CTF Training Camp - Crypto

Open Innovation Lab

Jason
Xaviera

Cryptography?

- Encryption & Decryption
- Classical cipher
  - Substitution ciphers
  - Transposition ciphers
- Modern cryptography
  - Symmetric-key cryptography
  - Public-key cryptography
  - Hash function

Before we start

- Common Encoding Scheme
  - Ascii
  - Base64
  - Morse code
  - And more...

Encryption & Decryption

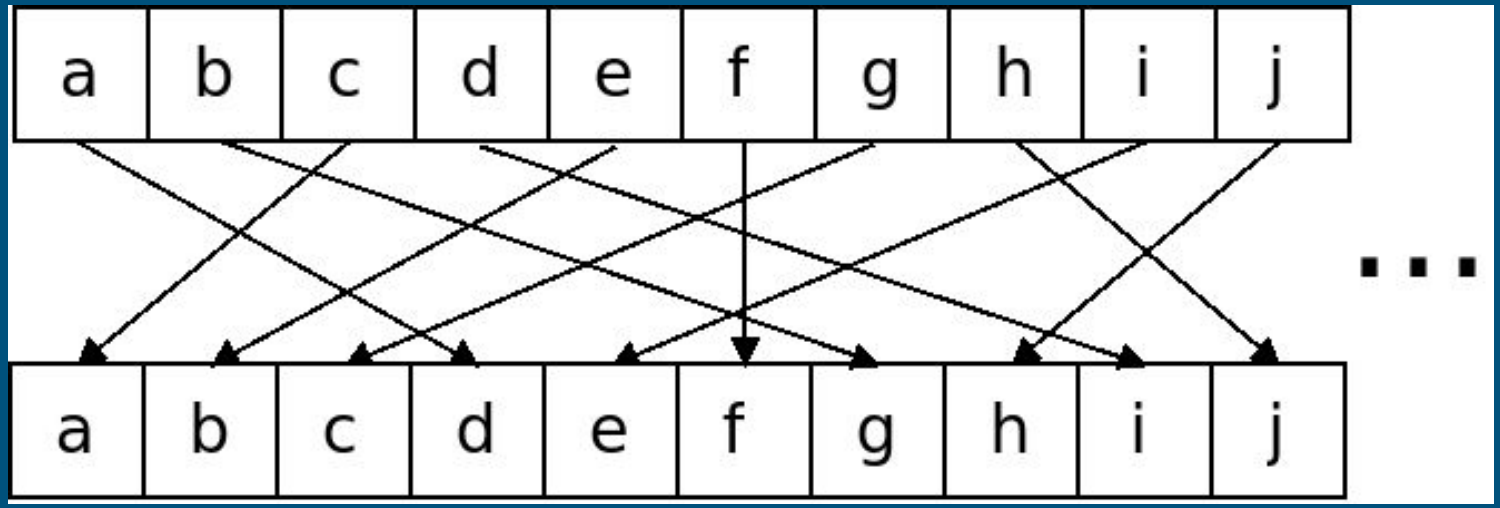
Some terminology :

- Plaintext = Message (m)
- Ciphertext = Encrypted Message (c)
- Key (k)
- Encryption with key k : $E_{k1}(m) \rightarrow c$
- Decryption: $D_{k2}(c) \rightarrow m$

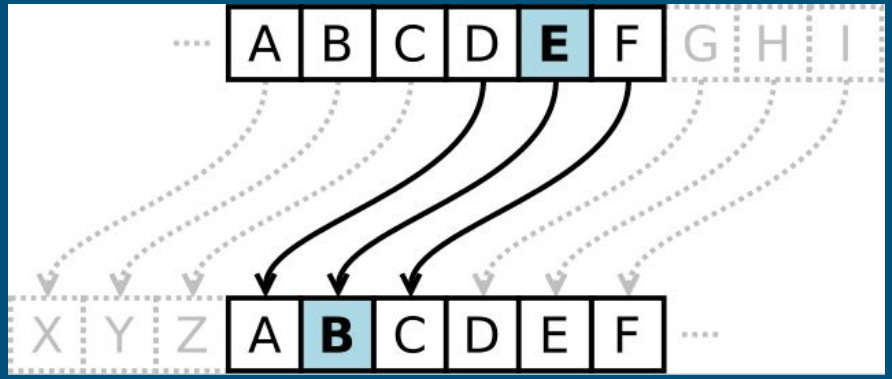
- *k1 = k2?*

Classical cipher

Substitution ciphers



Caesar cipher



Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

Key = ?

Exercise:

Ciphertext: ZXBPXO PXIXA
Plaintext = ?

Caesar cipher (Cont.)

What is mod?

- Encryption: $E_k(m) = (m + k) \bmod 26$
- Decryption: $D_k(c) = (c - k) \bmod 26$
- k = 13 -> ROT13

http://www.rot13.com/

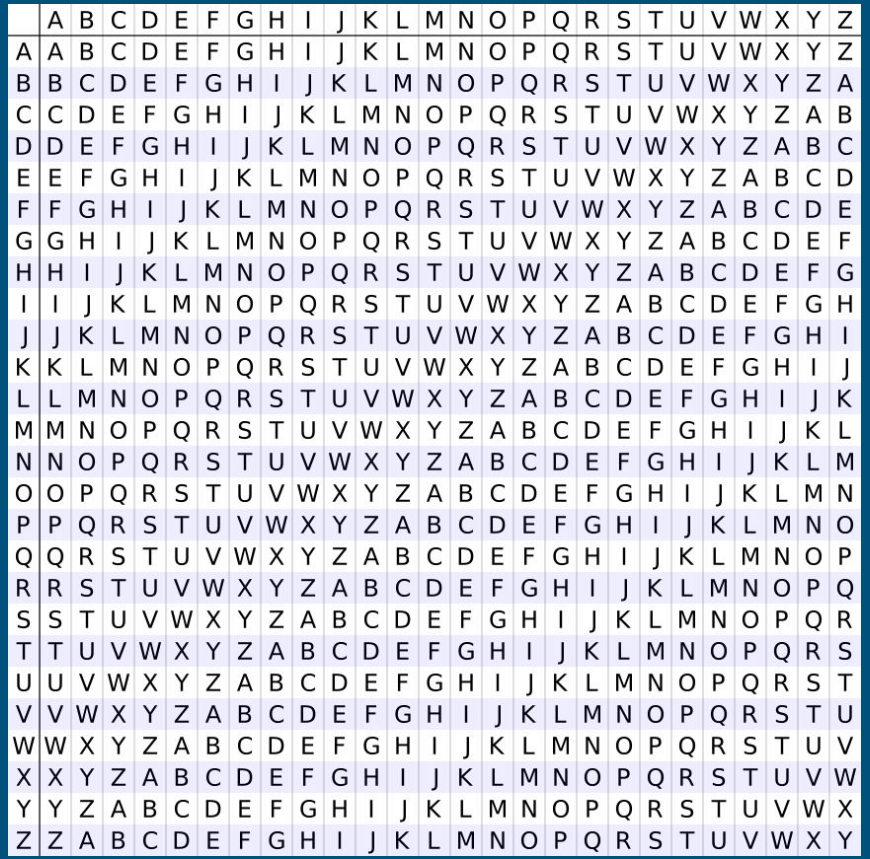
- picoCTF 2014 - Caesar (Crypto, 20p)

```
You find an encrypted message written on the documents. Can you decrypt it?
uiftfdsfuqbttqisbtfjtpgtqyrdhekuqsxjdtvyvkghlpvkfml
```

Vigenère cipher

- Similar to Caesar cipher
- Example:
- Message = attack at dawn, key = lemon

Plaintext:	ATTACKATDAWN
Key:	LEMONLEMONLE
Ciphertext:	LXFOPVEFRNHR



	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

Vigenère cipher (Cont.)

- Encryption: $E_k(m_i) = (m_i + k_i) \bmod 26$
- Decryption: $m_i = D_k(c_i) = (c_i - k_i) \bmod 26$

- SECCON CTF 2017 - Vigenere 3d (Crypto, 100p)

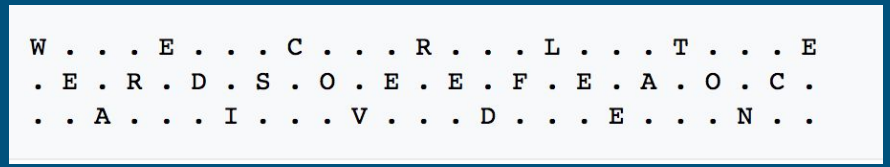
How to solve?

- Brute force (https://www.dcode.fr/tools-list)
- Frequency analysis

Transposition ciphers

- Rail Fence cipher

- Plaintext: WE ARE DISCOVERED FLEE AT ONCE
- Ciphertext: WECRL TEERD SOEEF EAOCA IVDEN

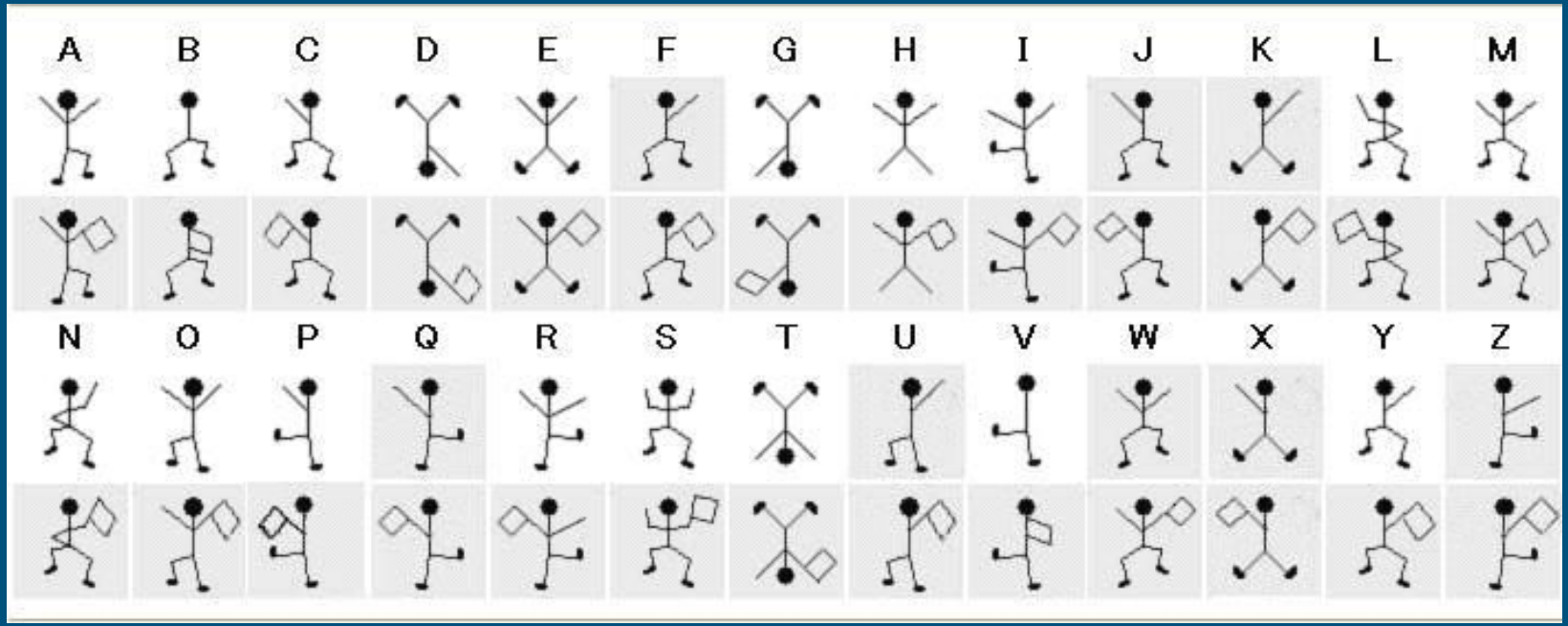


Transposition ciphers

- Columnar Transposition Cipher

h	o	w	a	r	e	u
3	4	7	1	5	2	6
T	h	e	q	u	i	c
k	b	r	o	w	n	f
o	x	j	u	m	p	s
o	v	e	r	t	h	e
l	a	z	y	d	o	g

Others?



Others?

2014 0ctf

Modern cryptography

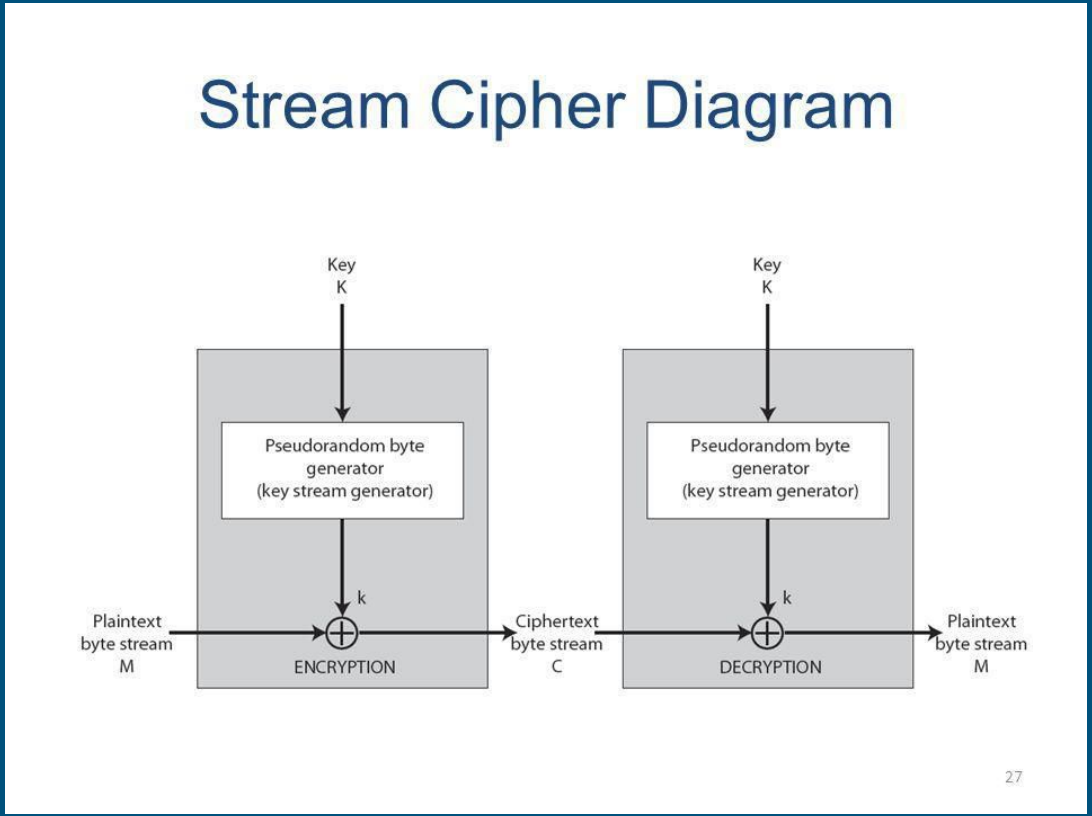
- Symmetric key v.s. Asymmetric key

=> encryption & decryption using the same key or not

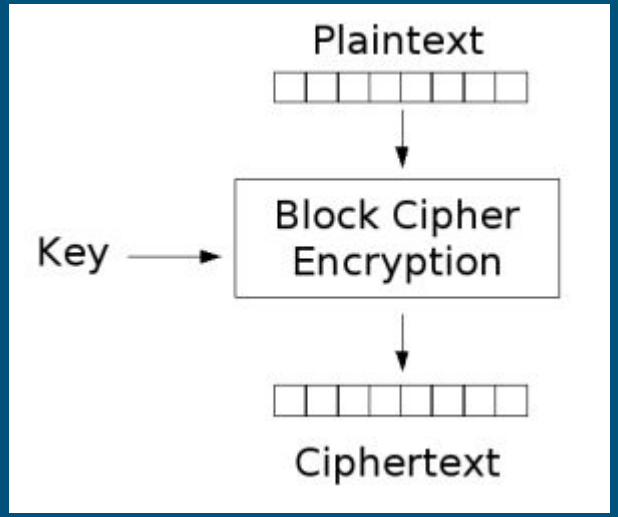
Symmetric-key cryptography

- Stream ciphers v.s. Block ciphers
- Mode of operation

Stream Cipher



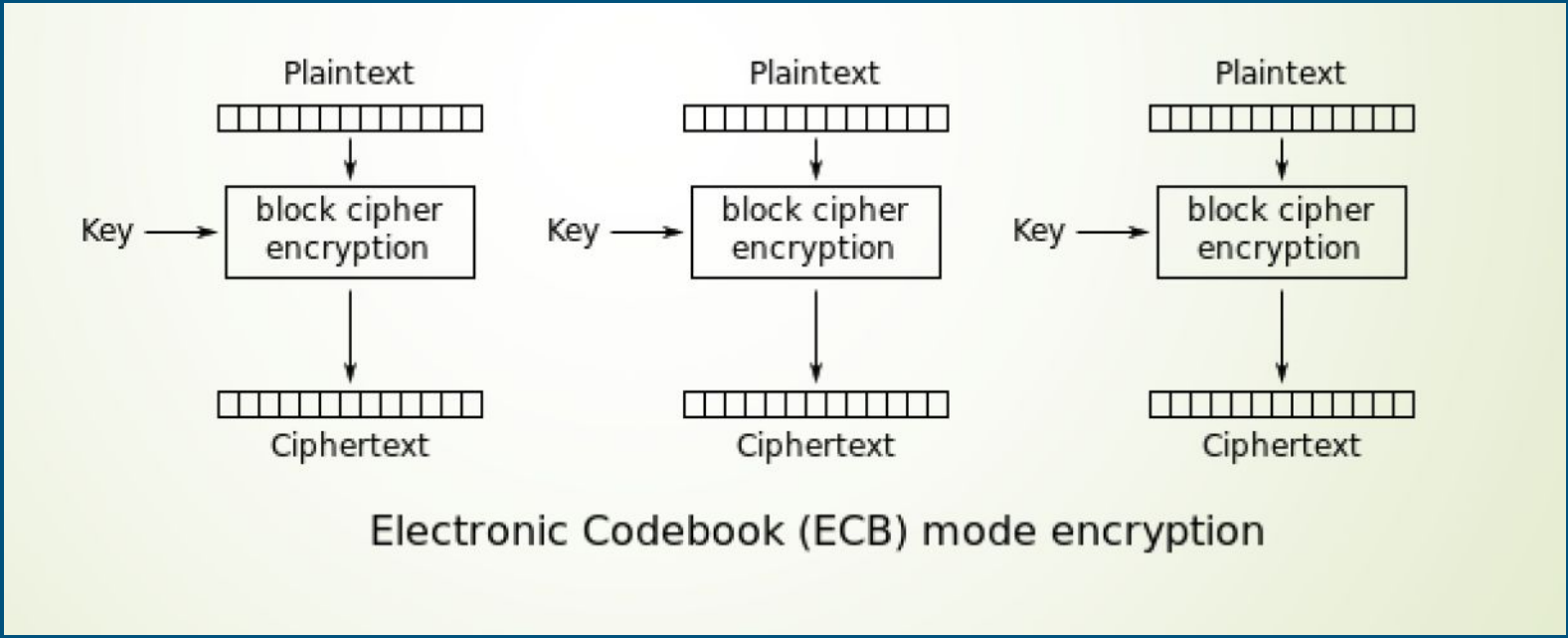
Block cipher



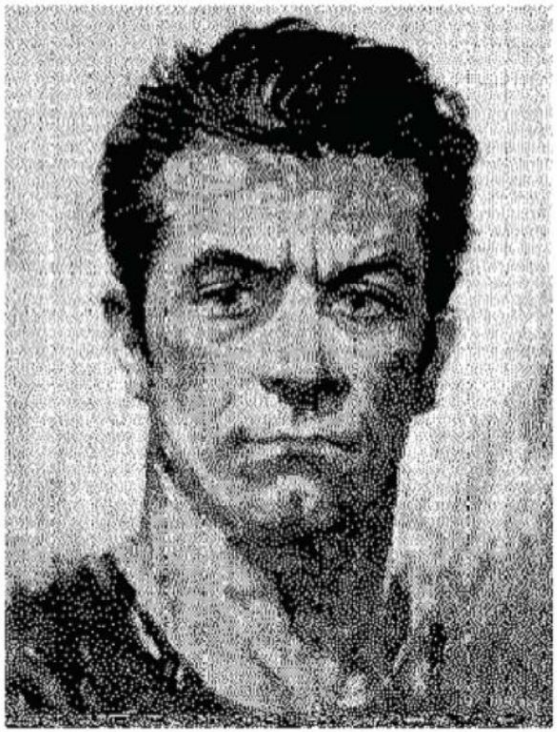
Mode of operation

- Electronic Code Book (ECB)
  - $c_i = Enc(sk, m_i)$
- Cipher Block Chaining (CBC)
  - $c_{-1} = IV$, $c_i = Enc(sk, c_{i-1} \text{ xor } m_i)$
- Cipher Feedback (CFB)
  - $c_{-1} = IV$, $c_i = Enc(sk, c_{i-1})$ xor mi
- Output Feedback (OFB)
  - $r_{-1} = IV$, ri = $Enc(sk, r_{i-1})$, $c_i = r_i \text{ xor } m_i$
- Counter (CTR)
  - $r_i = Enc(sk, IV \text{ xor } i)$, $c_i = r_i \text{ xor } m_i$

ECB


Plaintext
Key
block cipher encryption
Ciphertext
Plaintext
Key
block cipher encryption
Ciphertext
Plaintext
Key
block cipher encryption
Ciphertext
Electronic Codebook (ECB) mode encryption

Any problem?

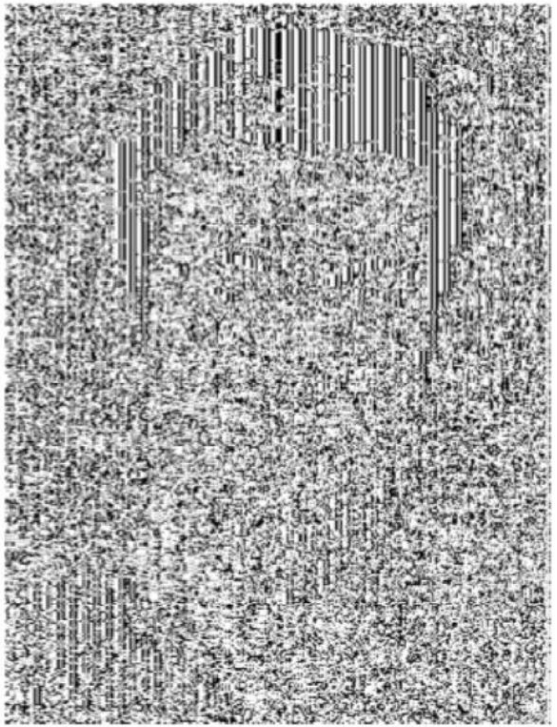


ECB-encrypted

with a

large AES-key

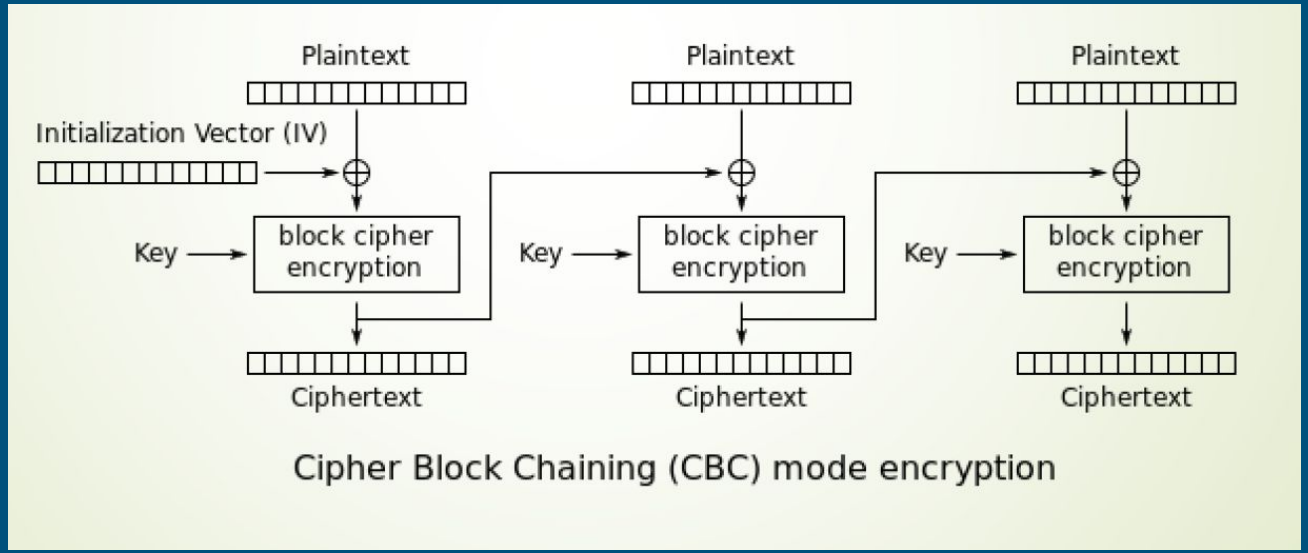
→



[Source: Bart Preneel]

CBC

- c_{-1} = IV
- c_i = Enc(sk, $c_{i-1} \oplus m_i$)
- c_0 = Enc(sk, IV $\oplus$ m_0)
- m_i = Dec(sk, c_i) $\oplus$ c_{i-1}
- m_0 = Dec(sk, c_0) $\oplus$ IV



CBC IV attack

- $m_0 = Dec(sk, c_0) \oplus IV$

=> $m_0 \oplus IV = Dec(sk, c_0)$ --- (1)

- $m_0' = Dec(sk, c_0') \oplus IV'$

=> $m_0' \oplus IV' = Dec(sk, c_0')$ --- (2)

- $c_0 = c_0'$

=> $Dec(sk, c_0) = Dec(sk, c_0')$

=> (1) = (2)

=> $m_0 \oplus IV = m_0' \oplus IV'$

=> $IV' = m_0' \oplus m_0 \oplus IV$

Example

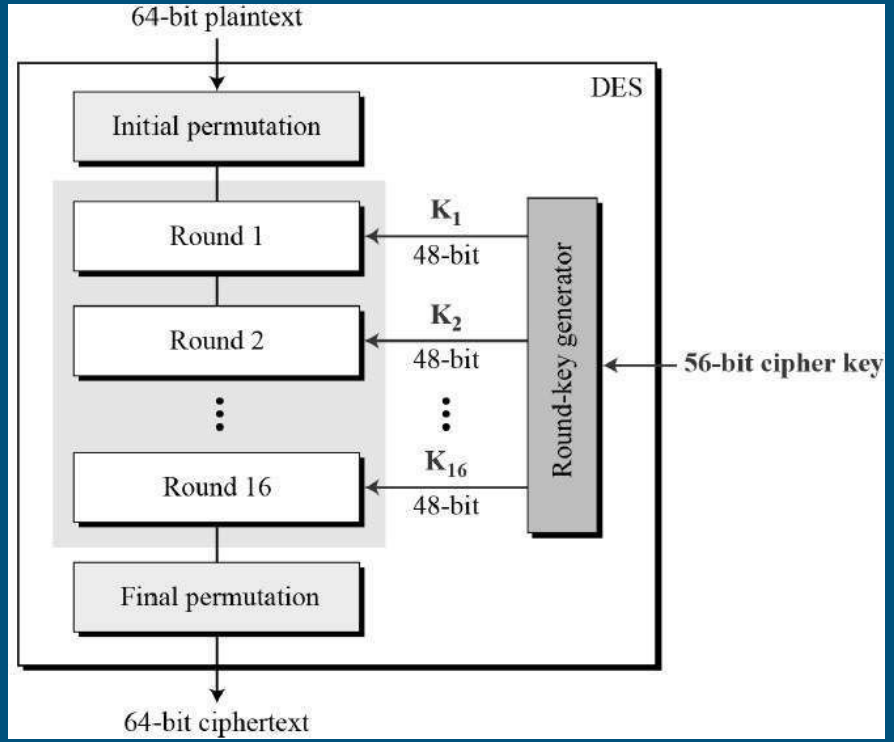
$IV' = m_0' \oplus m_0 \oplus IV$

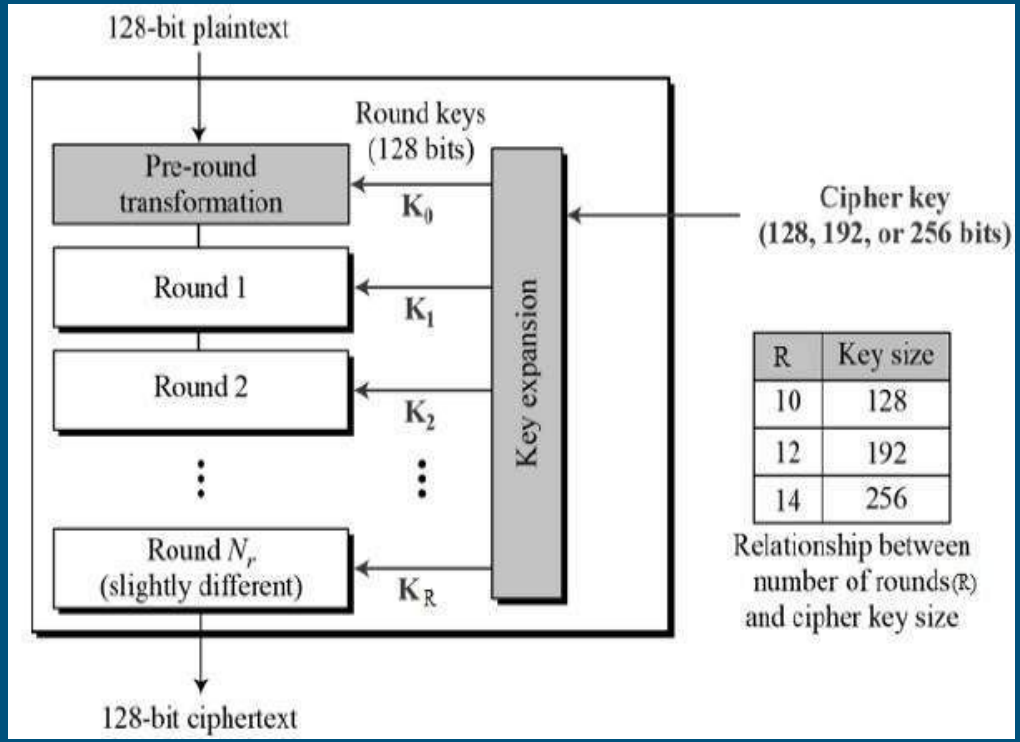
- Message: PwC HackaDay 2017 -> P3C H5ck5Day 2017
- Given IV = 5d965a85412589654754b78a98752147

- IV = 5d965a85412589654754b78a98752147
  m = 507743204861636b6144617920323031 37 (PwC HackaDay 2017)
  m' = 503343204835636b3544617920323031 37 (P3C H5ck5Day 2017)
  m_0 = 507743204861636b6144617920323031
  m_0' = 503343204835636b3544617920323031

- => IV' = 5dd25a85417189651354b78a98752147

DES -> AES



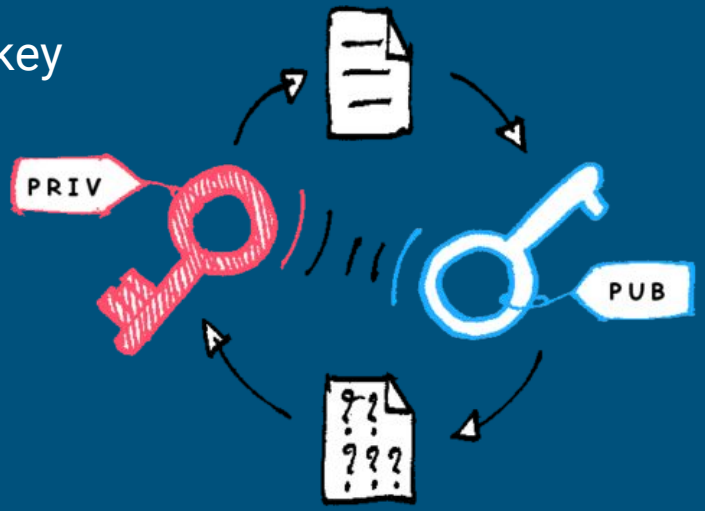


R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Public-key Cryptography (PKC)

- Asymmetric cryptography
- Encryptor and Decryptor using different key

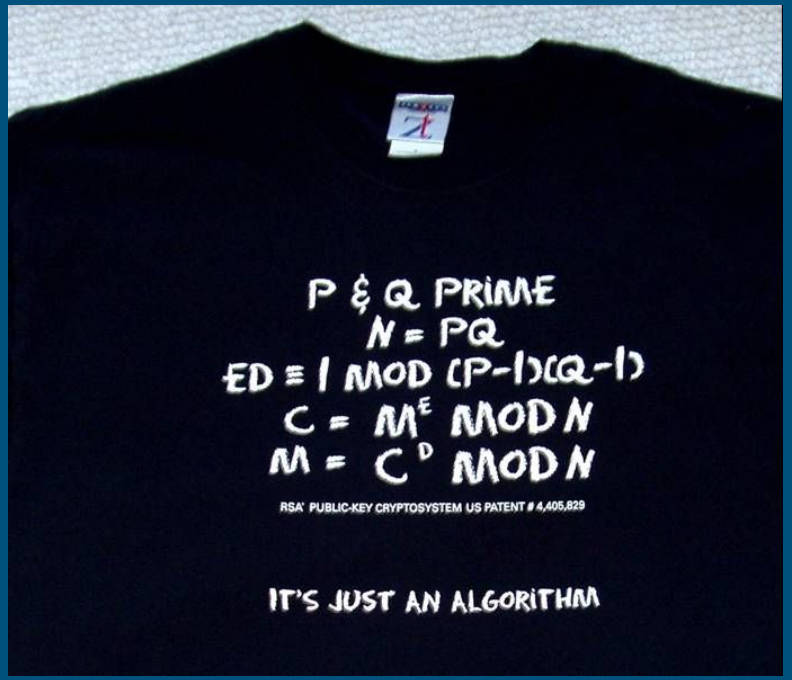


Public-key Cryptography (PKC)

- RSA (Rivest-Shamir-Adleman)
- Merkle-Hellman knapsack cryptosystem
- ElGamal encryption
- ...

RSA (Basic concept)

- Choose big primes P & Q, N= p*q
- Calculate $\varphi(N) = (p-1)(q-1) = r$
- Take a number e, which
  - $1 < e < r$
  - Gcd (e, r) = 1
- Calculate $ed = 1 \pmod{r}$
  - d = e^(-1) mod r



RSA (Basic concept)

- PUBLIC KEY : (n,e)
- PRIVATE KEY : (n,d)
- Let c be ciphertext, m be plaintext
    - c = m^(e) mod n
    - m = c^(d) mod n

RSA (simple practice)

Let’s generate our key!

Suppose p=97, q=103.

Then N = 9991 and $\varphi(n)$ = 9792.

E = 19, then d = 4123.

Public key: (9991, 19)
Private key: (9991, 4123)

RSA (simple practice)

Now let’s try to use the keys we generated.

Plaintext: HI (in ascii base 10 =7273)

Using RSA (Encryption): 7273^(19) = 676 (mod 9991)

Ciphertext: 676

Using RSA (Decryption): 676^(4123) = 7273 = HI

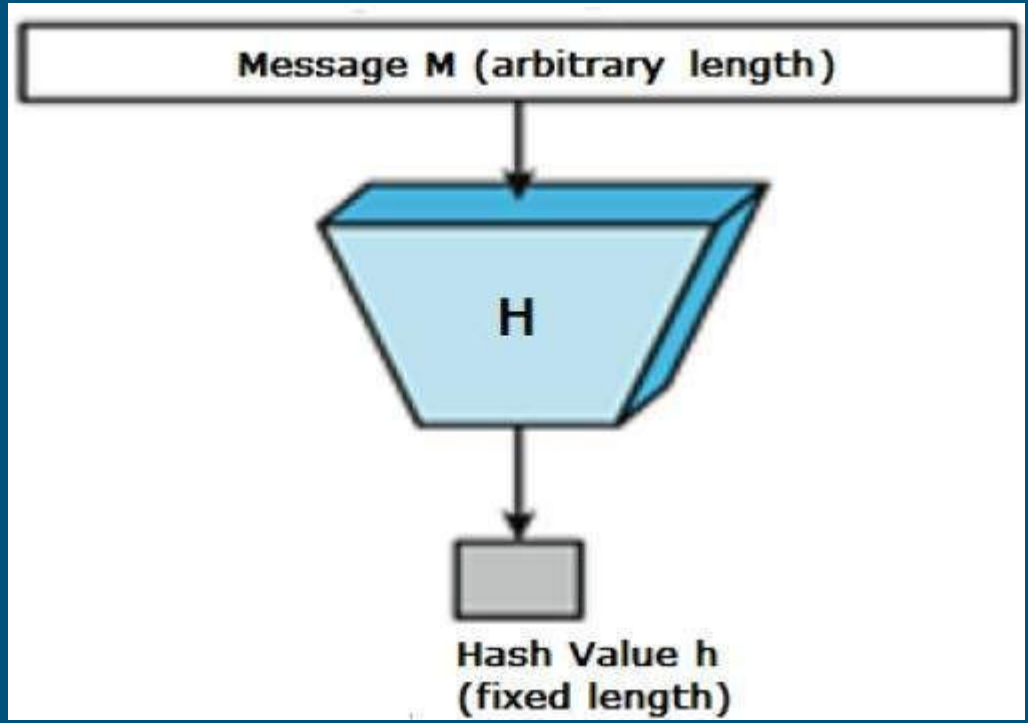
RSA (common weakness)

- N is not big enough -> p and q can be factorized
- P and Q are closed -> p and q can be factorized (Fermat’s Factorization)
- Encrypt the message with same n in different encryption
  - -> m can be obtained through calculation
- Wiener’s attack
- Coppersmith attack
- And more….

Simple Demo from jarvisoj

Hash function

- MD5
- SHA1, 2, 256, ...



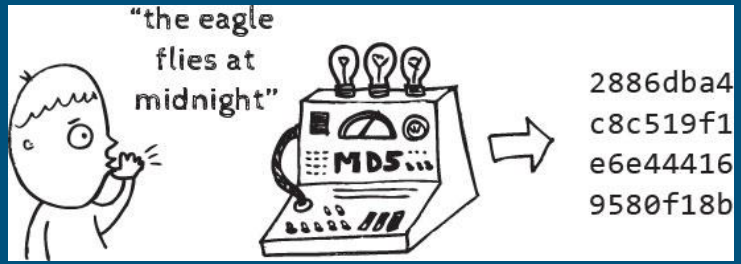
Hash function (Basic concept)

- Function used to map data. => Create a little ID to represent a piece of data
- Irreversible, One-way
- Uniqueness
- Calculated from every bit of the file => Tells completeness of a file

Hash function (Basic concept)

A Good Hash function should be:

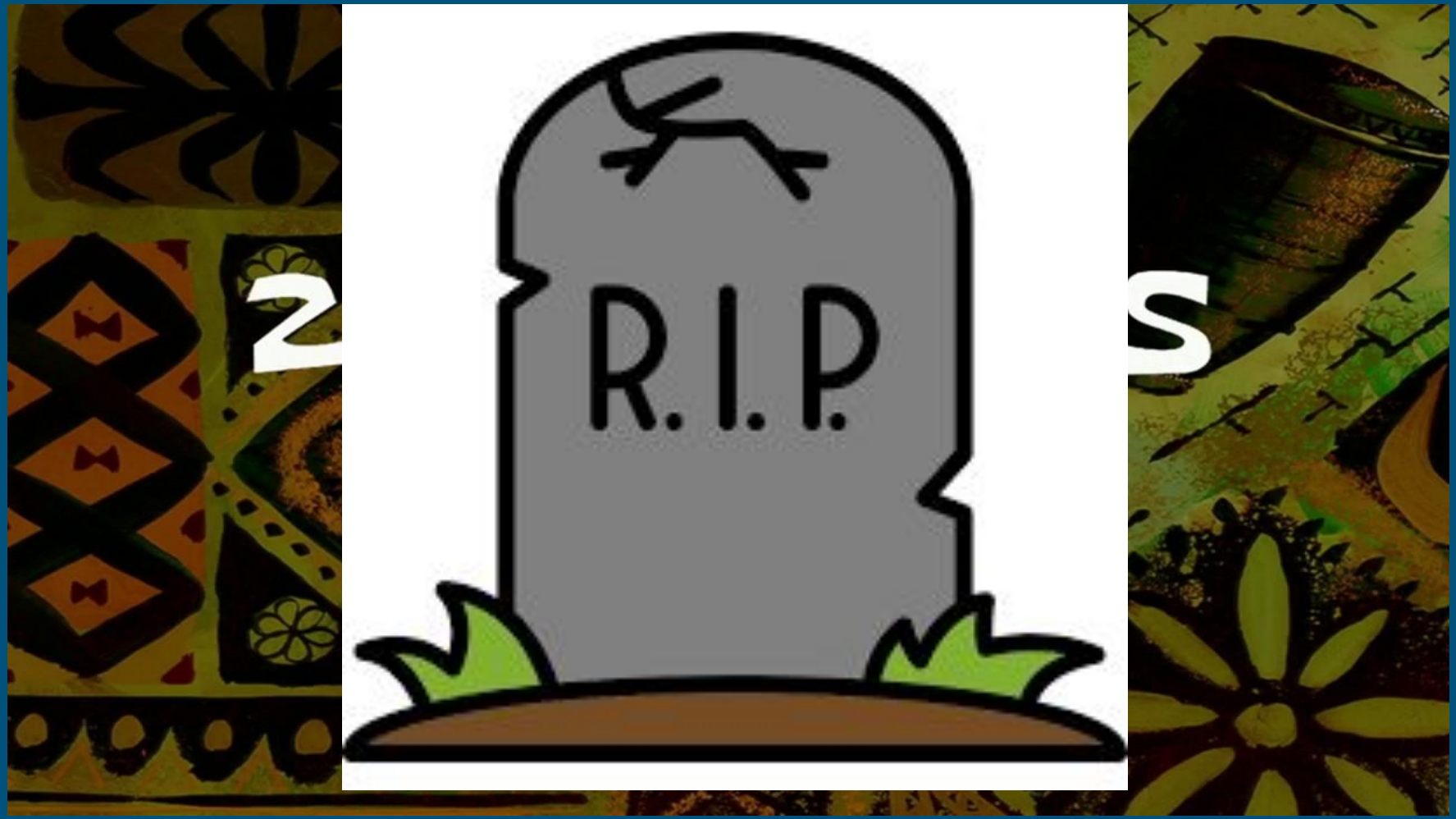
- Hash value can be calculated in limited time and resources (Quick)
- Hard, basically impossible to reverse the function
- Great change in hash value upon a little change in message
- Collision resistance
    - Hard to find two plaintext giving same hash value



Hash function (basic concept)

Collision:

- Two plaintext result in same hash value.
- Bits of output in hash functions are finite, while input of hash functions are infinite.
- So why we still use it?


R.I.P.

MD5 collision

But… I have heard of MD5 collision?

- It is still hard to reverse. (Nonlinear function)
- Due to cannot give great change in little changes.
- More commonly is done by dictionaries.

Q&A