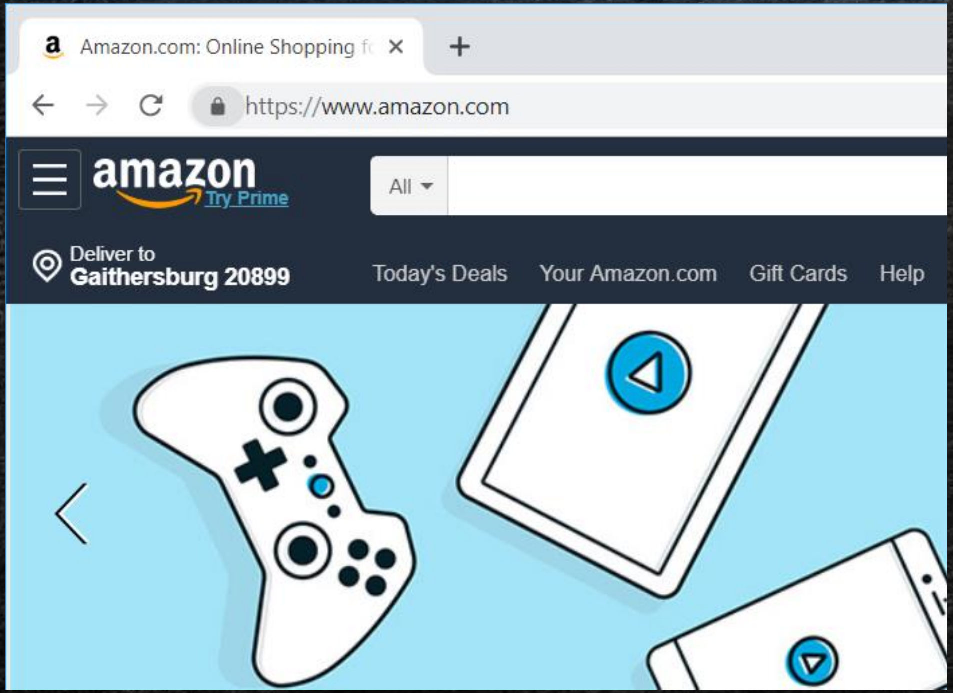
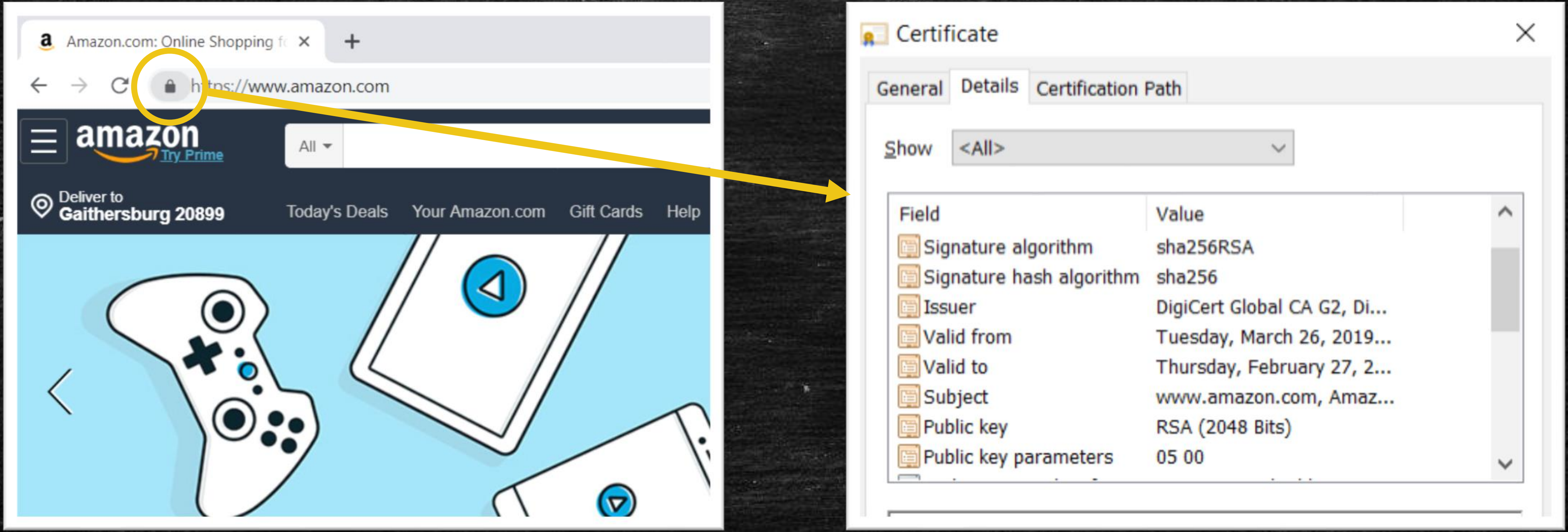
The Mathematics of Cryptography

Angela Robinson
National Institute of Standards and Technology

Cryptography sightings



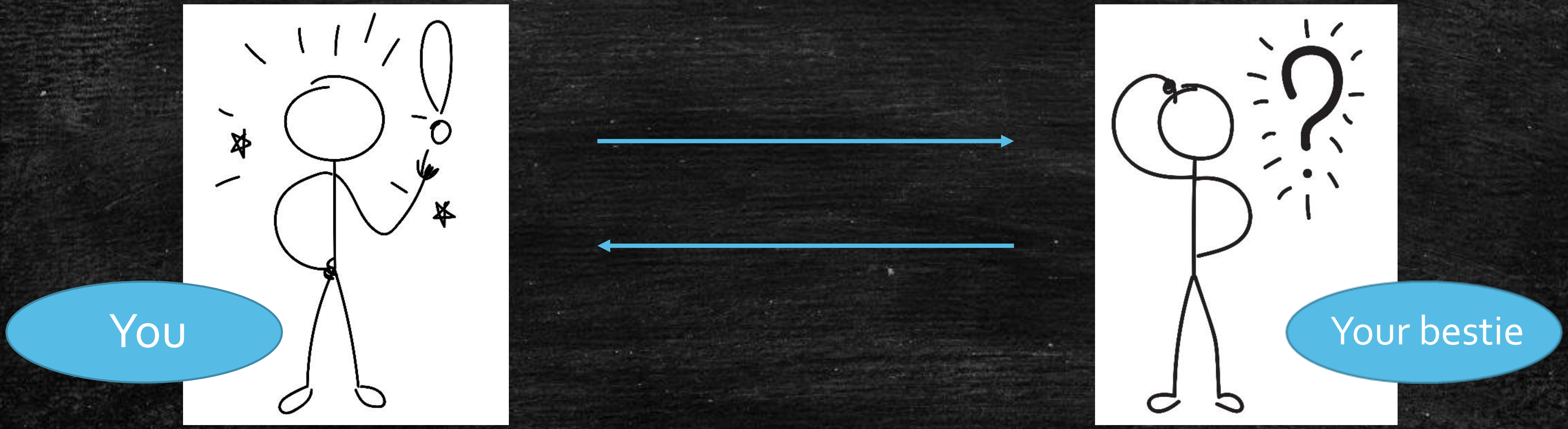
Cryptography sightings



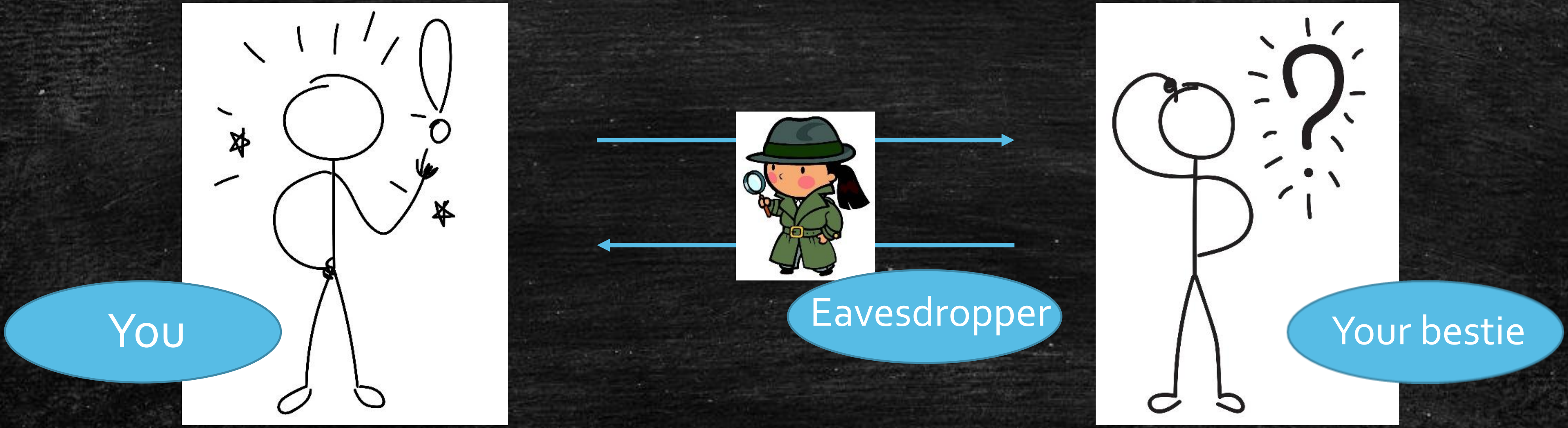
Secure websites are protected using:

- digital signatures – authenticity, integrity
- certificates – verify identity
- encryption – privacy

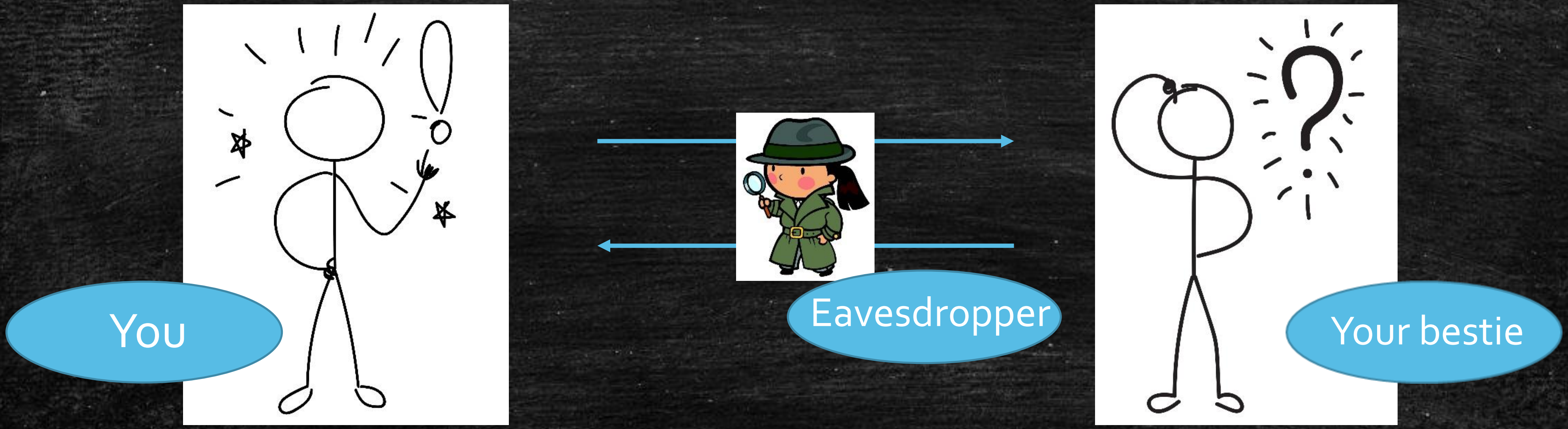
Encryption



Encryption



Encryption



Question: How can you communicate so that:

- Your bestie will understand your messages
- Eavesdroppers <u>cannot</u> understand your messages

Julius Caesar’s choice

S	E	C	R	E	T

Julius Caesar ruled a large empire

Communicated with his military leaders by messenger

Julius Caesar's choice

S	E	C	R	E	T
T	F	D	S	F	U

Encrypted his messages by shifting each letter 3 times *to the right*

Julius Caesar’s choice

S	E	C	R	E	T
T	F	D	S	F	U
U	G	E	T	G	V

Encrypted his messages by shifting each letter 3 times *to the right*

Julius Caesar’s choice

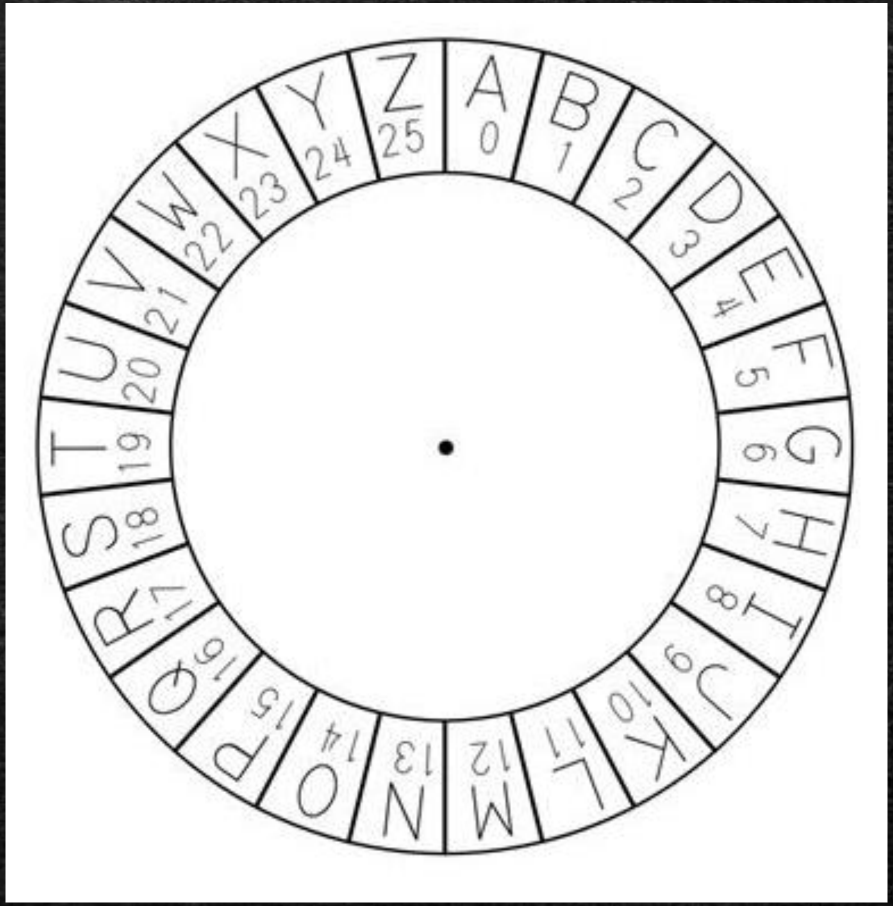
S	E	C	R	E	T
T	F	D	S	F	U
U	G	E	T	G	V
V	H	F	U	H	W

Send “V H F U H W” to military leaders

If anyone attacks the messenger, they won’t know what the secret message is

Shift Cipher

- Arrange letters in a circular fashion
- Assign numbers 0-25



Caesar used shift 3

Let shift be generalized to k

Shift Cipher

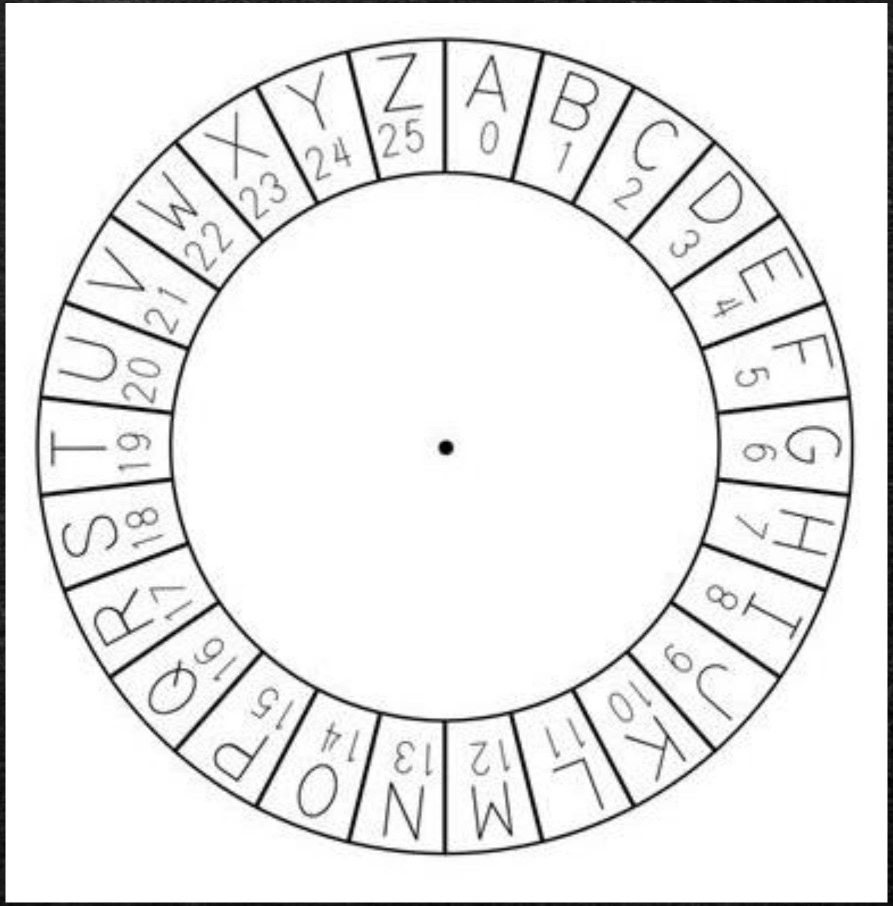
Caesar used shift 3

Let shift be generalized to k

k can be any number from 1 to 25.

What happens if we choose shift $k = 26$?

- Arrange letters in a circular fashion
- Assign numbers 0-25



Shift Cipher

Plaintext	**A**	**B**	**C**	**…**	**Y**	**Z**
Plaintext	0	1	2	…	24	25
Encrypt	$0 + k \; mod \; 26$	$1 + k \; mod \; 26$	$2 + k \; mod \; 26$		$24 + k \; mod \; 26$	$25 + k \; mod \; 26$

- Encryption:
  - Mathematically equivalent to *addition* by *k* modulo 26
- Decryption:
  - *Subtraction* by *k* modulo 26

Shift Cipher – Example
k= 12

Plaintext	W	A	R	N	I	N	G
Plaintext	22	0	17	13	8	13	6

- Encryption:
  - Mathematically equivalent to *addition* by 12 modulo 26
- Decryption:
  - *Subtraction* by 12 modulo 26

Shift Cipher – Example
k= 12

Plaintext	W	A	R	N	I	N	G
Plaintext	22	0	17	13	8	13	6
+12	34	12	29	25	20	25	18

- Encryption:
  - Mathematically equivalent to *addition* by 12 modulo 26
- Decryption:
  - *Subtraction* by 12 modulo 26

Shift Cipher – Example
k= 12

Plaintext	W	A	R	N	I	N	G
Plaintext	22	0	17	13	8	13	6
+12	~~34~~	12	~~29~~	25	20	25	18
mod 26	8	12	3	25	20	25	18

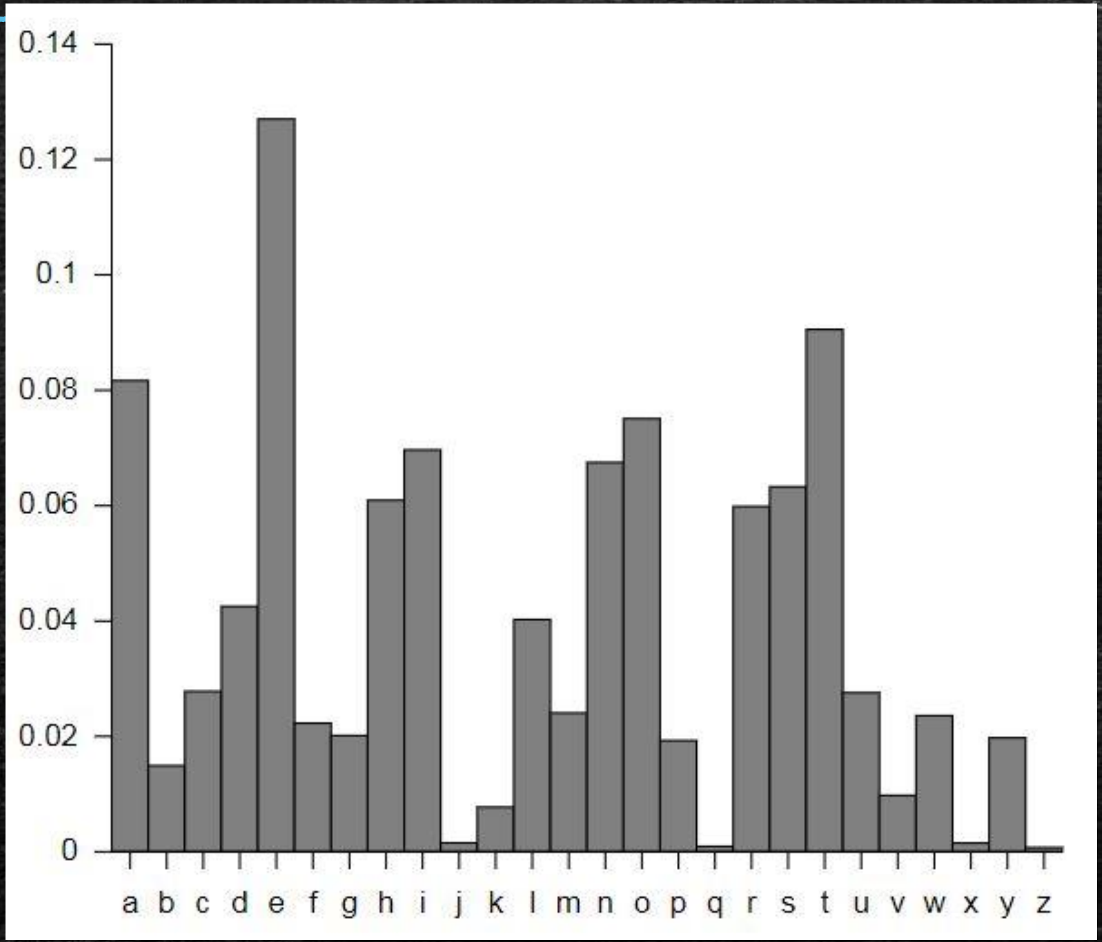
- Encryption:
  - Mathematically equivalent to *addition* by 12 modulo 26
- Decryption:
  - *Subtraction* by 12 modulo 26

# Shift Cipher – Example
k= 12

Plaintext	W	A	R	N	I	N	G
Plaintext	22	0	17	13	8	13	6
+12	~~34~~	12	~~29~~	25	20	25	18
mod 26	8	12	3	25	20	25	18
Ciphertext	I	M	D	Z	U	Z	S

WARNING $\longrightarrow$ IMDZUZS

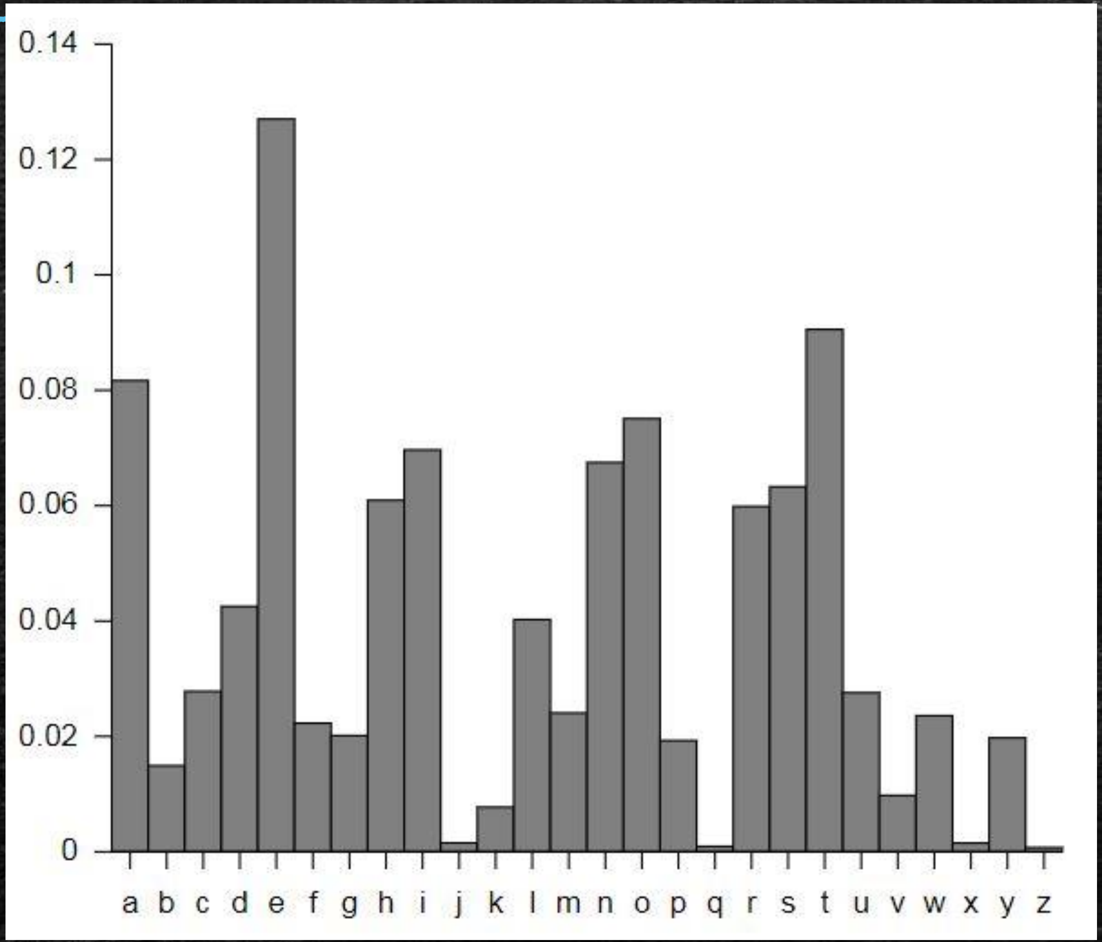
Cryptanalysis of Shift Cipher



Some letters are more commonly used in the English alphabet than others:

E, A, T, O …

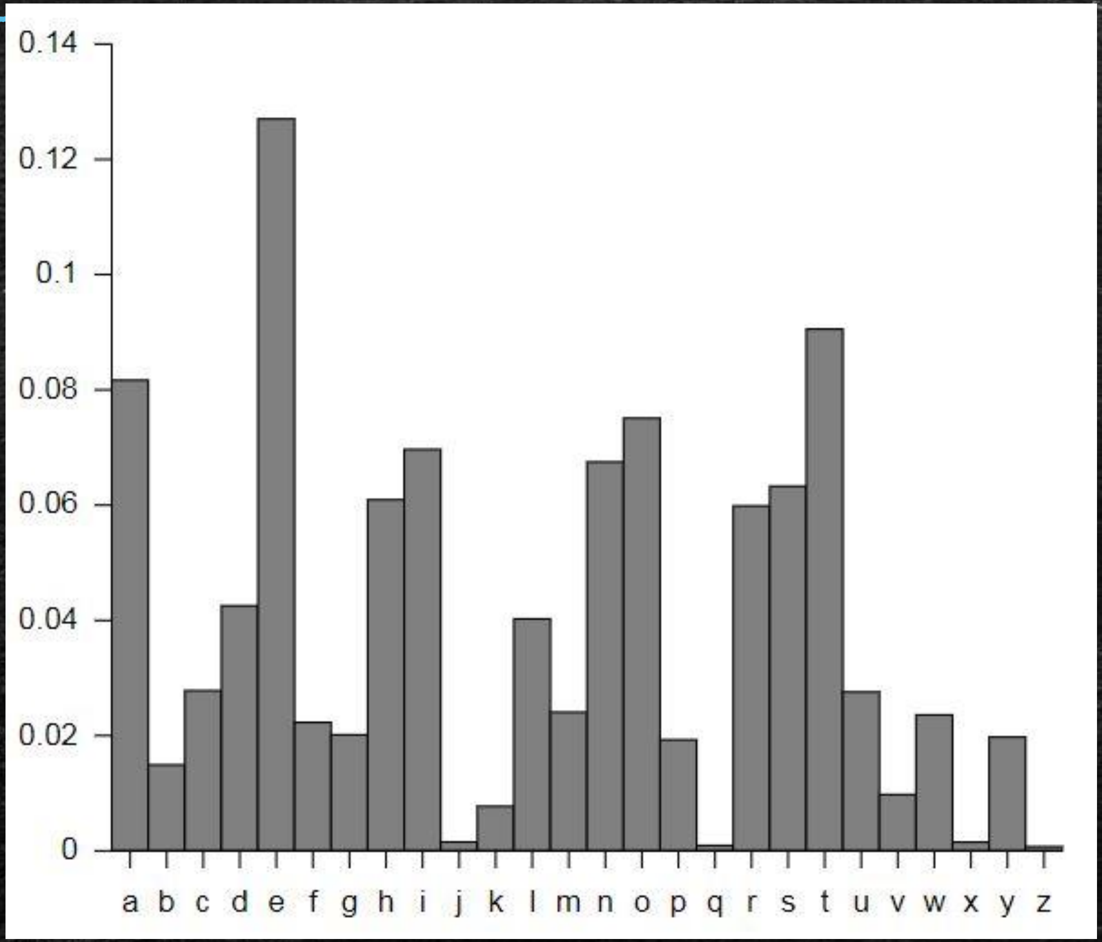
Cryptanalysis of Shift Cipher



Suppose you receive a Shift Cipher ciphertext:

```
wkh sdvvzrug lv vhyhq
grqw whoo dqbrqh
```

Cryptanalysis of Shift Cipher



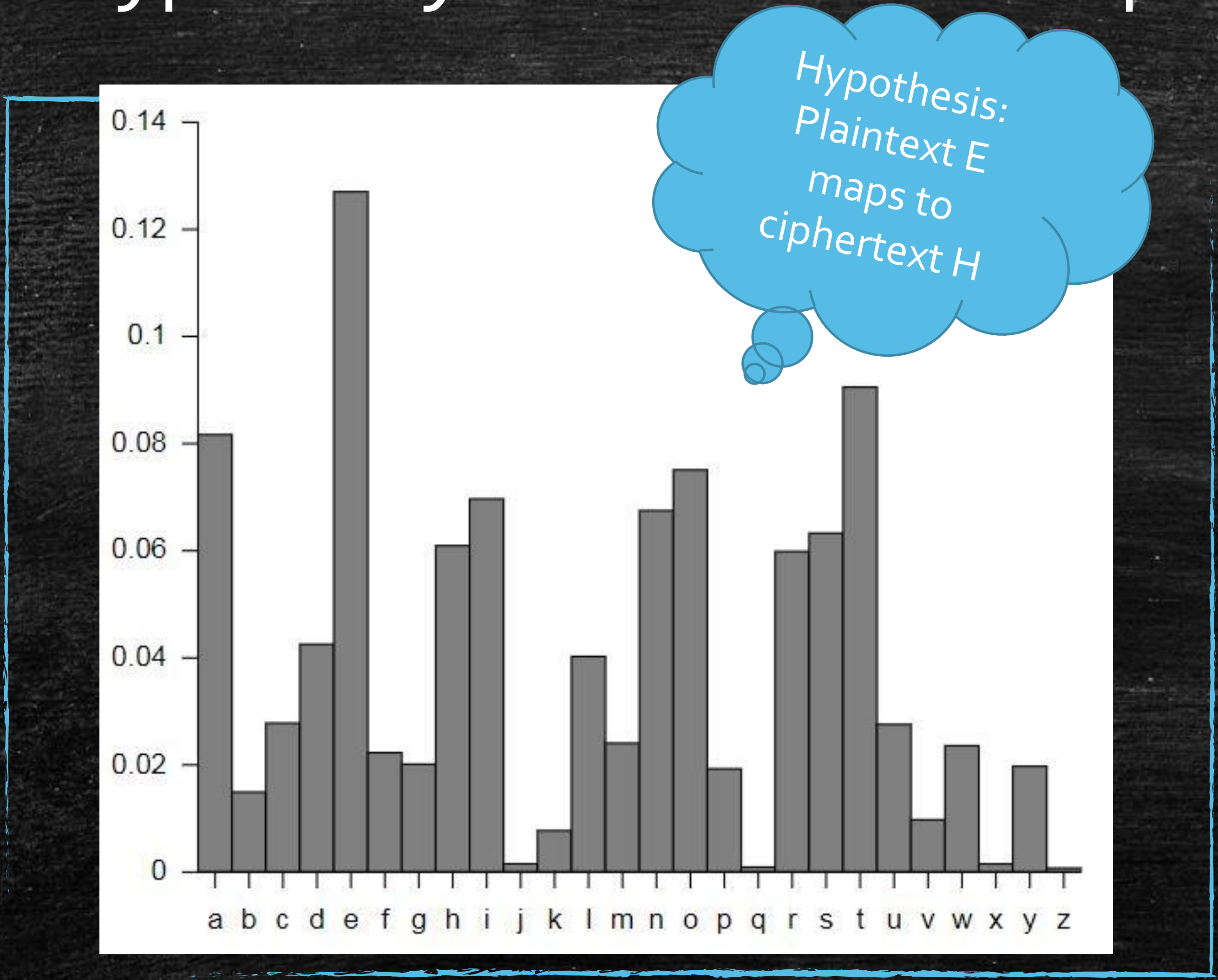
wkh sdvvzrug lv vhyhq
grqw whoo dqbrqh

Construct a letter frequency chart:

h = 5
v = 4

w = 3
q = 3
r = 3
g = 3
d = 2
b = 1
k = 1
l = 1
s = 1
y = 1

Cryptanalysis of Shift Cipher

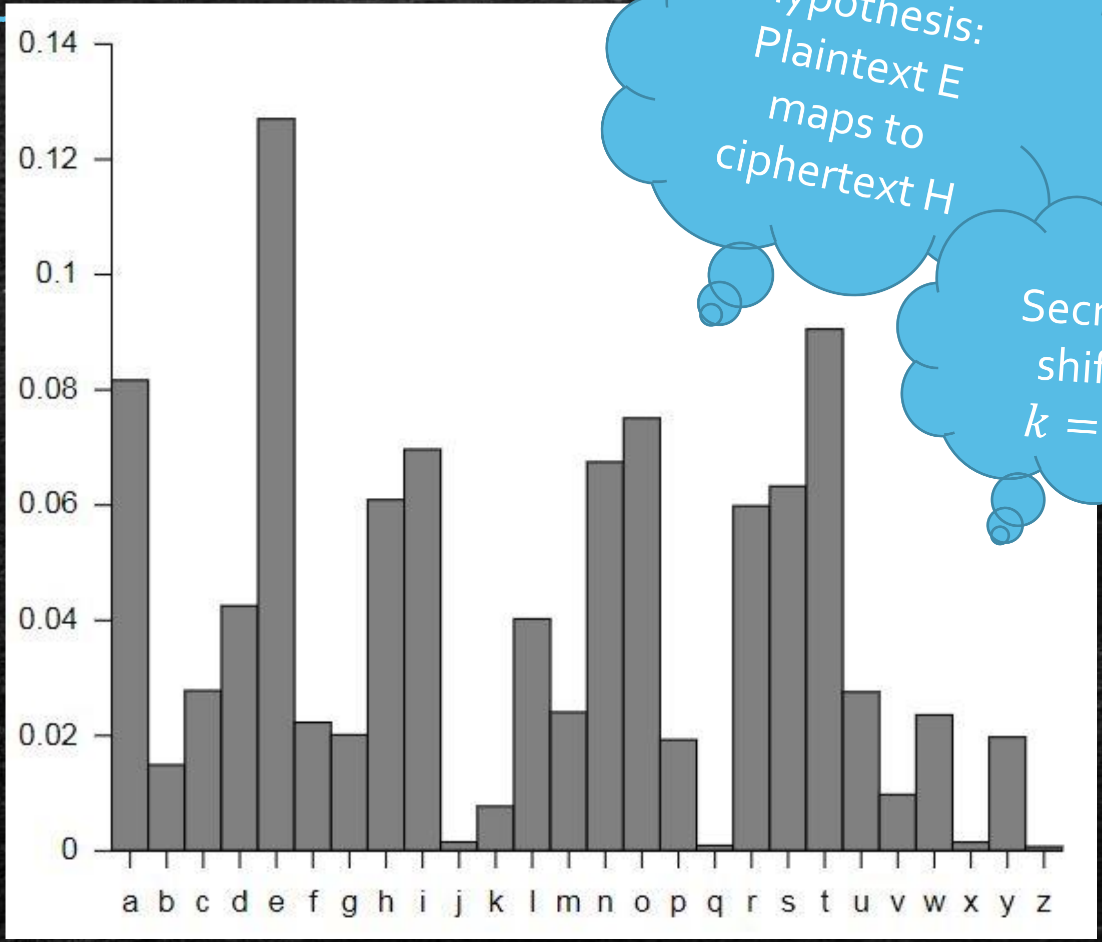



```
wkh sdvvzrug lv vhyhq
grqw whoo dqbrqh
```

Construct a letter frequency chart:

h = 5
v = 4
q = 3
r = 3
g = 3
d = 2
b = 1
k = 1
l = 1
s = 1
y = 1

Cryptanalysis of Shift Cipher



Hypothesis: Plaintext E maps to ciphertext H

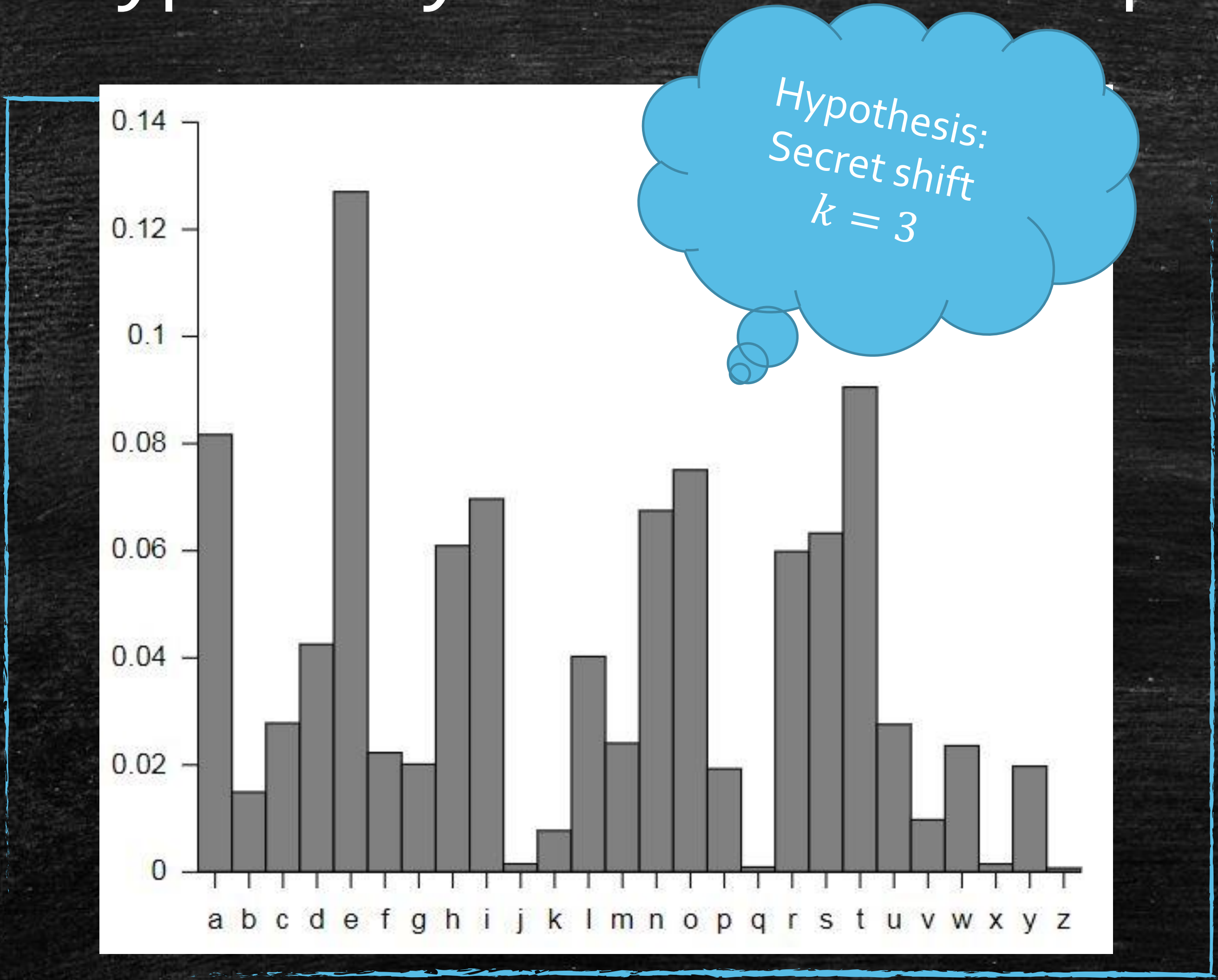
Secret shift $k = 3$

wkh sdvvzrug lv vhyhq grqw whoo dqbrqh

Construct a letter frequency chart:

h = 5
v = 4
q = 3
r = 3
g = 3
d = 2
b = 1
k = 1
l = 1
s = 1
y = 1

Cryptanalysis of Shift Cipher



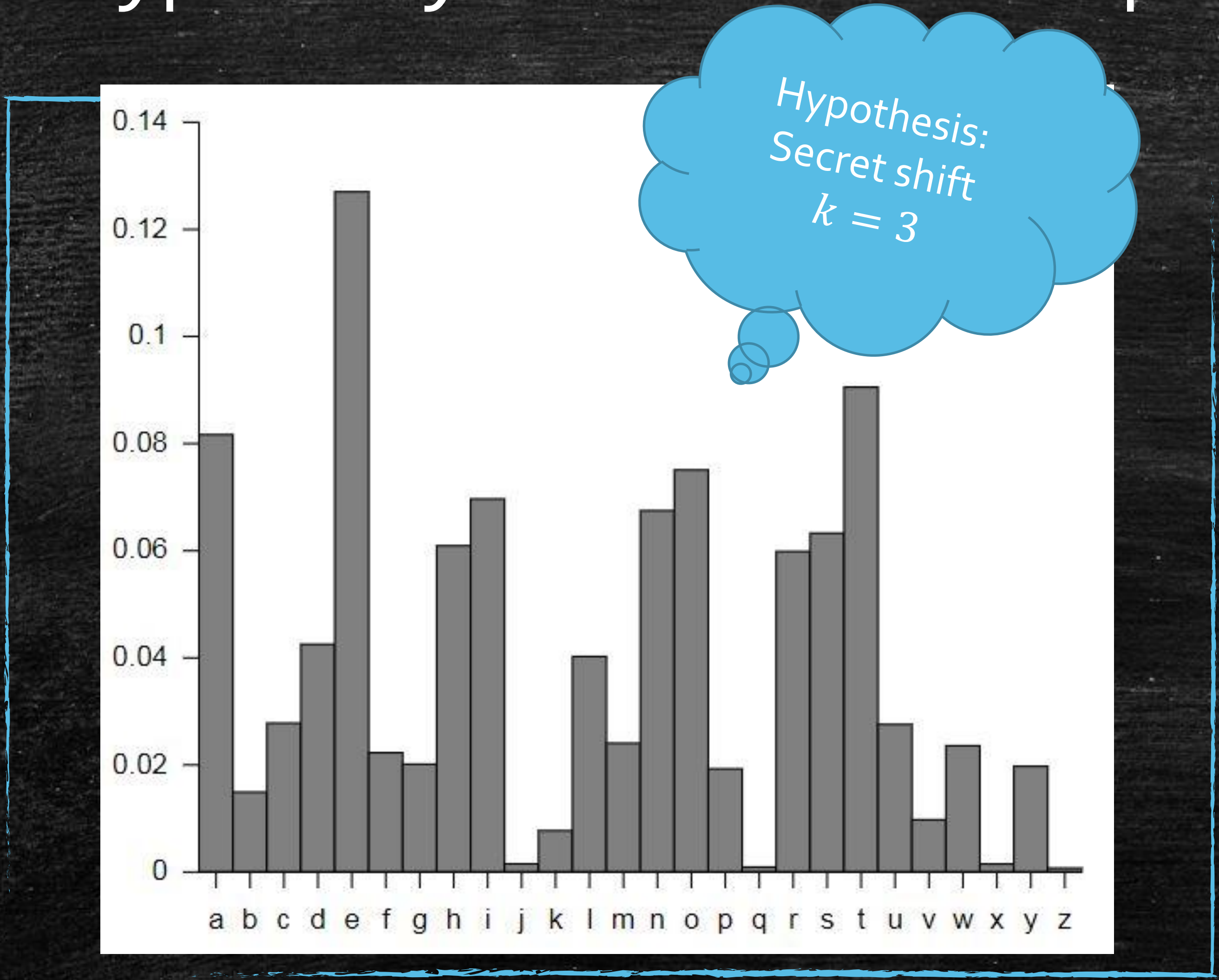
wkh sdvvzrug lv

THE

vhyhq grqw whoo

dqbrqh

Cryptanalysis of Shift Cipher



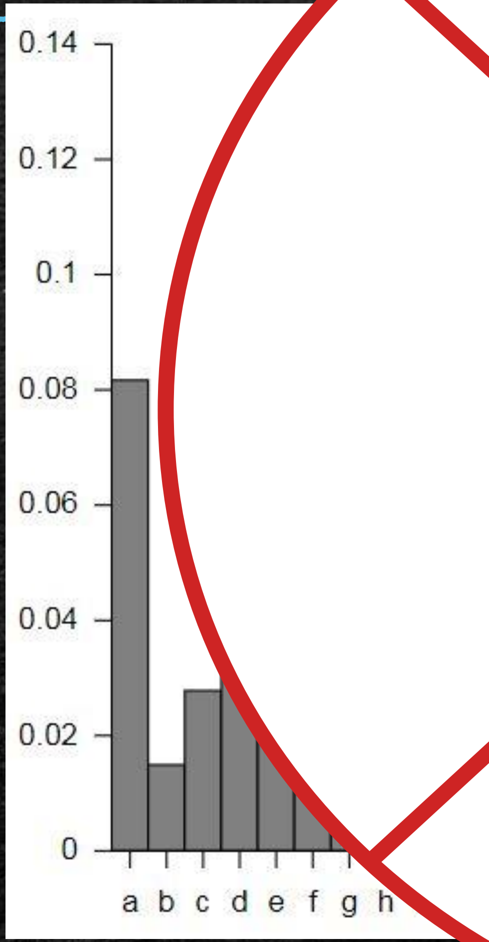
wkh sdvvzrug lv

THE PASSWORD IS

vhyhq grqw whoo

dqbrqh

Cryptanalysis ... r



... sdvvzrug lv

... PASSWORD IS

... grqw whoo

... qh

Only 26 distinct shifts possible

Too easy to “guess” the key!

Affine Cipher - encryption

- Instead of *plain addition* modulo 26:
  - Multiplication first
  - Then addition modulo 26

Plaintext	M	E	S	S	A	G	E
	12	4	18	18	0	6	4

Affine Cipher - encryption

- Instead of plain addition modulo 26:
  - Multiplication first
  - Then addition modulo 26

- Try (3,10)
  - Multiply by 3
  - Add 10 modulo 26

Plaintext	M	E	S	S	A	G	E
	12	4	18	18	0	6	4

Affine Cipher - encryption

- Instead of plain addition modulo 26:
  - Multiplication first
  - Then addition modulo 26

- Try (3,10)
  - Multiply by 3
  - Add 10 modulo 26

Plaintext	M	E	S	S	A	G	E
	12	4	18	18	0	6	4
x 3	36	12	54	54	0	18	12

Affine Cipher - encryption

- Instead of plain addition modulo 26:
  - Multiplication first
  - Then addition modulo 26

- Try (3,10)
  - Multiply by 3
  - Add 10 modulo 26

Plaintext	M	E	S	S	A	G	E
	12	4	18	18	0	6	4
x 3	36	12	54	54	0	18	12
+ 10	~~46~~	22	~~64~~	~~64~~	10	~~28~~	22
mod 26	20	22	12	12	10	2	22

Affine Cipher - encryption

- Instead of plain addition modulo 26:
  - Multiplication first
  - Then addition modulo 26

- Try (3,10)
  - Multiply by 3
  - Add 10 modulo 26

Plaintext	M	E	S	S	A	G	E
	12	4	18	18	0	6	4
x 3	36	12	54	54	0	18	12
+ 10	~~46~~	22	~~64~~	~~64~~	10	~~28~~	22
mod 26	20	22	12	12	10	2	22
	U	W	M	M	K	C	W

Affine Cipher - decryption

- Ciphertext
  $$C = a \cdot M + b \ mod \ 26$$

Need a way to “reverse” these mathematical steps:

1. Multiplication first
2. Then addition modulo 26

Affine Cipher - decryption

- Ciphertext

$$C = a \cdot M + b \; mod \; 26$$

Want to isolate "M"

Need a way to "reverse" these mathematical steps:

1. Multiplication first
2. Then addition modulo 26

Affine Cipher - decryption

- Ciphertext

$$C = a \cdot M + b \; mod \; 26$$

Want to isolate "M"

1. Subtract b

~~2. Divide by~~ $\cancel{a}$

   Multiply by the **multiplicative inverse** of $a \; mod \; 26$

Need a way to "reverse" these mathematical steps:

1. Multiplication first
2. Then addition modulo 26

Modular multiplicative inverse

Definition

- A multiplicative inverse of an integer a mod 26 is an integer x so that:

$$ax \equiv 1 mod\ 26.$$

Modular multiplicative inverse

Definition

- A multiplicative inverse of an integer a mod 26 is an integer x so that:

$$ax \equiv 1 mod\, 26.$$

Example:

- Let a=3.

$$3 * 1 = 3\, mod\, 26$$
$$3 * 2 = 6\, mod\, 26$$
$$3 * 3 = 9\, mod\, 26$$
$$\vdots$$
$$3 * 9 = 27 \equiv 1\, mod\, 26$$

Modular multiplicative inverse

Definition

- A multiplicative inverse of an integer a mod 26 is an integer x so that:

$$ax \equiv 1 mod\, 26.$$

Example:

- Let a=3.

$$3 * 1 = 3\; mod\; 26$$
$$3 * 2 = 6\; mod\; 26$$
$$3 * 3 = 9\; mod 26$$
$$\vdots$$
$$3 * 9 = 27 \equiv 1\; mod\; 26$$

Modular multiplicative inverse

Definition

- A multiplicative inverse of an integer a mod 26 is an integer x so that:

$$ax \equiv 1 mod\, 26.$$

Example:

- Let a=3.

$$3 * 1 = 3\; mod\; 26$$
$$3 * 2 = 6\; mod\; 26$$
$$3 * 3 = 9\; mod 26$$
$$\ldots$$
$$3 * 9 = 27 \equiv 1\; mod\; 26$$

The direct way to compute a modular multiplicative inverse is using the Extended Euclidean Algorithm!

Euclidean Algorithm

Euclid’s Division Theorem:

For any integers n, d there are unique integers q, r such that

$n = d \cdot q + r$ and $0 \leq r < d$.

Not every integer has a inverse modulo 26!

Affine cipher keys must have a multiplicative inverse for successful decryption!

Euclidean Algorithm

Euclid's Division Theorem:

For any integers n, d there are unique integers q, r such that

$n = d \cdot q + r$ and $0 \leq r < d$.

Suppose we want to find the greatest common divisor of integers a, b. Division Theorem states:

There are unique integers q, r such that

$$a = b \cdot q + r.$$

Euclidean Algorithm

Euclid's Division Theorem:

For any integers n, d there are unique integers q, r such that

$n = d \cdot q + r$ and $0 \leq r < d$.

Suppose we want to find the greatest common divisor of integers a, b. Division Theorem states:

There are unique integers q, r such that

$$a = b \cdot q + r.$$

If d divides a,

and d divides b,

then d must divide r

Euclidean Algorithm

Euclid's Division Theorem:

For any integers n, d there are unique integers q, r such that

$n = d \cdot q + r$ and $0 \leq r < d$.

Suppose we want to find the greatest common divisor of integers a, b. Division Theorem states:

there are unique integers q, r such that

$$a = b \cdot q + r.$$

If d divides a,

and d divides b,

then d must divide r

Euclidean Algorithm

Compute gcd(119,42):

119=42*2 + 35

42=35*1+7

35=7*5+0

The last nonzero remainder is the gcd!
Then 119 and 42 are not relatively prime.

If d divides a,

and d divides b,

then d must divide r

Euclidean Algorithm

Compute gcd(119,42):

119=42*2 + 35

42=35*1+7

35=7*5+0

The last nonzero remainder is the gcd! Then 119 and 42 are not relatively prime.

If $\gcd(a, b) = 1$, then a has a multiplicative inverse mod b.

If d divides a,

and d divides b,

then d must divide r

Affine Cipher - cryptanalysis

How many keys?

- Keys (a,b)
- a must be **relatively prime** to 26
- b an integer in {0,1,2,…,25}

Letter frequency analysis?

- This attack still applies
- Still not secure

Affine Cipher - cryptanalysis

How many keys?

- Keys (a, b)
- a must be **relatively prime** to 26
- b an integer in {0,1,2,…,25}

Letter frequency analysis?

- This attack still applies
- Still not secure

1	~~14~~
~~2~~	15
3	~~16~~
~~4~~	17
5	~~18~~
~~6~~	19
7	~~20~~
~~8~~	21
9	~~22~~
~~10~~	23
11	~~24~~
~~12~~	25
~~13~~	

Affine Cipher - cryptanalysis

How many keys?

- Keys (a, b)
- a must be **relatively prime** to 26
- b an integer in {0,1,2,…,25}

12 choices for a
26 choices for b

$12 * 26$ =312 choices for (a,b)

Letter frequency analysis?

- This attack still applies
- Still not secure

1	~~14~~
~~2~~	15
3	~~16~~
~~4~~	17
5	~~18~~
~~6~~	19
7	~~20~~
~~8~~	21
9	~~22~~
~~10~~	23
11	~~24~~
~~12~~	25
~~13~~	

Preventing letter frequency attacks

The problem with Shift Ciphers and Affine Cipher is that plaintext letters consistently map to the same ciphertext letters:

WARNING $\longrightarrow$ IMDZUZS

MESSAGE $\longleftarrow$ UWMMKCW

Must encrypt so that, for example, plaintext A's map to different letters in ciphertext.

One time pad

Suppose secret key k is a long string of random letters:

F D O J C E T M Q Z P I I Y …
5 3 14 9 2 4 19 12 16 25 15 8 8 24

Alice encrypts her message: MESSAGE by adding the first 7 letters of the secret key as follows

	M	E	S	S	A	G	E
	12	4	18	18	0	6	4
+ KEY	5	3	14	9	2	4	19
mod 26							

One time pad

Suppose secret key k is a long string of random letters:

F D O J C E T M Q Z P I I Y …
5 3 14 9 2 4 19 12 16 25 15 8 8 24

Alice encrypts her message: MESSAGE by adding the first 7 letters of the secret key as follows

	M	E	S	S	A	G	E
	12	4	18	18	0	6	4
+ KEY	5	3	14	9	2	4	19
mod 26	17	7	~~32~~	~~27~~	2	10	23
	17	7	6	1	2	10	23
	R	H	G	B	C	K	X

One time pad

One-time pad secret key is a long string of random letters:

F D O J C E T M Q Z P I I Y …
5 3 14 9 2 4 19 12 16 25 15 8 8 24

Affine cipher secret key is a pair of integers (a, b)

Shift cipher secret key is one integer k

Security vs efficency

One-time pad

secret key is a long string of random letters, length n

26^n possible keys

Affine cipher

secret key is a pair of integers (a, b)

312 possible keys

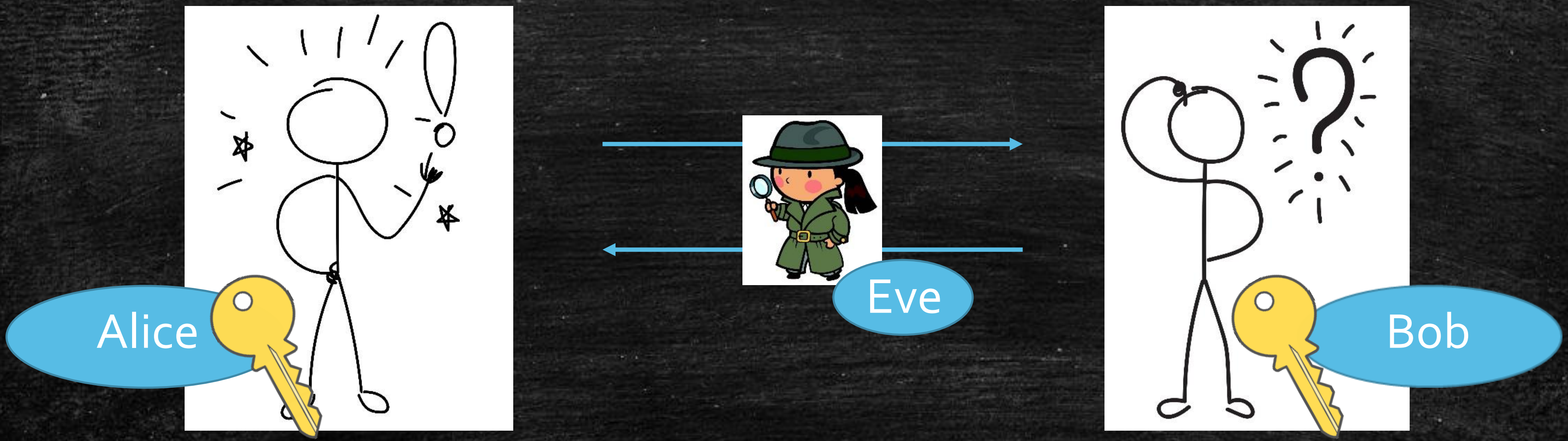
Shift cipher

secret key is one integer k

25 possible keys

Goals of cryptography

Key Exchange

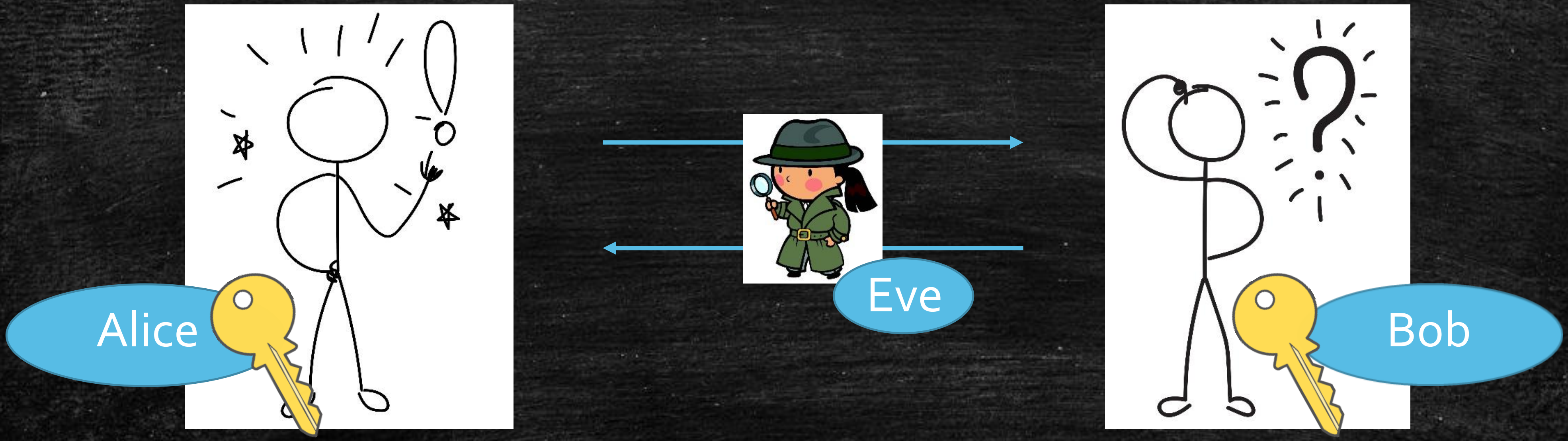


Notice that in the Shift Cipher and Affine cipher, the same key is used to encrypt and decrypt.

Then Alice and Bob must share a key **before** they can communicate privately.

Goals of cryptography

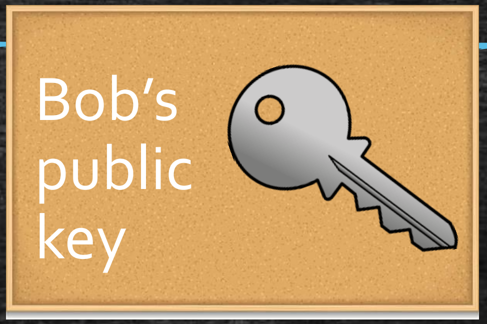
Key Exchange



Question: How can Alice and Bob communicate so that

- they both learn a shared secret key
- the eavesdropper <u>does not</u> learn the key?

Goals of cryptography



Public key encryption

Question: How can Alice and Bob communicate so that

- Bob can understand Alice's messages
- eavesdroppers <u>cannot</u> understand Alice's messages
- Alice and Bob DON'T need to share the same secret key ?

Thank you!

angela.robinson@nist.gov