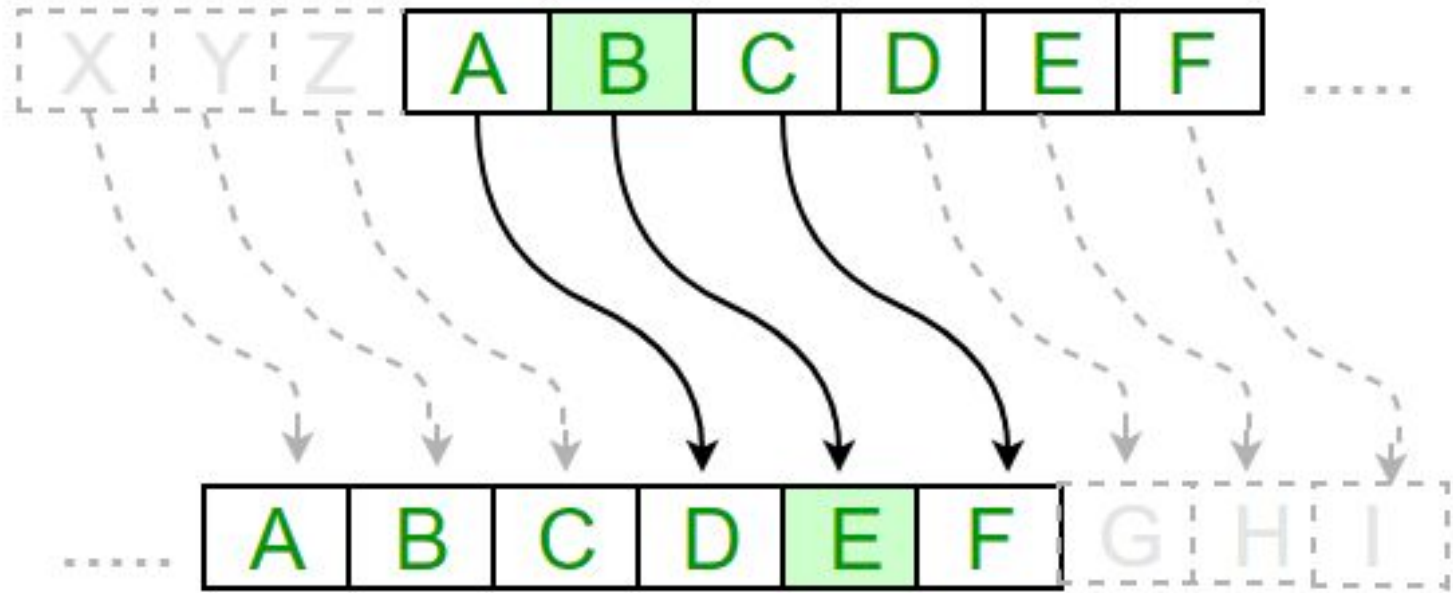


Breaking Weak Encryption

By Andrew Bernal and Joan Montas

Caesar Cipher



Decrypting with the Caesar Cipher

Encrypt: "Hello"

Decrypt: Slccd



The diagram illustrates a Caesar cipher shift by 3 spaces. It consists of two rows of 26 boxes each, representing the alphabet. The top row contains the letters A through Z in order. The bottom row contains the letters D through Z, followed by A, B, and C. Red vertical lines connect each letter in the top row to its corresponding letter in the bottom row, showing a consistent shift of 3 positions to the right. For example, A is connected to D, B to E, and so on, with Z connected to C.

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
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

Alphabet shifted by 3 spaces.

Vulnerabilities?

$$E_n(x) = (x + n) \bmod 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x + n) \bmod 26$$

(Decryption Phase with shift n)

Substitution Cipher

③

Substitution Cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZ

QWERTYUIOPASDFGHJKLZXCVBNM

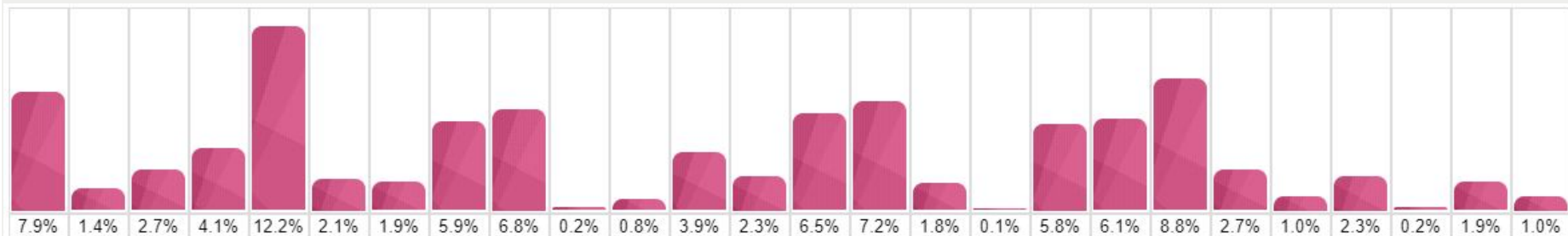
GRAY FOX HAS ARRIVED
UKQN YGB IQL QKKOCTR

Vulnerabilities?

Abū Yūsuf Ya‘qūb ibn ‘Ishāq aṣ-Ṣabbāḥ al-Kindī (/æɪˈkɪndi/; Arabic: أبو يوسف يعقوب بن إسحاق الصَّبَّاح الكندي; Latin: *Alkindus*; c. 801–873 AD)



Frequency Analysis



Vigenere

- Blaise de Vigenere
- Giovan Battista Bellaso (auto key cipher 1553)
- Friedrich Kasiki ("Attacking polyalphabetic substitution" - 1863)



Vigenere Cipher

• Plaintext:

ATTACKATDAWN

• Key:

LEMON

• Keystream:

LEMONLEMONLE

• Ciphertext:

LXFOPVEFRNIR

	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

Improvements on substitution?

Bigrams - Playfair Cipher

P	L-A	Y	F
I	R	E	X
B	C	D	G
K	N-O	Q	S
T	U	V	W
			Z

OL

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

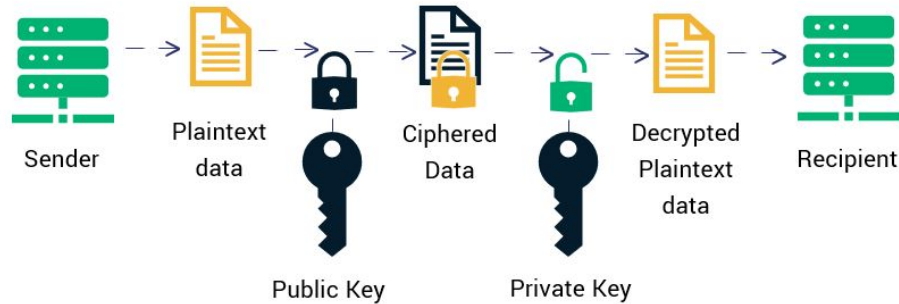
NA

Bigram Frequencies

No	Unigram	Frequencies	No	Unigram	Frequencies
1	TH	2.71	16	OR	1.06
2	HE	2.33	17	EA	1.00
3	IN	2.03	18	TI	0.99
4	ER	1.78	19	AR	0.98
5	AN	1.61	20	TE	0.98
6	RE	1.41	21	NG	0.89
7	ES	1.32	22	AL	0.88
8	ON	1.32	23	IT	0.88
9	ST	1.25	24	AS	0.87
10	NT	1.17	25	IS	0.86
11	EN	1.13	26	HA	0.83
12	AT	1.12	27	ET	0.76
13	ED	1.08	28	SE	0.73
14	ND	1.07	29	OU	0.72
15	TO	1.07	30	OF	0.71

RSA

How RSA Encryption Works



RSA Algorithm

Key Generation

Select p, q p and q both prime; $p \neq q$
Calculate $n = p \times q$
Calculate $\phi(n) = (p-1)(q-1)$
Select integer e $\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d $de \bmod \phi(n) = 1$
Public key $KU = \{e, n\}$
Private key $KR = \{d, n\}$

Encryption

Plaintext: $M < n$
Ciphertext: $C = M^e \bmod n$

Decryption

Plaintext: C
Ciphertext: $M = C^d \bmod n$

Stop my evil plan. Break my codes.

