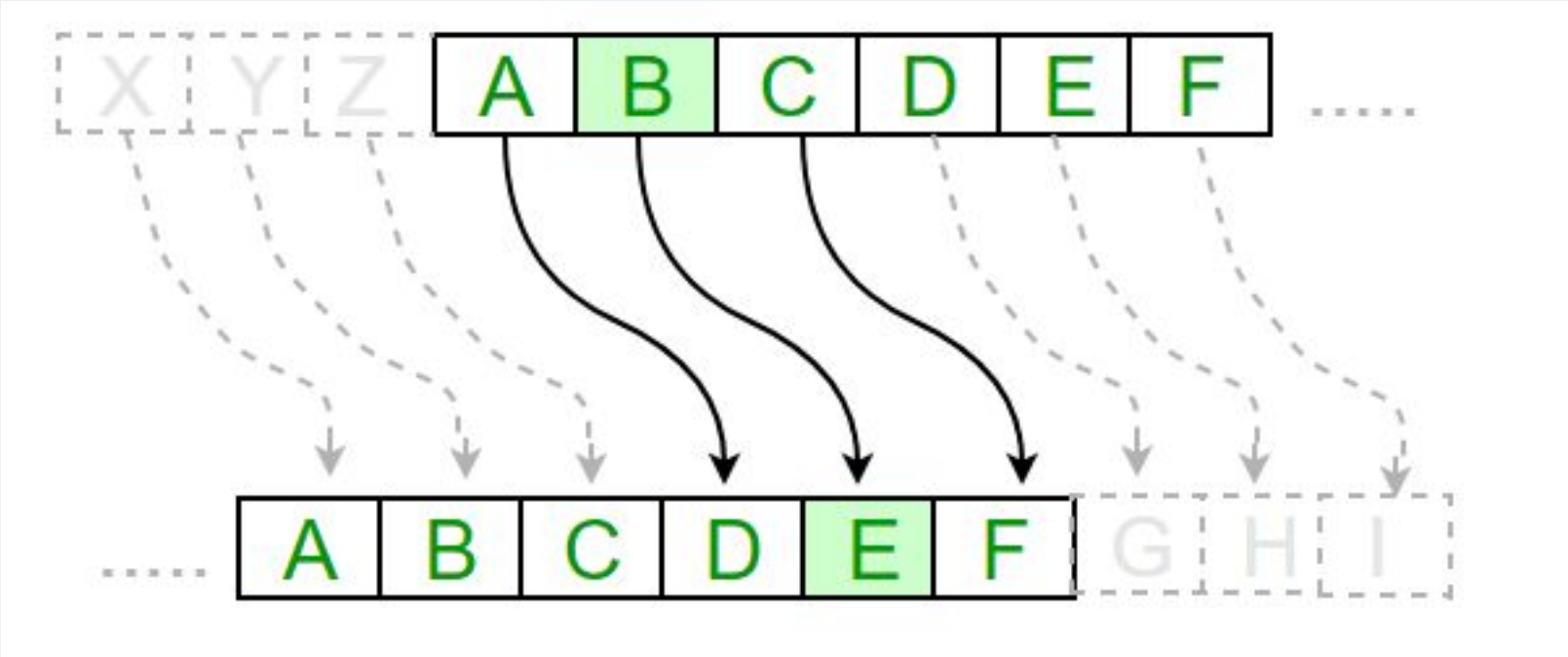
Breaking Weak Encryption

By Andrew Bernal and Joan Montas

Caesar Cipher



Decrypting with the Caesar Cipher

Encrypt: “Hello”
Decrypt: Slccd

Vulnerabilities?

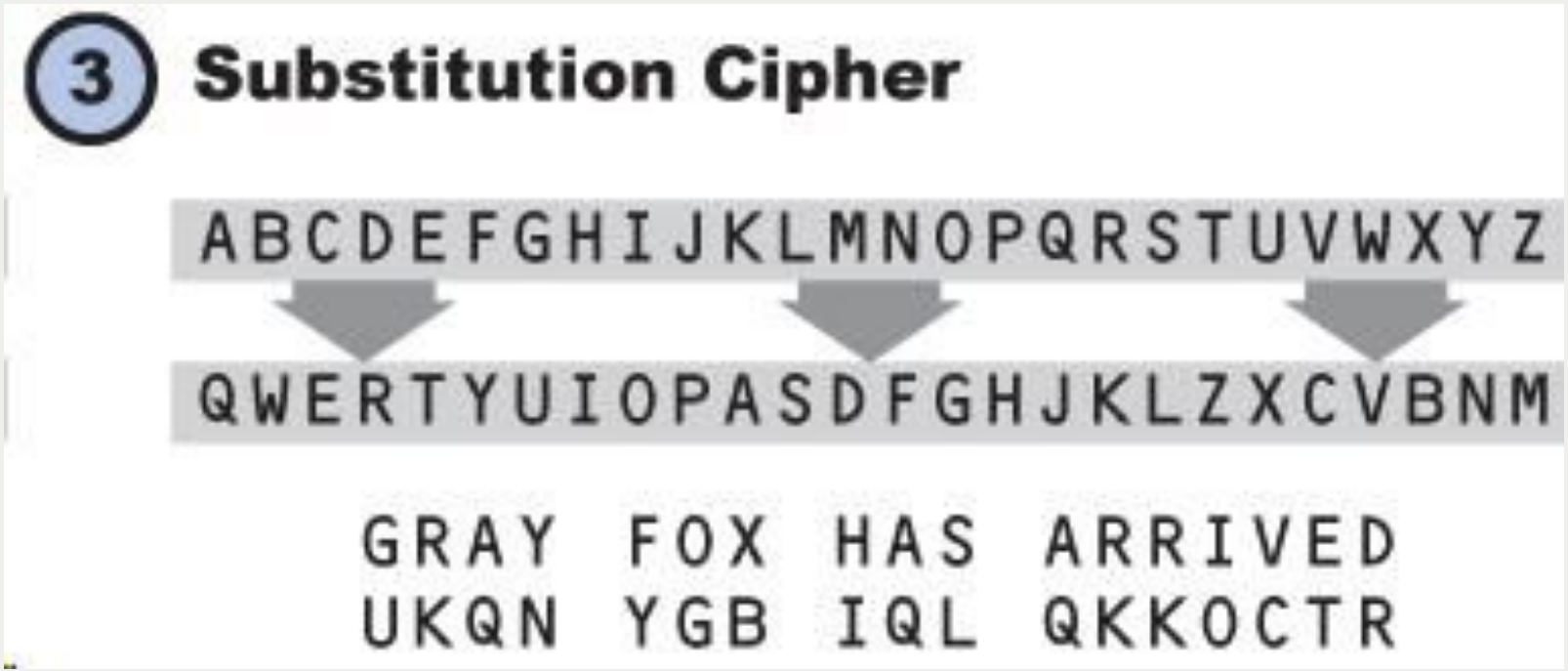
$$E_n(x) = (x + n) \bmod 26$$

(Encryption Phase with shift n)

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

(Decryption Phase with shift n)

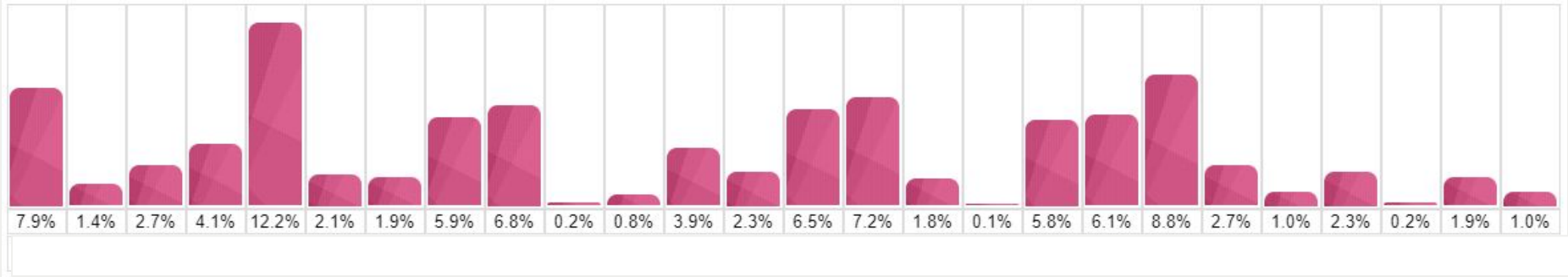
Substitution Cipher



Vulnerabilities?

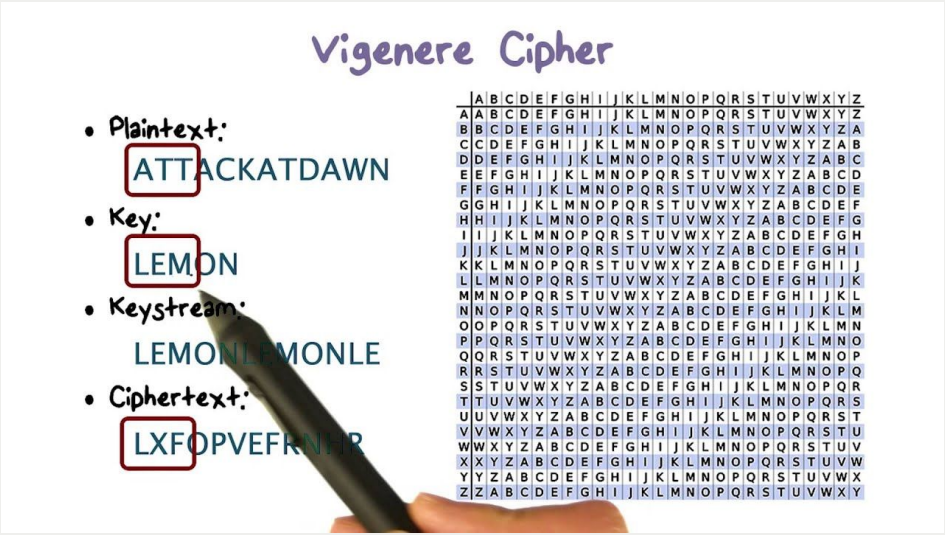
Abū Yūsuf Ya‘qūb ibn ’Isḥāq aṣ-Ṣabbāḥ al-Kindī (/ælˈkɪndi/; Arabic: أبو يوسف يعقوب بن إسحاق الصبّاح الكندي; Latin: *Alkindus*; c. 801–873 AD)

Frequency Analysis



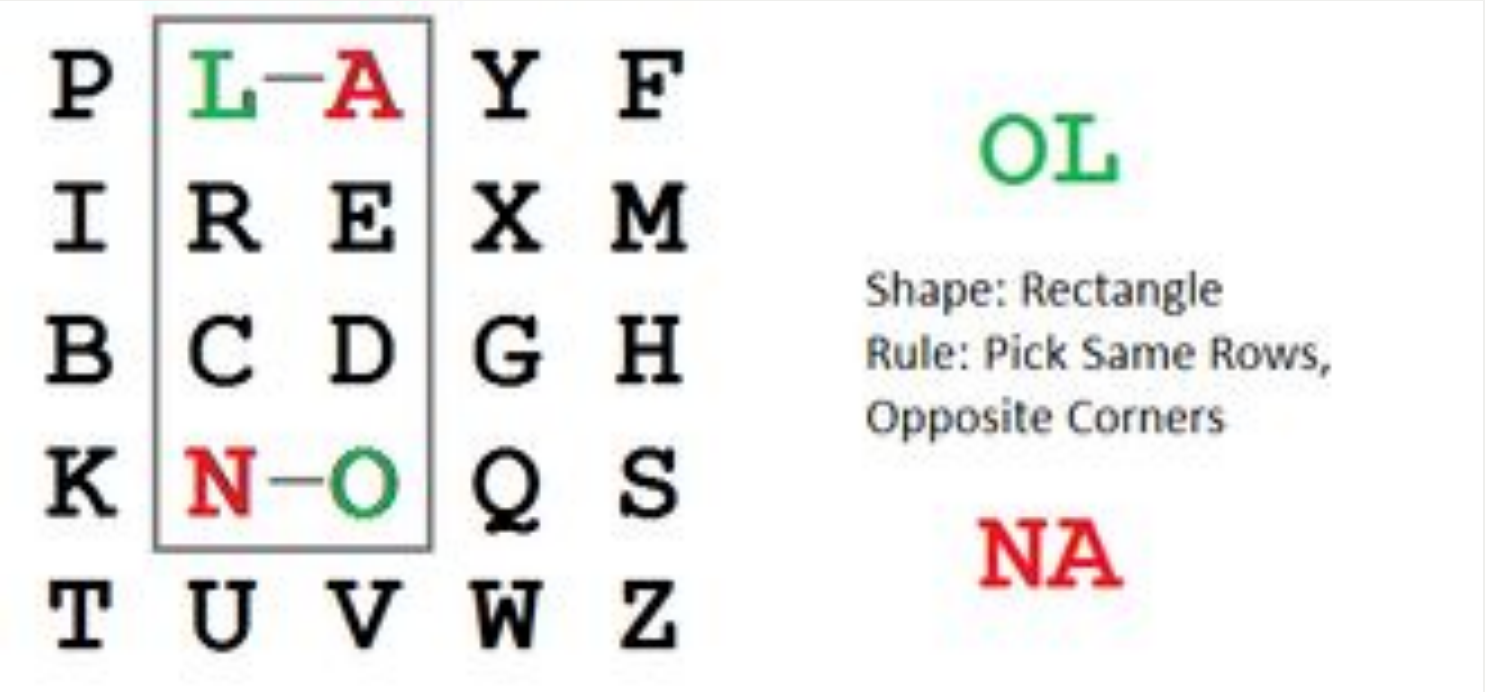
Vigenere

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



Improvements on substitution?

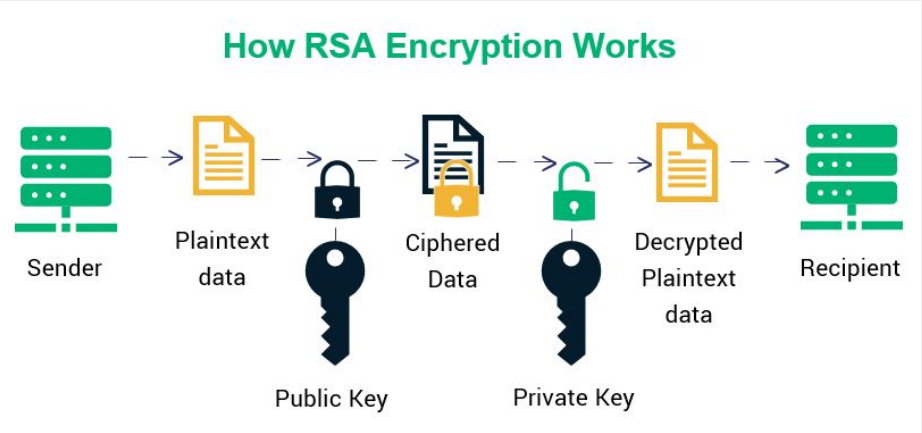
Bigrams – Playfair Cipher



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



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:	$C = M^e \pmod n$

Decryption

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

Stop my evil plan. Break my codes.