

# Cryptography

by

Dmitry Kremenskov



First grade

# Graduation



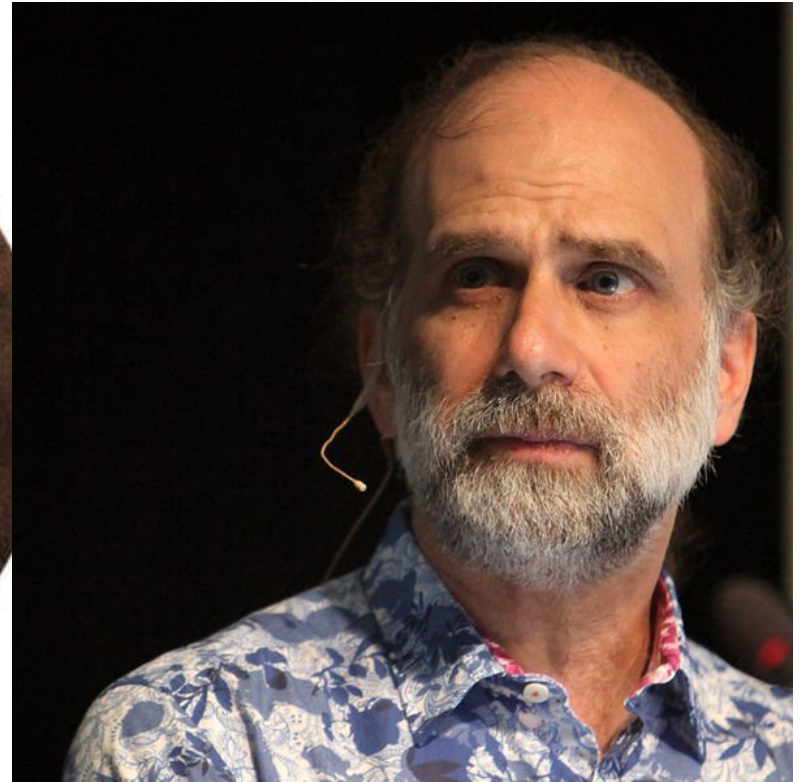


007



Maybe not 007...





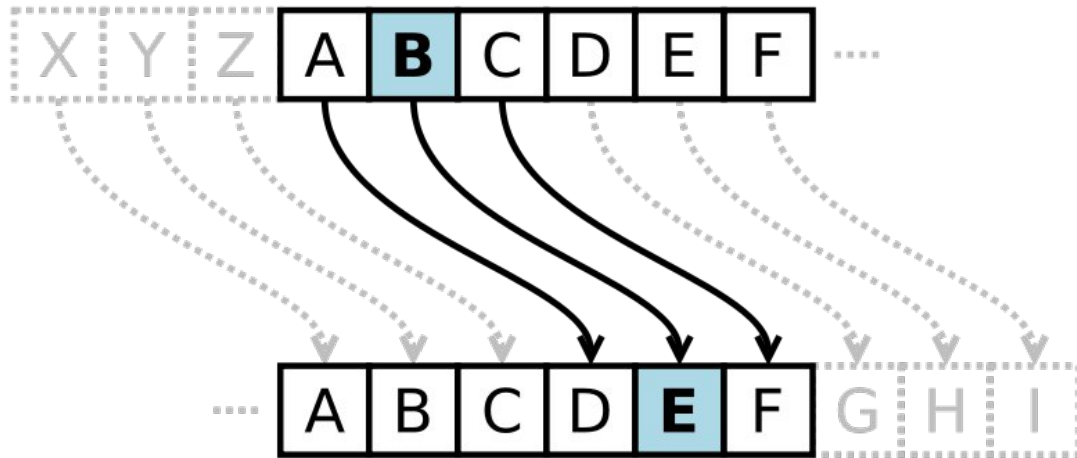
Familiar faces?





**Cryptography** is the practice and study of techniques for secure communication in the presence of third parties

# Ceasar's cipher







Spartans

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y



Vigenere



# One-time pad





# With codes

## One Time Pad

27564 34498 86670 32451...  
99812 34610 16843 46662...  
etc,...

(lines of 'random' numbers)

*A pad of paper sheets, each with a different sequence of apparently randomly varying numbers.*

## Code Book

19456 A  
34139 Aardvark  
03458 Able  
34347 ...

96350 Apple  
67295 ...

12395 B  
07732 Babe  
67208 Baboon  
00530 ...

83521 Betray  
61311 ...

*Book listing letters of the alphabet and useful words with their codes.*

# And then to the interesting part

$$T_u = T \pmod{(T^2 - uT + 1)}$$

$$B(n) = \#\{u : 0 \leq u < n, n \text{ is a psp}(T_u)\}$$

$$SB(n) = \#\{u : 0 \leq u < n, n \text{ is an spsp}(T_u)\}.$$

$$B(n) < n/2 \text{ and } SB(n) < n/8,$$

$$n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s} \ (p_1 < p_2 < \cdots < p_s)$$

$$\tau(n) < \begin{cases} 1/n^{4/3}, & \text{for } n \text{ nonsquare free with } s = 1; \\ 1/n^{2/3}, & \text{for } n \text{ square free with } s = 2; \\ 1/n^{2/7}, & \text{for } n \text{ square free with } s = 3; \\ \frac{1}{8^{s-4} \cdot 166(p_1+1)}, & \text{for } n \text{ square free with } s \text{ even } \geq 4; \\ \frac{1}{16^{s-5} \cdot 119726}, & \text{for } n \text{ square free with } s \text{ odd } \geq 5; \\ \frac{1}{4^s} \prod_{i=1}^s \frac{1}{p_i^{2(r_i-1)}}, & \text{otherwise, i.e., for } n \text{ nonsquare free with } s \geq 2. \end{cases}$$

$$2(y+3) + 4(y+12) = -2(y+10) + 4(y+6) + 3(2y+8)$$

$$2y + 6 + 4y + 48 = -2y - 20 + 4y + 24 + 6y + 24$$

$$3(2x+5y) + 2(4x+6y) = 4(9x+5y) + 3(2x+4y) + 2(4x+5y)$$

$$6x + 15y + 8x + 12y = 36x + 20y + 6x + 12y + 8x + 10y$$

$$3(a+b) + 4(a+2b) + 5(a+3b) = -3(a+4b) + 2(-6a+4b) + 3(2a+5b)$$

$$3a + 3b + 4a + 8b + 5a + 15b = -3a - 12b - 12a + 8b + 6a + 15b$$

$$2(m+2n) + 3(-2m+4n) = 5(6m-7n) + 3(5m+6n) + 2(4m+5n)$$

$$2m + 4n - 6m + 12n = 30m - 35n + 15m + 18n + 8m + 10n$$

$$7(x+4y-6z) = 4(4x-6y-7z) - 2(z+7x+3y)$$



The background is a dark blue digital landscape. At the center is a large, glowing blue padlock. Surrounding it are various elements: binary code (0s and 1s) at the top and bottom; circuit-like patterns and glowing lines on the left and right; and financial data on the bottom left, including a bar chart and a line graph. The text "Cryptography is interesting!" is centered over the padlock.

*Cryptography  
is  
interesting!*