

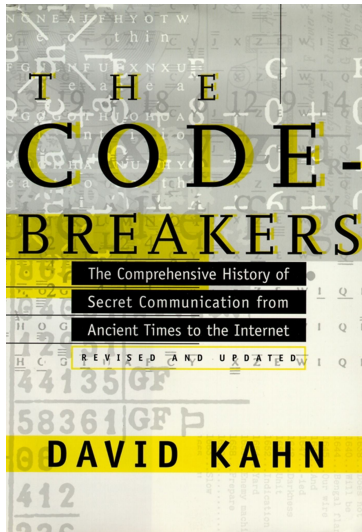
GEMS OF TCS

SECRET KEY CRYPTOGRAPHY

Sasha Golovnev

November 6, 2023

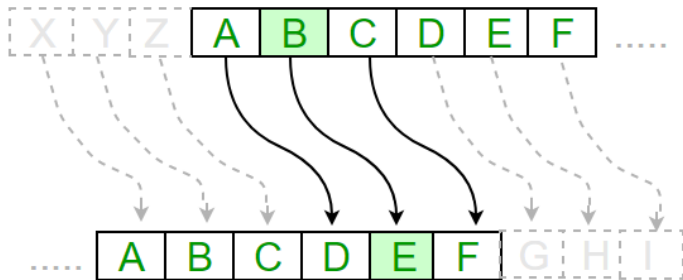
THE CODEBREAKERS



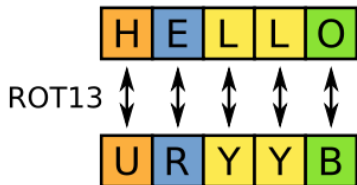
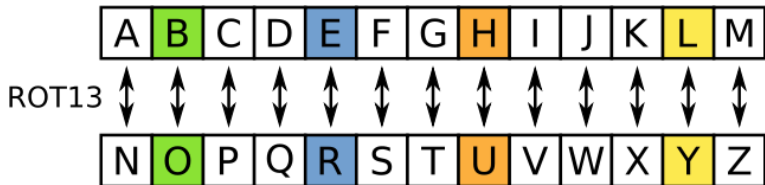
PIG LATIN

emsgay ofyay eorythay

CAESAR CIPHER

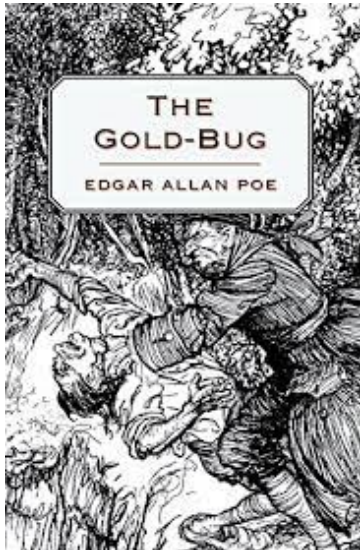


ROT13



SUBSTITUTION CIPHERS


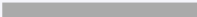






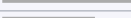












BREAKING SUBSTITUTION CIPHERS



Dancing Man Code (Sherlock Holmes)

X	+	5	X	X	Y	X	Y	Y	Y	Y	X	5	Y
A	B	C	D	E	F	G	H	I	J	K	L	M	
5	Y	Y	Y	Y	5	X	Y	Y	X	5	Y	Y	
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
X	5	X	5	X	5	X	5	X	5	X	5		
1	2	3	4	5	6	7	8	9	0				

LETTER FREQUENCY

e	13%	
t	9.1%	
a	8.2%	
o	7.5%	
i	7%	
n	6.7%	
s	6.3%	
h	6.1%	
r	6%	
d	4.3%	
l	4%	
c	2.8%	
u	2.8%	
m	2.4%	
w	2.4%	
f	2.2%	
g	2%	
y	2%	
p	1.9%	
b	1.5%	
v	0.98%	

EXAMPLE

qvw jds jqosu yqcw al jds qisnqes qtsnczqg qns
uysgj al jds ebisngtsgj cg vsuu jdqg q uszbgw

GOOD CIPHER

ONE-TIME PAD

PERFECT SECRECY

STREAM CIPHERS