

# Класическа криптография

- Неразбиваеми шифри: шифър на Vernam
- Che Guevara и Fidel Castro
- Доказателство на Shannon
- Проект VENONA
- Quantum Key Distribution

# Шифър на Vernam (1917)

“most important in the history of cryptography”

Gilbert Vernam [AT&T] (XOR патент USA)

**Съобщение:** последователност от 0 и 1

$M = 011001100111001010001000100010$

**Ключ:** **случайна** последователност от 0 и 1

$K = 101101100101001010010101001011$

**Кодирано съобщение:**  $C_i = M_i \oplus K_i \text{ mod } 2$

$C = 110100000010000000011101101001$

**Декодирано съобщение:**  $D_i = C_i \oplus K_i \text{ mod } 2$

$D = 011001100111001010001000100010$

# Che Guevara to Fidel Castro

A 6	E 8	I 39	M 70	Q 71	U 52	Y 1
B 38	F 30	J 31	N 76	R 58	V 50	Z 59
C 32	G 36	K 78	O 9	S 2	W 56	
D 4	H 34	L 72	P 79	T 0	X 54	

- Подредени в 5-цифрени блокчета  
Съобщение: горният ред в групата от 3 реда
- Ключ: средният ред в групата
- Шифрограма: съобщението и ключа са събрани (без 1 наум) за да получим долната линия
- Декодиране: шифрограмата „-“ ключа

0 2 3 8 6	5 8 7 6 7	0 8 7 6 2	6 3 1 2 3	7 6 4 8 7	0 6 2 6 7	6 9 0 6 8
6 1 8 6 4	6 8 6 3 2	4 6 0 5 1	8 7 9 3 1	7 8 2 9 2	0 3 0 2 3	4 6 9 9 3
6 9 1 4 0	1 0 3 9 9	4 4 7 1 3	4 0 0 1 4	4 4 6 7 9	0 9 2 8 0	0 5 9 5 5
2 3 7 9 7	6 8 2 7 9	6 5 8 6 7	0 8 7 0 9	5 8 3 9 5	7 6 5 8 8	7 2 3 9 7
6 2 7 7 3	4 1 1 6 9	4 2 3 5 7	4 7 4 5 5	6 2 1 3 3	7 1 3 9 0	4 5 5 3 4
8 5 6 8 0	0 9 3 3 8	0 7 1 1 4	4 5 1 5 4	1 0 4 2 8	6 7 7 7 8	1 7 8 2 3
6 3 0 9 5	8 7 0 8 9	5 8 6 7 2	7 1 5 2 8	7 2 8 4 3	9 3 7 0 9	4 9 8 7 6
4 8 7 9 4	0 7 8 8 1	4 9 3 2 8	8 0 0 9 8	6 2 9 8 3	4 8 6 9 6	8 7 7 1 6
0 1 9 8 9	8 4 8 6 9	9 6 9 9 7	5 1 5 1 6	3 4 7 2 2	7 1 3 9 5	2 8 7 8 8
3 2 7 2 6	5 0 8 3 3	8 2 0 8 8	2 8 7 2 7	6 8 6 2 6	3 1 8 3 3	7 3 1 1 1
8 4 5 5 0	1 8 4 7 1	7 8 2 1 3	7 6 6 9 4	5 8 8 3 0	4 2 5 4 0	6 2 6 3 0
1 6 2 7 6	6 9 2 0 4	5 0 2 9 1	9 4 3 1 1	5 6 4 5 6	7 3 3 7 3	3 5 7 4 1
7 7 7 2 7	2 8 3 6 6	5 8 9 7 6	4 6 7 6 0	9 7 6 1 3	0 5 8 6 7	6 3 2 3 7
1 2 7 6 4	3 5 6 0 1	9 4 5 0 8	5 2 0 6 0	5 7 8 7 1	5 2 5 0 4	7 8 6 9 3
8 9 7 7 1	5 3 9 6 7	4 2 4 7 4	9 2 7 2 0	4 4 4 8 4	5 7 3 6 1	3 1 8 7 2
2 1 7 7 3	7 8 2 0 8	7 6 9 2 6	3 8 3 9 6	3 2 6 7 6	0 3 9 4 6	4 1 4 8 3
6 7 6 1 8	0 0 6 2 1	0 7 4 0 8	7 5 5 9 3	6 7 2 3 0	6 7 8 0 8	8 1 7 7 2
8 0 0 0 1	7 8 8 2 9	7 3 3 2 4	0 3 8 8 1	9 9 8 0 6	6 0 7 4 4	2 8 1 7 5
1 5 4 3 9	7 6 8 5 8	9 8 7 6 7	2 6 7 9 6	5 9 3 7 7	9 3 9 8 7	6 2 9 4 6
2 2 8 9 2	3 0 5 6 2	3 8 0 9 1	4 8 1 6 9	4 8 4 2 3	4 6 5 2 5	1 3 1 7 1
3 1 2 2 1	<del>3 0 5 6 2</del>	2 6 7 5 8	6 1 8 9 5	9 7 7 9 0	3 9 7 0 2	3 5 0 2 7
	0 6 3 1 0					
5 8 7 2 8	7 3 3 3 3	0 0 0 7 7	1 5 8 8 2	8 5 8 5 0	6 5 8 7 2	8 8 7 2 8
0 6 3 8 9	2 5 0 6 7	3 2 2 4 7	8 8 0 1 1	1 2 9 8 3	3 2 3 2 1	2 2 7 0 1
5 4 0 8 2	9 8 3 3 2	3 2 2 1 4	9 2 3 9 3	6 7 9 3 3	9 7 1 5 3	0 0 5 2 3

14-025

# Неразбиваемост (случаен ключ)

(C. Shannon, 1949,  $\exists$  !)

## Теорема (версия ЛГ)

За всяко (прехванато) кодирано съобщение

$C = M \oplus K \in \mathbf{Z}_2^N$  и за всяко отнапред

зададено декодирано съобщение  $D' \in$

$\mathbf{Z}_2^N$  съществува ключ  $K' \in \mathbf{Z}_2^N$  такъв, че

$$C \oplus K' = D'.$$

## Доказателство:

$$K' = C \oplus D' \in \mathbf{Z}_2^N$$

**Допълнение:** единственост! (Shannon)

# Claude E. Shannon (1916 – 2001)



- Американски математик
- Електрически инженер
- Компютърен изследовател
- Криптограф
- Известен като „Бащата на информационната теория“

Сумата на едно съобщение със случайна величина е отново случайна величина, т.е. в сумата не се съдържа никаква информация

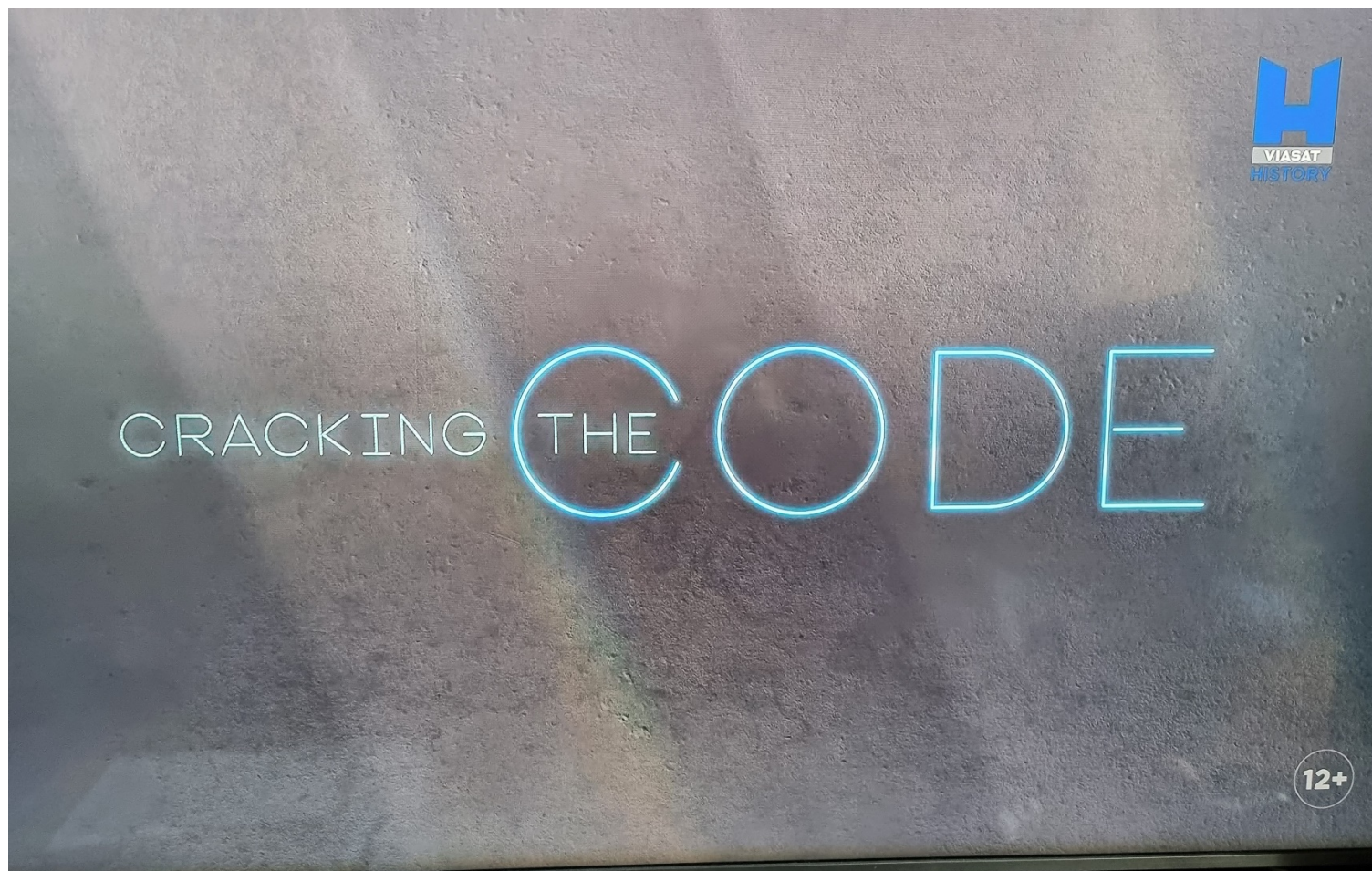
# Неразбиваем: условия

1. Ключът трябва да е поне толкова дълъг колкото съобщението;
2. Ключът трябва да е напълно случаен (равномерно разпределен в множеството на всички ключове и независим от съобщението -Truly random);
3. Ключът не трябва да бъде използван отново – нито изцяло нито частично;
4. Ключът трябва да бъде пазен тайно от комуникиращите страни.

# One-time pad шифри

## Изводи:

- Съобщението е толкова сигурно колкото сигурен е ключът (случаен)
- Ако има повторения в ключа от съобщението може да се извлече вярна информация



Материали взети от Wikipedia и Viasat History Channel

# Сталин и атомната бомба



# VENONA project (1943–1980)

Най-важният разузнавателен  
(криптографски) проект в историята на САЩ

Декриптиране на съобщения предадени от  
разузнавателните служби на СССР, като  
НКВД, КГБ и ГРУ в САЩ

- Неизвестен за Franklin Roosevelt and Harry Truman;
- 3000 съобщения преведени от руски на английски;

# VENONA: разсекретен 1995

**TELEGRAM**

**RECEIVED**  
BY: \_\_\_\_\_

CLASS OF SERVICE	SYMBOL
TELEGRAM	
DAY LETTER	BLUE
NIGHT MESSAGE	NITE
NIGHT LETTER	NL

CLASS OF SERVICE	SYMBOL
TELEGRAM	
DAY LETTER	BLUE
NIGHT MESSAGE	NITE
NIGHT LETTER	NL

Ref No: 6/SIF/I729

PUAUU UREEO ZTTTU ETPEP TRART RRAZW PTRAR TWZUE  
RIWAT EPETR TPEWA IORRR APOUO PURTE RTZEA TRUTT  
RTWZT

**TOP SECRET**  
**VENONA**

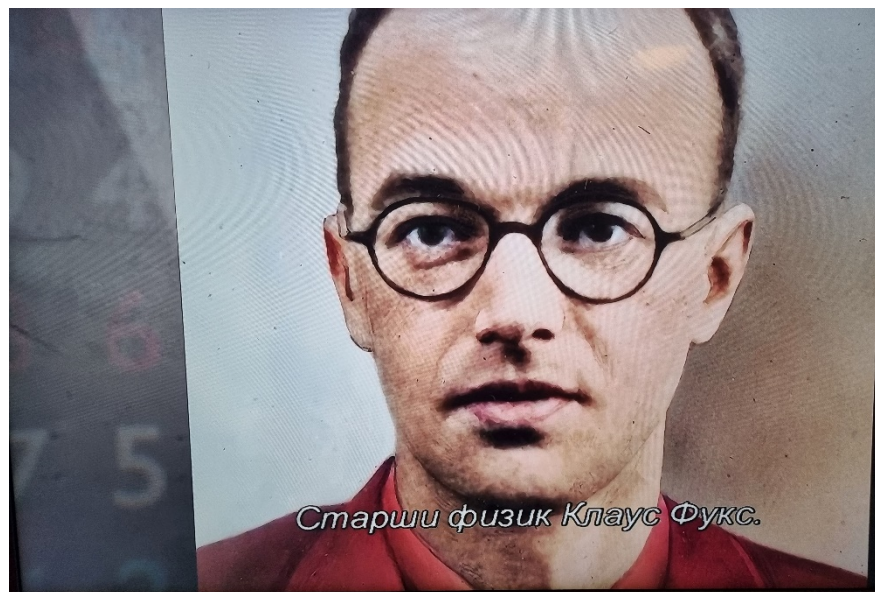
7 2 3 7 1 0

# VENONA: впечатляващ пробив

- Първи пробив: Берлин 1945: СССР Code Book
- Meredith Gardner: възстановява работещо копие
- Буквите са числа, уникален номер, Морзов код, IBM с перфокарти, първото число показва номера на OTP (сорт.-повторенията показват дублиране)
- Разкрити са кодовите имена на 200 агенти на СССР (35 000 one-time pads използвани от СССР повече от 1 път); Julius & Ethel Rosenberg
- Човешка грешка, атака с груба сила; през 1945 СССР прекратява дублирането: VENONA на тъмно

# Klaus Fuchs: течът от „Manhattan“

- VENONA: CHARLES and REST



Сталин получава съобщения по проекта Манхатън от 1942

Към 1945 СССР разполага с всичката информация да създаде собствена атомна бомба

Признава и лежи в затвор 9 години

VENONA: Течът на информация по Проекта Манхатън е спрял. Това не позволява на СССР да Построи водородна бомба Преди САЩ

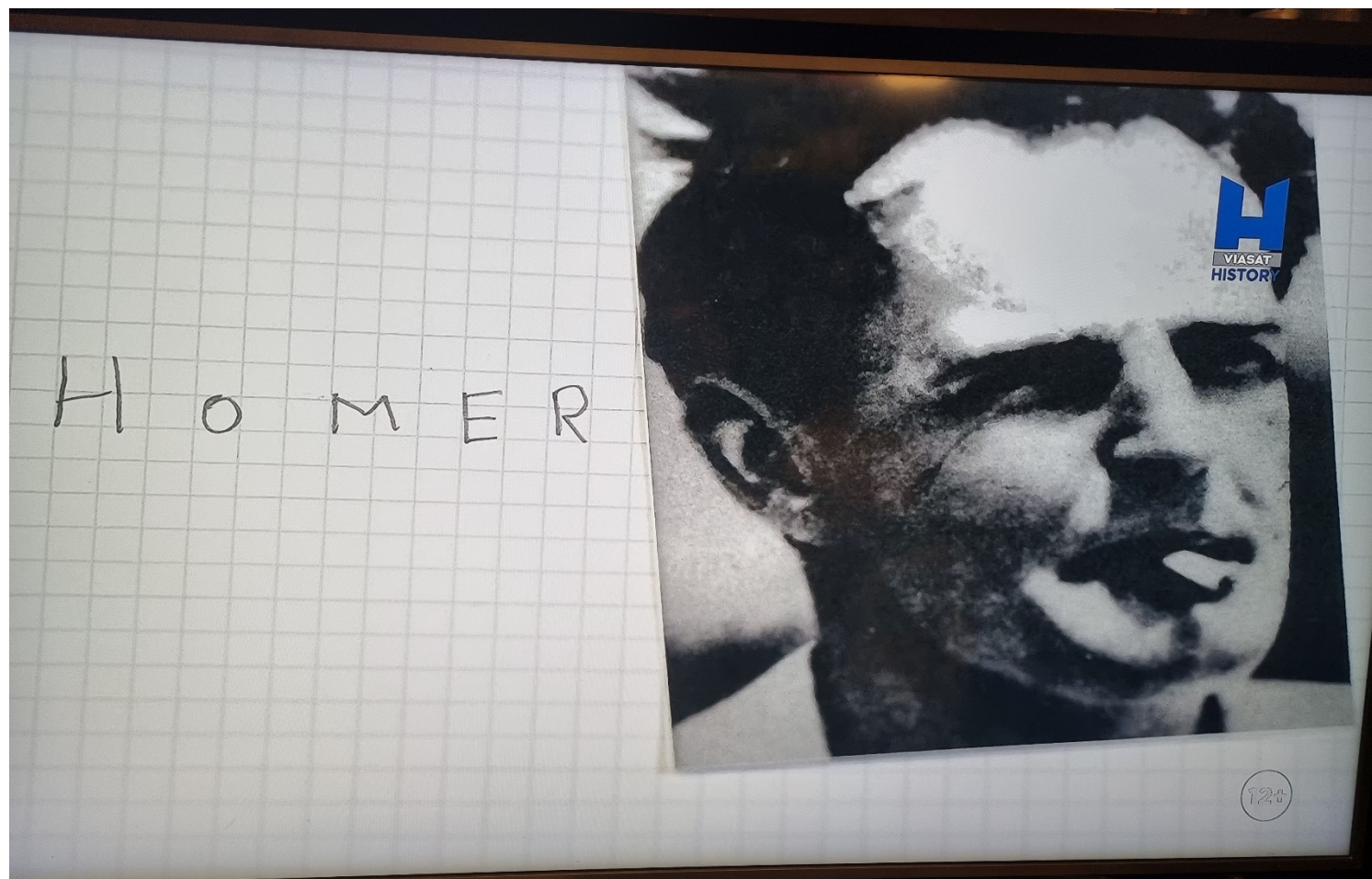
# Cambridge Five: най-опасният шпионски пръстен в САЩ

- Британска група за шпионаж в САЩ върху проекта Manhattan
- През 1944 г. Чърчил изпраща секретна телеграма директно до президента на САЩ
- През 1946 екипът на VENONA открива, че телеграмата е изпратена на Сталин от английско говорещ дипломат: Homer

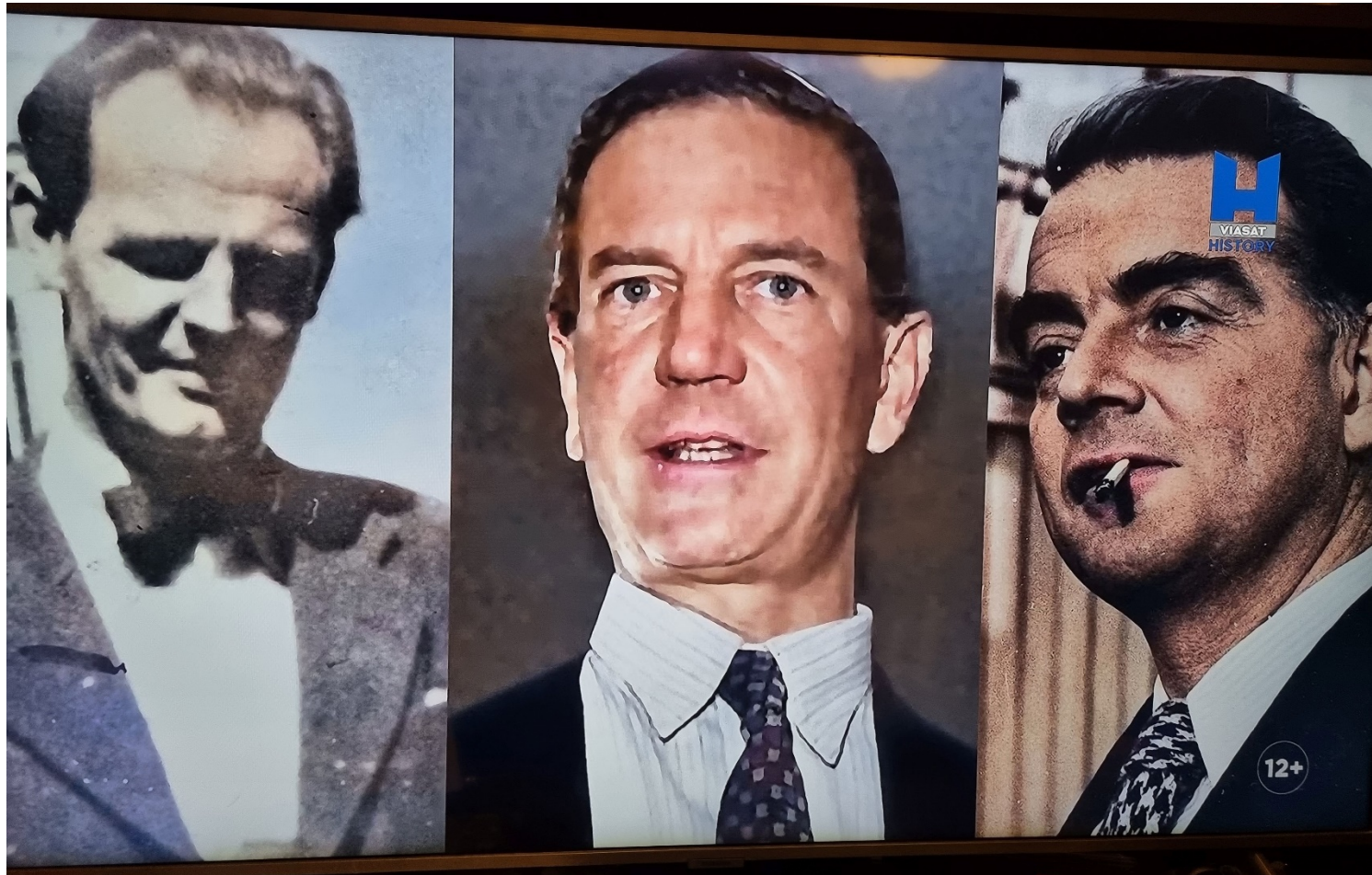
# VENONA: Homer

- British Foreign Office изпраща във Washington дипл. Kim Philby да помага за разследването
- VENONA разкрива, че Homer е Donald Maclean - 1 секретар в UK посолството във Washington
- За периода 1944-1945 е предал на Сталин 12 top-secret съобщения свързани с H-bomb
- Philby предупреждава Maclean, че е разкрит и той бяга в Москва с още един агент от Cambridge; Philby е изгонен от BFO

# Разкрит: кодово име Номер



# Homer, Kim Philby and Guy Burgess



# Благодарният СССР

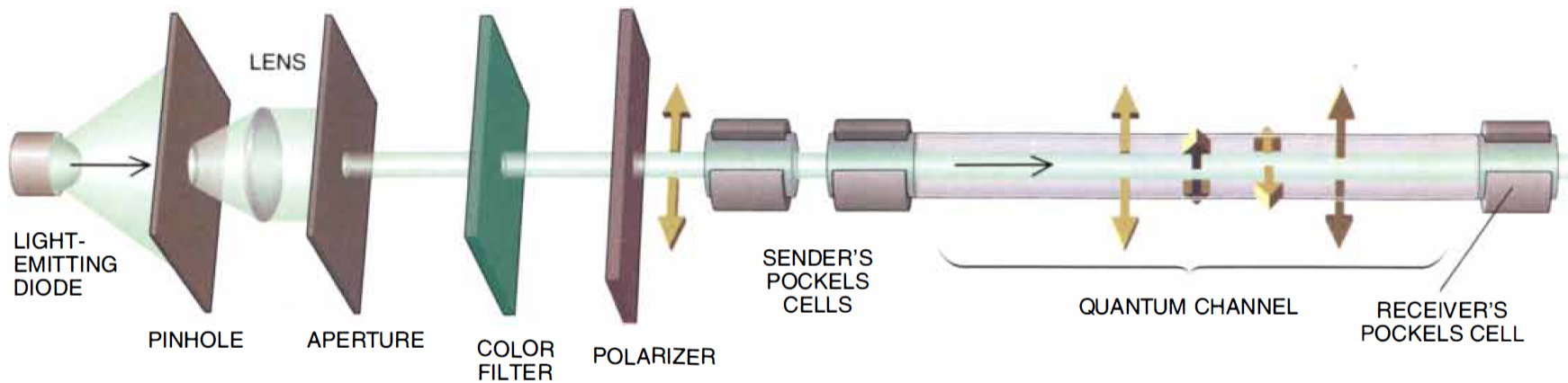


# Quantum Key Distribution (QKD)

- **Шифър на Vernam:** (неразбиваем) основа
- **Квантов генератор на случайни числа:**  
източник + beam-splitter + детектори
- **Протокол за споделяне на секретен ключ:**  
фотони по квантов канал (оптично влакно)
- **Квантови степени на свобода:**  
поляризация на фотоните
- **Забрана за копиране:** no-cloning theorem

# Квантово споделяне на ключ

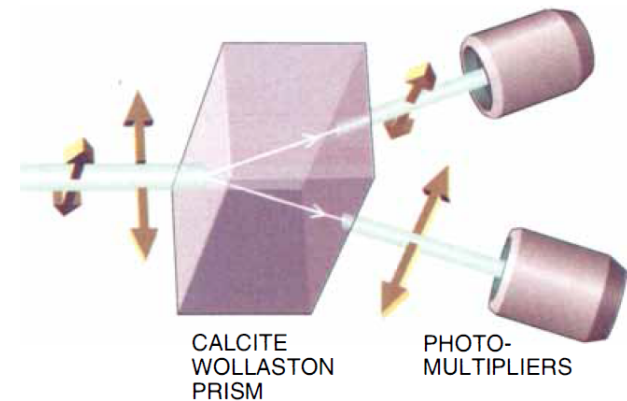
- **Случаен ключ:** споделен по квантов канал
- **Безусловна принципна сигурност:** основана на законите на квантовата физика (**no-cloning theorem**), а не на недоказани предположения за **computational complexity**
- **Заплаха за сигурността:** само в техническото изпълнение (контрамерки)



**QUANTUM SYSTEM can distribute information in perfect secrecy. The transmitter produces faint flashes of green light from a light-emitting diode. The pinhole, lens and filter create a collimated beam of dim flashes. The light is then polarized horizontally. Two Pockels cells change the polarization to 0,**

**45, 90 or 135 degrees. The polarized light flashes are released from the transmitter and eventually reach the receiver. There another Pockels cell shifts the polarization by either 45 degrees or not at all. The action of this Pockels cell allows the receiver to choose between measuring rectilinear or diagonal**

1. LED produces faint flashes of green light.
2. Pinhole, lens, and filter turn dim flashes into a collimated beam.
3. Light beam is polarized horizontally.
4. Pockels cells randomly select an orientation of 45,90, 135 or 180 degrees.
5. Polarized light leaves the transmitter and enters the fiber optic.
6. The polarized photons enter the receiver where another pockels cell randomly chooses to measure rectilinear or diagonal polarization
7. The Prism directs the photons to respective photo-multipliers depending on their polarization



**polarization. In the rectilinear case, a horizontally polarized photon will be directed toward the right photomultiplier; a vertically polarized photon will be directed toward the left photomultiplier.**

# Заклучение

- Квантова криптография: решение на заплахите към класическите методи за криптиране
- Проблем с разпространението на ключове
- Очакваният провал на системите с public/private ключове
- Принцип на неопределеност на Heisenberg, mutually unbiased bases
- Einstein-Podolsky-Rosen двойки сплетени фотони
- Post-Quantum Cryptography