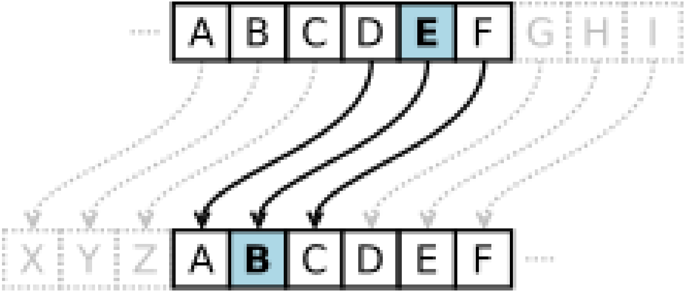
Cryptography



Lorenz cipher, WWII



Caesar cipher



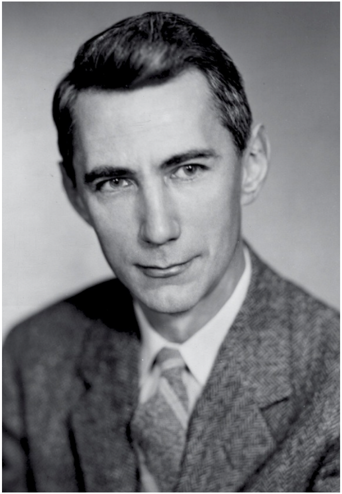
Hack the caesar cipher

E	11.1607%	56.88	M	3.0129%	15.36
A	8.4966%	43.31	H	3.0034%	15.31
R	7.5809%	38.64	G	2.4705%	12.59
I	7.5448%	38.45	B	2.0720%	10.56
O	7.1635%	36.51	F	1.8121%	9.24
T	6.9509%	35.43	Y	1.7779%	9.06
N	6.6544%	33.92	W	1.2899%	6.57
S	5.7351%	29.23	K	1.1016%	5.61
L	5.4893%	27.98	V	1.0074%	5.13
C	4.5388%	23.13	X	0.2902%	1.48
U	3.6308%	18.51	Z	0.2722%	1.39

Perfect security

Is there a cipher that is unbreakable?

Shannon 1949



Communication Theory of Secrecy Systems*

By C. E. SHANNON

1. Introduction and Summary

THE problems of cryptography and secrecy systems furnish an interesting application of communication theory.[1] In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography.[2] There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.

The treatment is limited in certain ways. First, there are three general types of secrecy system: (1) concealment systems, including such methods as invisible ink, concealing a message in an innocent text, or in a fake covering cryptogram, or other methods in which the existence of the message is concealed from the enemy; (2) privacy systems, for example speech inversion, in which special equipment is required to recover the message; (3) "true" secrecy systems where the meaning of the message is concealed by cipher, code, etc., although its existence is not hidden, and the enemy is assumed to have any special equipment necessary to intercept and record the transmitted signal. We consider only the third type—concealment systems are primarily a psychological problem, and privacy systems a technological one.

Secondly, the treatment is limited to the case of discrete information, where the message to be enciphered consists of a sequence of discrete symbols, each chosen from a finite set. These symbols may be letters in a language, words of a language, amplitude levels of a "quantized" speech or video signal, etc., but the main emphasis and thinking has been concerned with the case of letters.

The paper is divided into three parts. The main results will now be briefly summarized. The first part deals with the basic mathematical structure of secrecy systems. As in communication theory a language is considered to

* The material in this paper appeared originally in a confidential report "A Mathematical Theory of Cryptography" dated Sept. 1, 1945, which has now been declassified.

[1] Shannon, C. E., "A Mathematical Theory of Communication," *Bell System Technical Journal*, July 1948, p. 379; Oct. 1948, p. 623.

[2] See, for example, H. F. Gaines, "Elementary Cryptanalysis," or M. Givierge, "Cours de Cryptographie."

656

Vernam cipher, one-time pad, 1917

t	k	$c = t \oplus k$
0	0	0
0	1	1
1	0	1
1	1	0

Table: XOR $t \oplus k$

Thus you you have a text (t) and key (k) then you can get an encoded text as follows

$$c = t \oplus k$$

original text can be restored as

$$t = c \oplus k$$

Key distribution. Discrete log

$$x = ind_g(a) \mod p$$

min x such that

$$g^x \equiv a \mod p$$

Key distribution. Diffie-Hellman (1)

Known data: g, p
Alice choose random a and calculates

$$A \equiv g^a \mod p$$

Bob choose random b and calculates

$$B \equiv g^b \mod p$$

Alice and Bob exchange the A and B and calculate K as

$$K \equiv B^a \mod p$$

or

$$K \equiv A^b \mod p$$

Key distribution. Diffie-Hellman (2)

Alice and Bob exchange the A and B and calculate K as

$$K \equiv B^a \mod p$$

or

$$K \equiv A^b \mod p$$

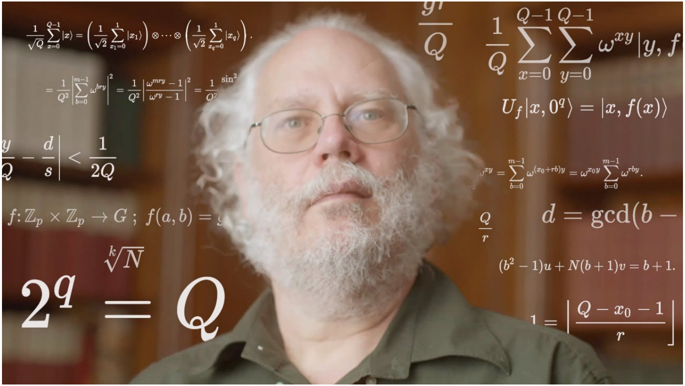
because

$$K \equiv g^{ab} \mod p$$

Discrete logarithm complexity

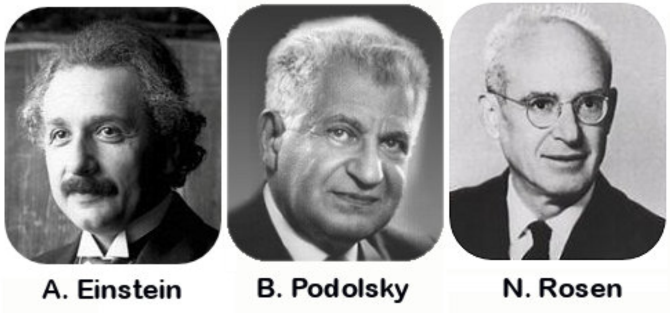
$$\mathbf{P} \neq \mathbf{NP}$$

Shor algorithm



Quantum cryptography

Einstein–Podolsky–Rosen paradox

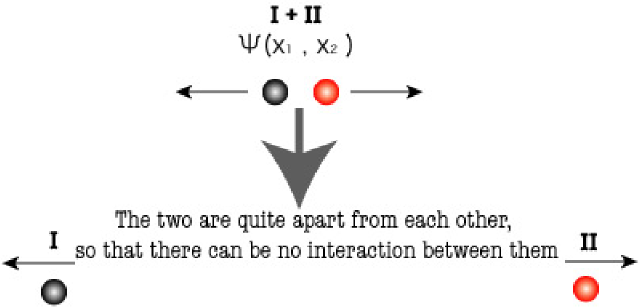


Heisenberg inequality

$$\Delta p \Delta q \geq \frac{\hbar}{2}$$

Einstein–Podolsky–Rosen paradox (1)

EINSTEIN-PODOLSKY-ROSEN PARADOX, (1)



Suppose you measure the momentum of the black particle (I); then you can know the momentum of the red particle (II) as well. Likewise, if you measure the position of the black, then you can know the position of the red as well. In both cases, the measurement can be done **without disturbing** the red (since there can be **no interaction** between the black and the red).

Einstein–Podolsky–Rosen paradox (2)

EINSTEIN-PODOLSKY-ROSEN PARADOX, (2)

If you measure the momentum **p**, then the momentum of the red is **-p**. Since the momentum of the red was measured without disturbing it, that quantity must be regarded as **real**.

If you measure the position q_1, then the position of the red is q_2. Since the position of the red was measured without disturbing it, that quantity must be regarded as **real**.

Einstein–Podolsky–Rosen paradox (3)

- Heisenberg inequality is invalid
- Special theory of relativity is invalid

Bell experiment. Classical case

$$f = \frac{1}{2}\left(ab + a'b + ab' - a'b'\right), a, a', b, b' \in \{-1, +1\}.$$

therefore $f \in \{-1, +1\}$ and $|\langle f \rangle| \leq 1$

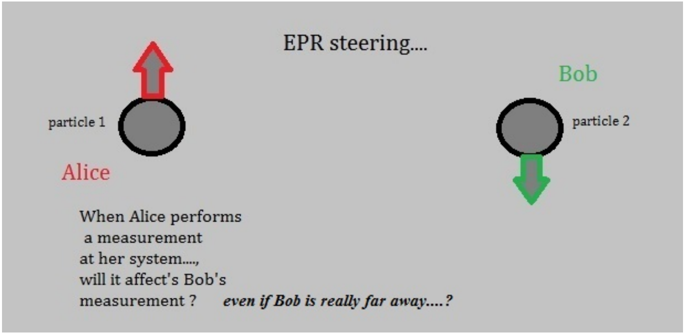
Bell experiment. Quantum case

$$|\langle f \rangle| = \sqrt{2} > 1$$

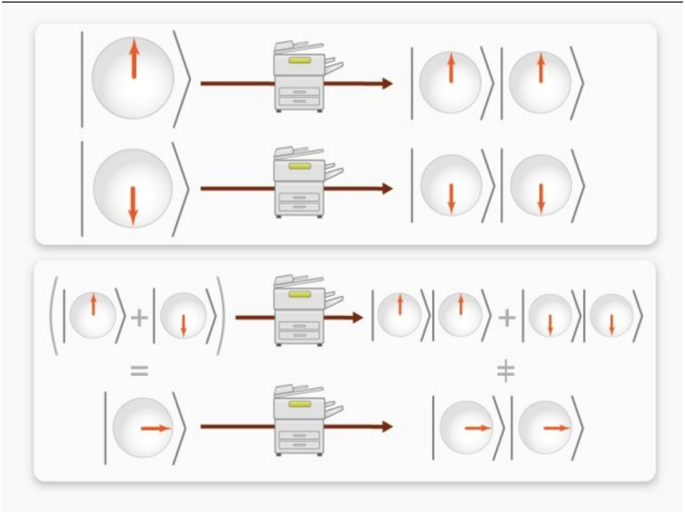
Quantum cryptography. Base principles

1. Measurement is random
2. Alice and Bob measurements are correlated
3. No-cloning theorem

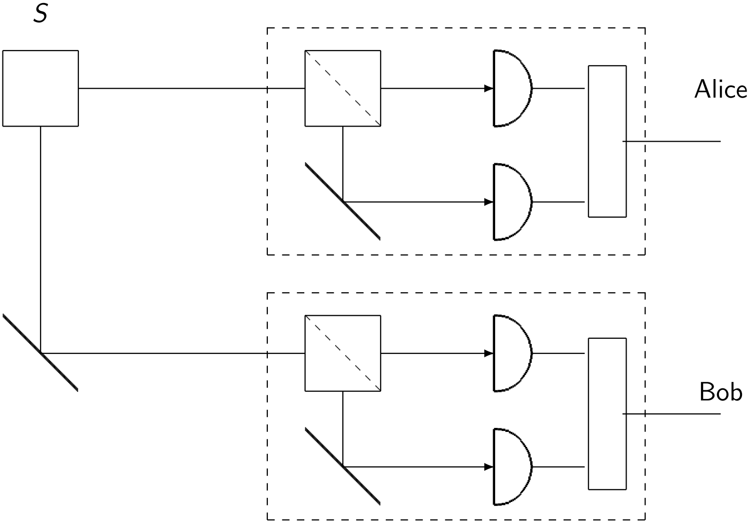
Measurement is random but correlated



No-cloning theorem



Quantum cryptography. Key distribution



Questions


SHRODINGER VS. HEISENBERG
CAT-DEAD OR ALIVE?
WHAT DO YOU THINK?
I DON'T KNOW
cloudcomics.blogspot.com
Cloud Comics © 2012