Crypto for Bounty Hunters(bug bounty village)

BY

SHRUTIRUPA BANERJIEE

Whoami?

WAF Research @Qualys

InfosecGirls Pune Chapter Lead

WomenWhoCode Pune Lead

Blockchain and Security Enthusiast

Speaker @OwaspSeasides, @Rootconf, @Bsides Singapore and various meetups (infosecgirls, cyberfrat, null)

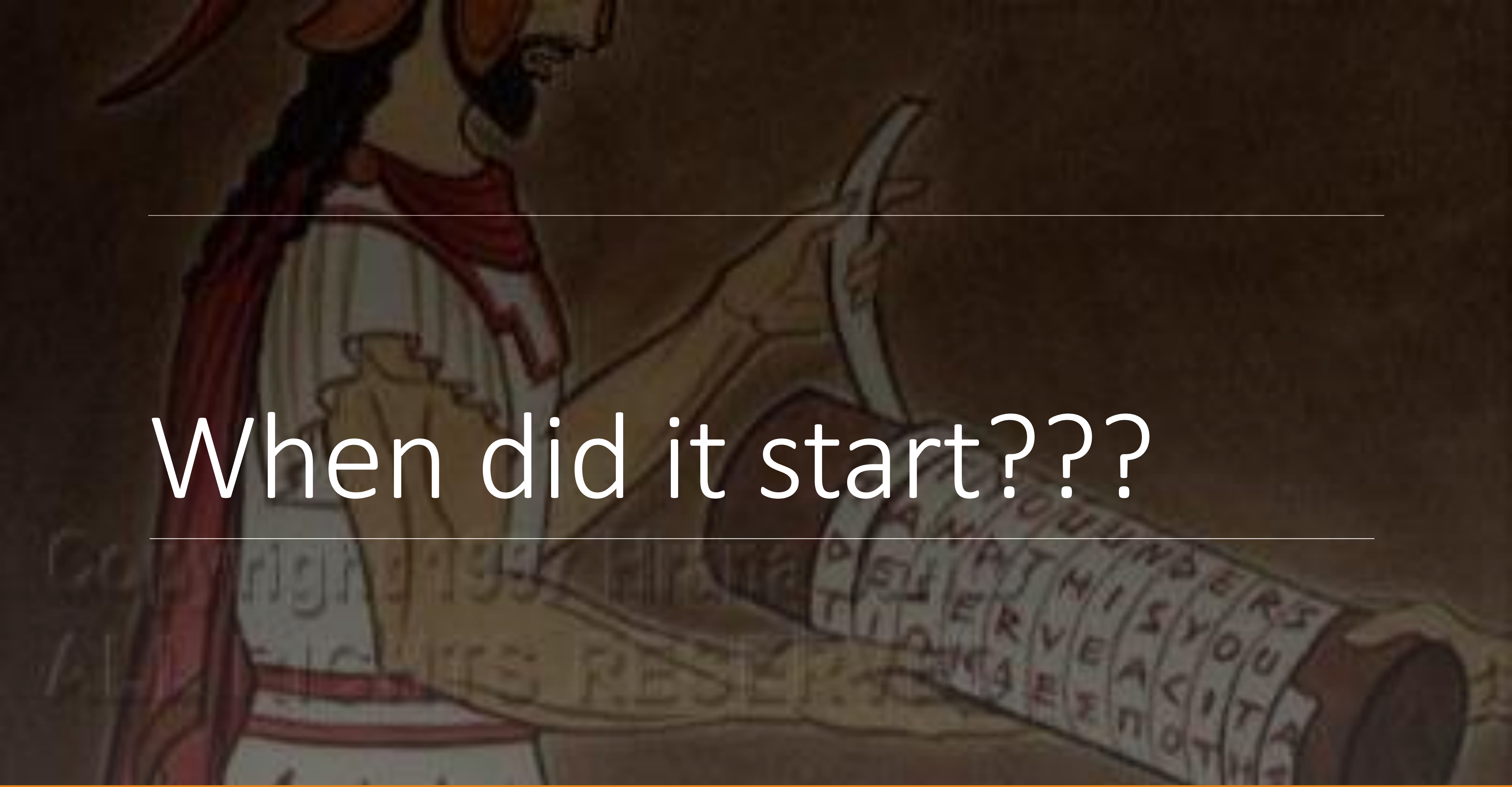
Independent Researcher

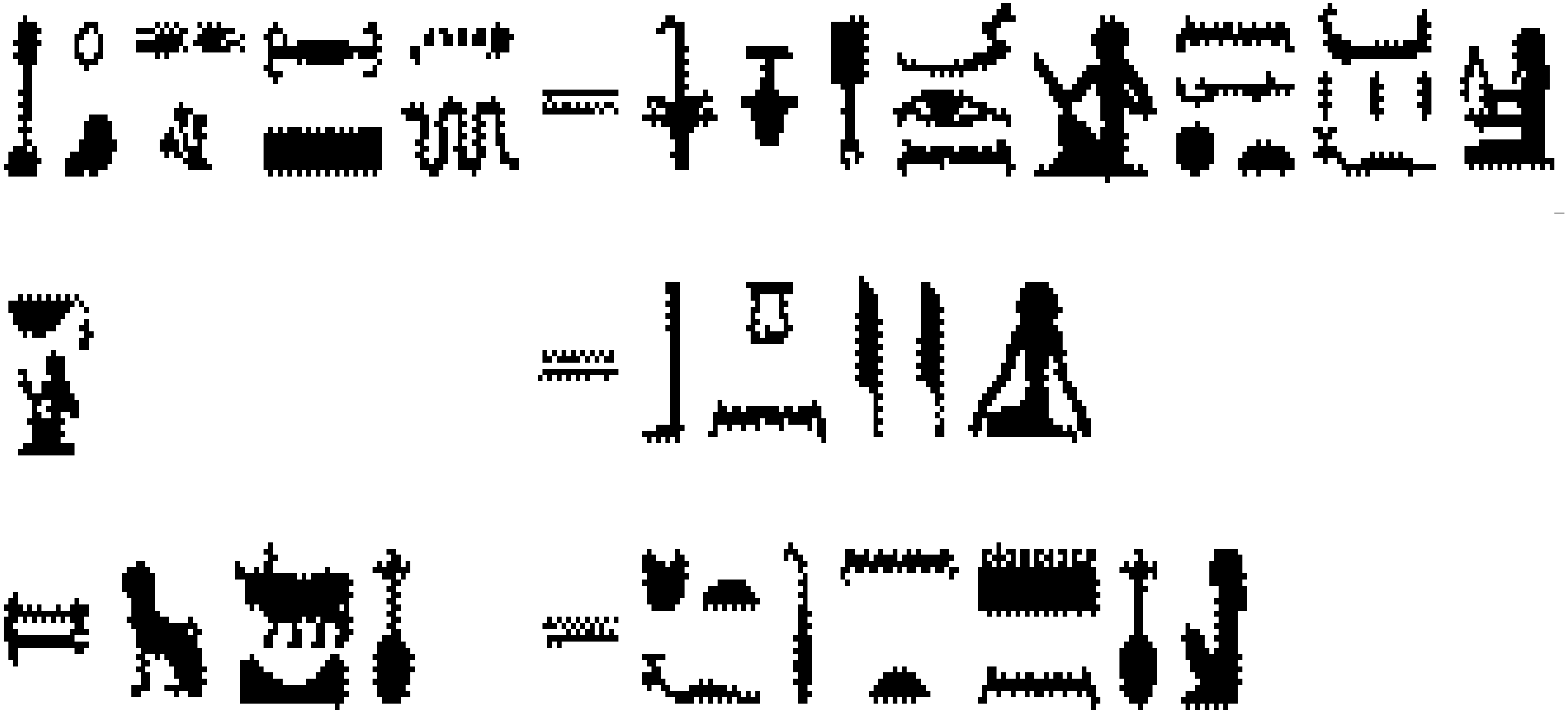
Note: A maths lover (so do not judge me)

Agenda

- History – CIA Triad
- Why are we talking about it
- Where does it come into picture
- Some classic cryptography examples
- Actual Crypto hacking
- Some examples and their reports

When did it start???

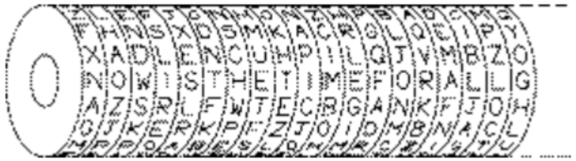




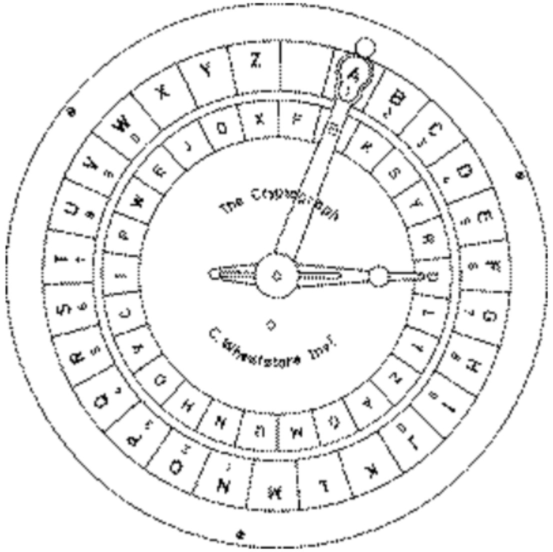
Hieroglyphic encipherments of proper names and titles, with cipher hieroglyphs at left, plain equivalents at right

Machine Ciphers

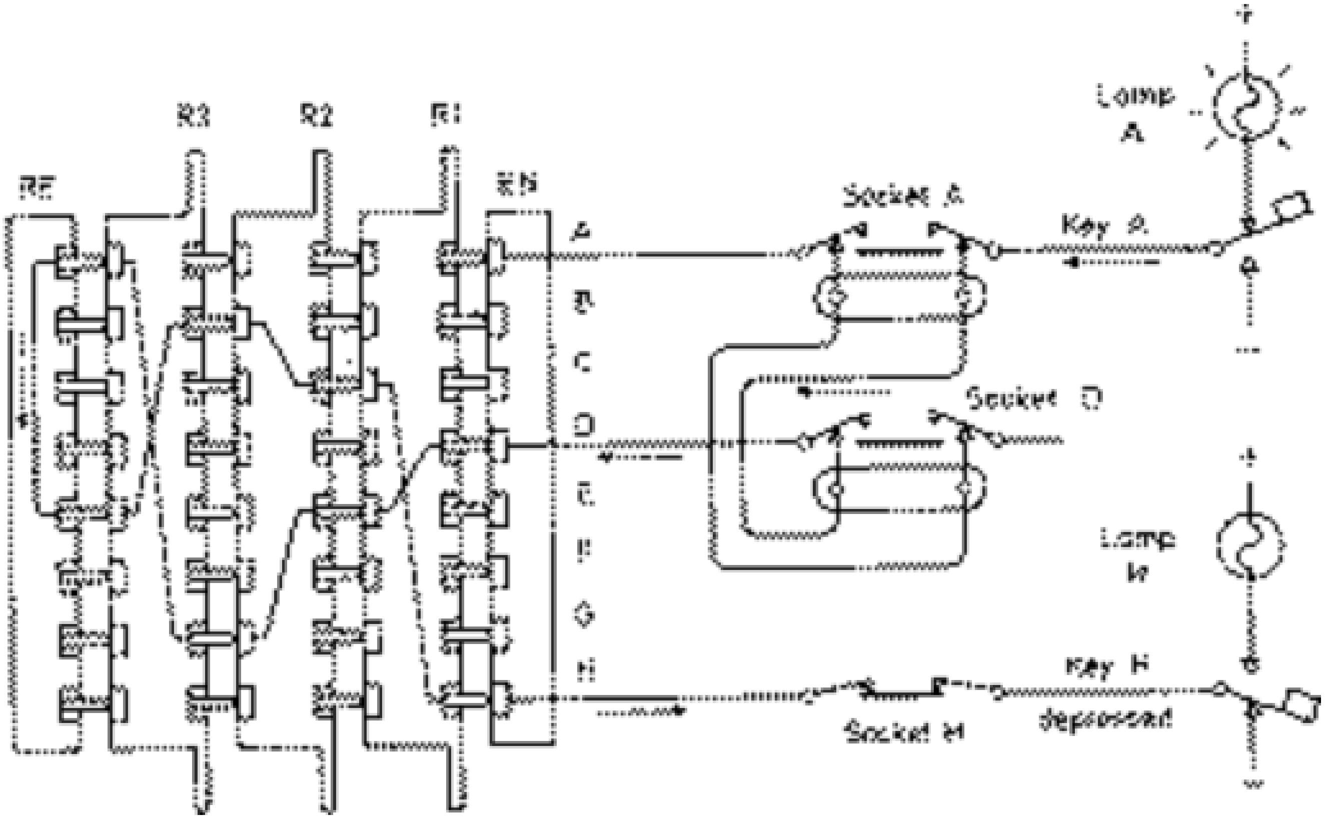
- **Jefferson cylinder**, developed in 1790s, comprised 36 disks, each with a random alphabet, order of disks was key, message was set, then another row became cipher



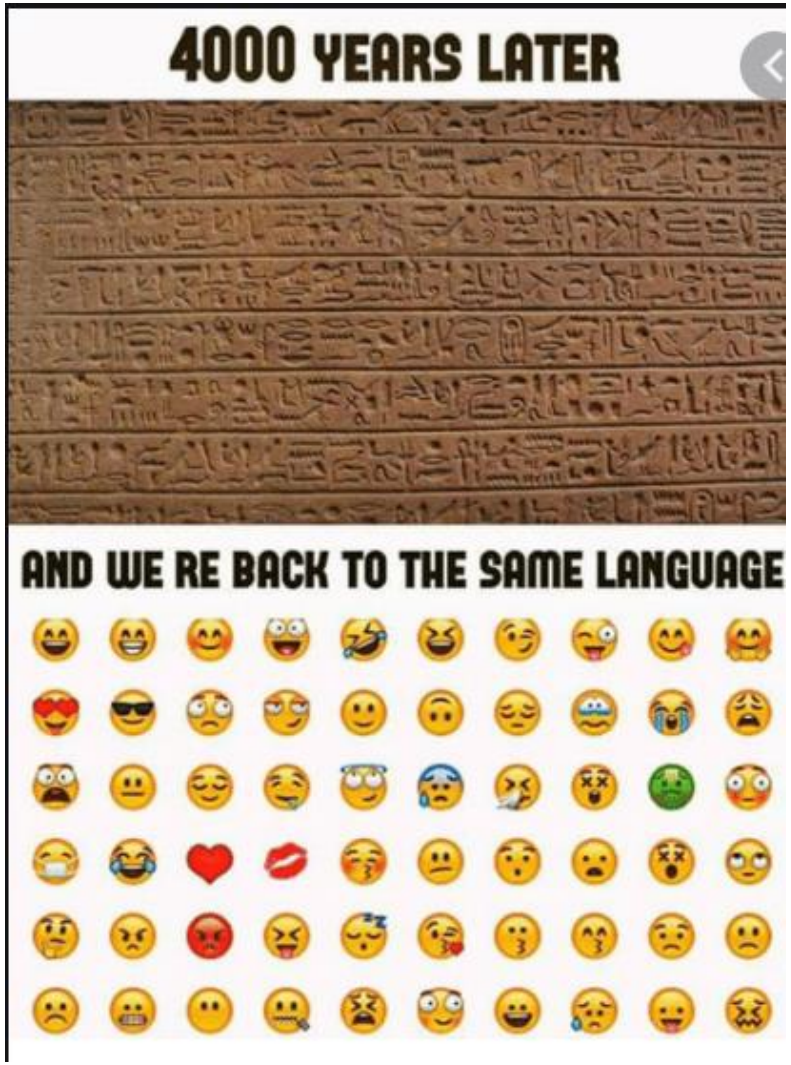
- **Wheatstone disc**, originally invented by Wadsworth in 1817, but developed by Wheatstone in 1860's, comprised two concentric wheels used to generate a polyalphabetic cipher



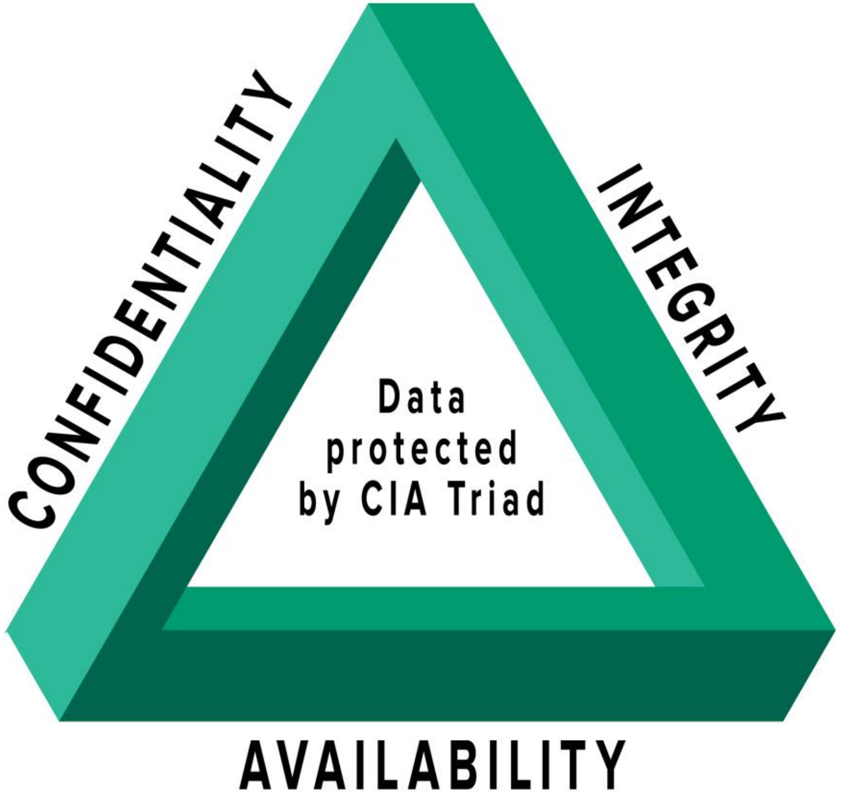
- **Enigma Rotor machine**, one of a very important class of cipher machines, heavily us
  providing a substitution using a continuosly changing alphabet



Basically…


4000 YEARS LATER
AND WE RE BACK TO THE SAME LANGUAGE

Why Are We Talking About This?
eyereturn

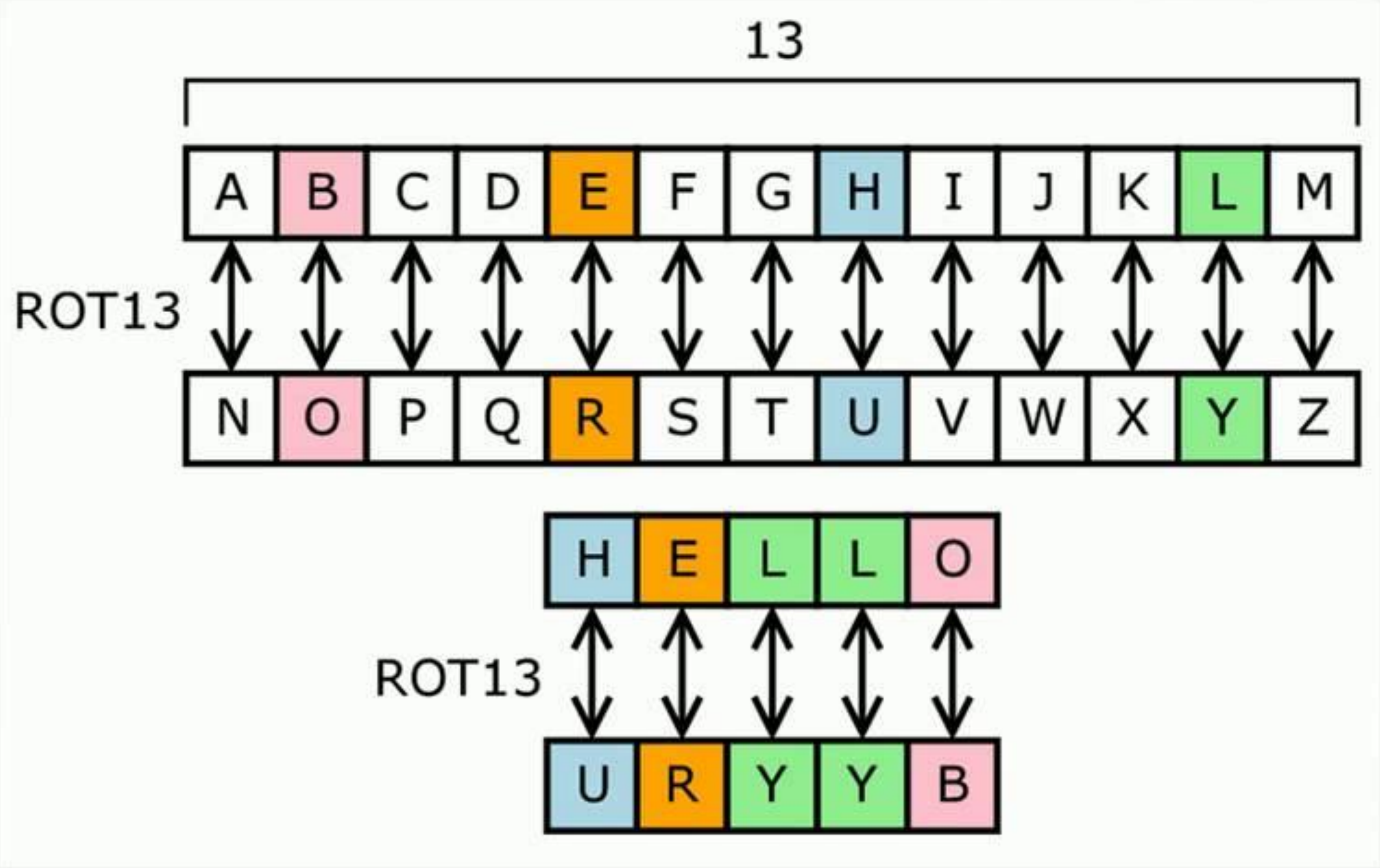

CONFIDENTIALITY
INTEGRITY
AVAILABILITY
Data protected by CIA Triad

Let’s look into some classic cryptography techniques???

Classical Cryptographic Techniques

- have two basic components of classical ciphers: **substitution** and **transposition**
- in substitution ciphers letters are replaced by other letters
- in transposition ciphers the letters are arranged in a different order
- these ciphers may be:
- **monoalphabetic** - only one substitution/ transposition is used, or
- **polyalphabetic -** where several substitutions/ transpositions are used
- several such ciphers may be concatentated together to form a **product cipher**

Substitution cipher



13

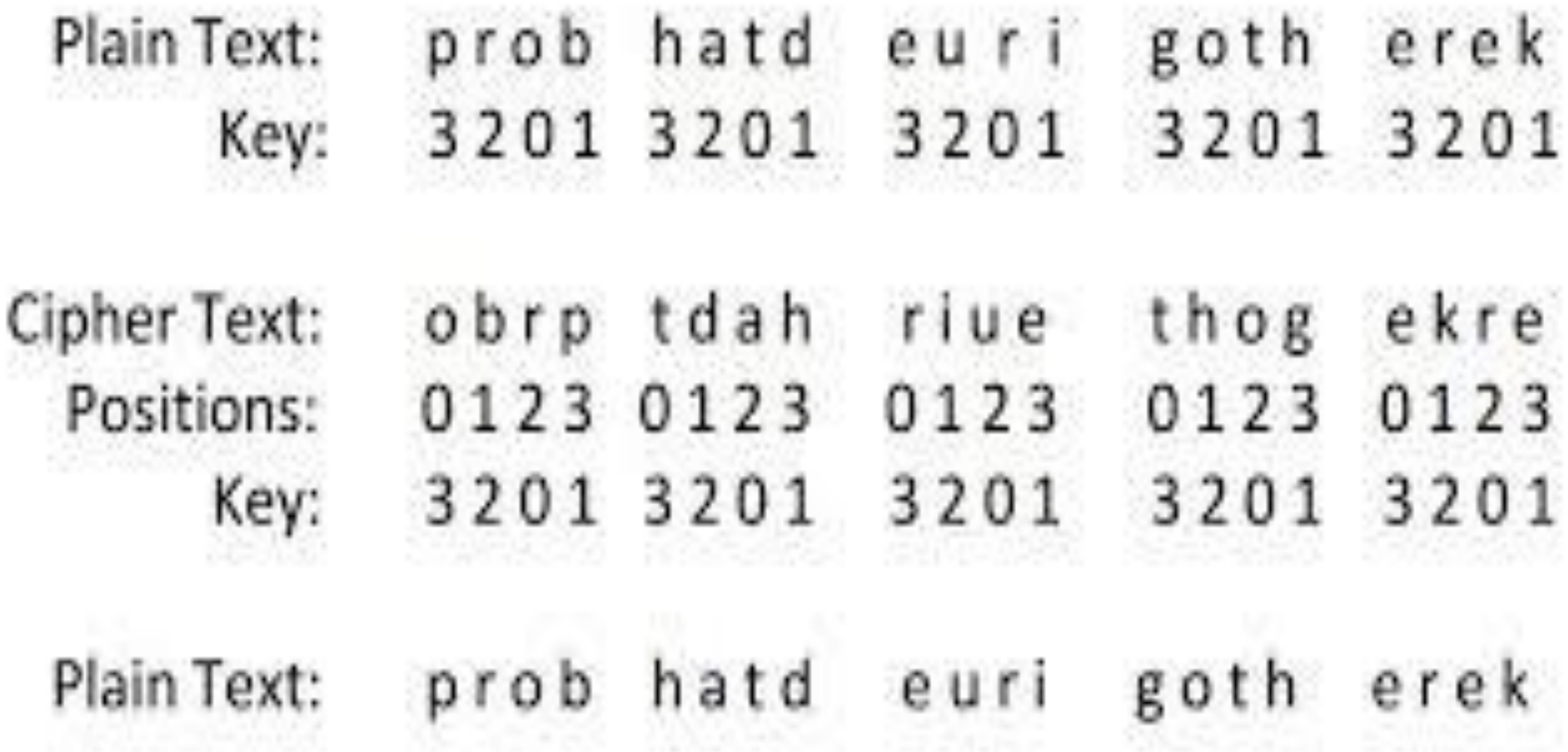
A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

ROT13

H	E	L	L	O
U	R	Y	Y	B

ROT13

https://en.wikipedia.org/wiki/File:ROT13.png



Plain Text:	prob	hatd	euri	goth	erek
Key:	3201	3201	3201	3201	3201
Cipher Text:	obrp	tdah	riue	thog	ekre
Positions:	0123	0123	0123	0123	0123
Key:	3201	3201	3201	3201	3201
Plain Text:	prob	hatd	euri	goth	erek

Monoalphabetic substitution

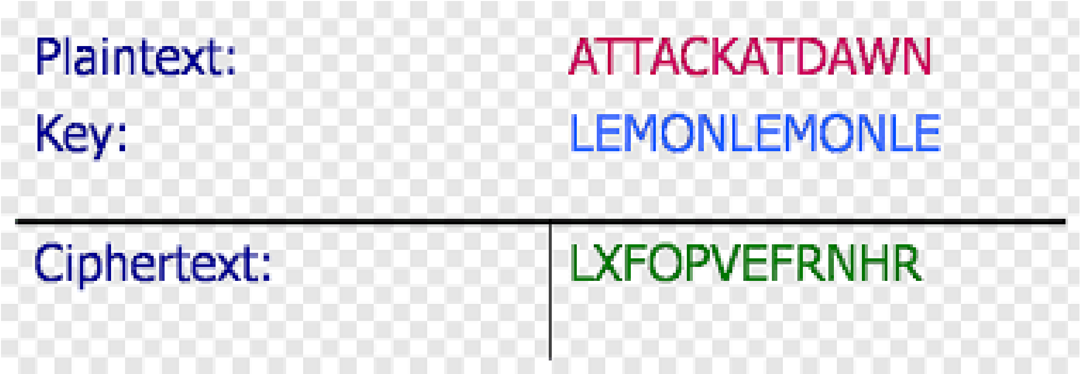
enciphering

open alphabet

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

cipher alphabet

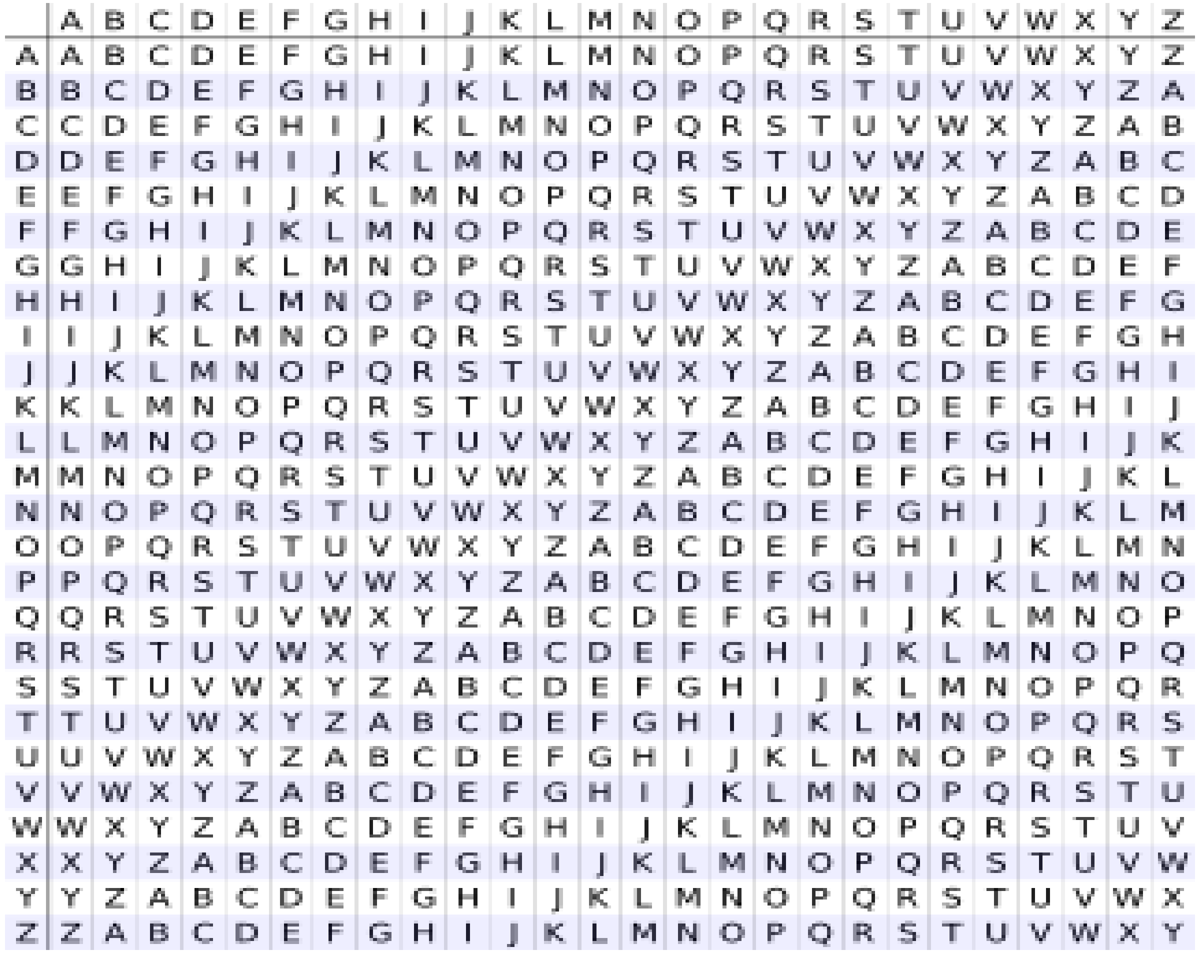
keyword:	KEYWORD
plain text:	ALKINDI
ciphertext:	K



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

Polyalphabetic Substitution

But before that…

Are you aware of these terminologies???

Encoding

Encryption

Hashing

PKI

Digital Signature

And many more…

For classic cryptography based attacks:

https://platform.avatao.com/paths/4b027084-49cd-4c82-9a75-24bb9eb8f861/info

Let’s talk real

How do you look for the crypto flaw in web applications?

AUTHENTICATION AND AUTHORIZATION (JWT)

USE OF SECRET KEYS

IS CBC STILL USED?

CAN WE TAMPER ELECTRONIC CODE BOOK?

SOME APPLICATIONS STILL USE MD5 FOR HASHING

WEAK SSL

ORACLE PADDING

DO WE STILL HAVE HEARTBLEED? AND HOW DO WE EXPLOIT IT?

Note: It’s basically the flaw in the implementation of the code, done by the humans.

Lets try some of them out ☺

What is JWT

- Json Web Token
- Used for authentication
- ✓ Contains signed data structure

How does it look like?

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ
zdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4
gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJ
SMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

What can we do about it???

Sensitive information?

Changing the algorithm and signing with our own key

Changing algorithm to none

Heartbleed

Poodle Attack

Padding oracle

One of the errors in padding while decrypting the sslv3.0 (need to check)

The adversary has a cipher text through interception and wants to decrypt it

It would take the cipher text as is and submit it to the server

The server would decrypt the cipher text and check if the pad has the correct format

If the pad is invalid, we will get a pad error or if the mac is invalid, we will get a mac error

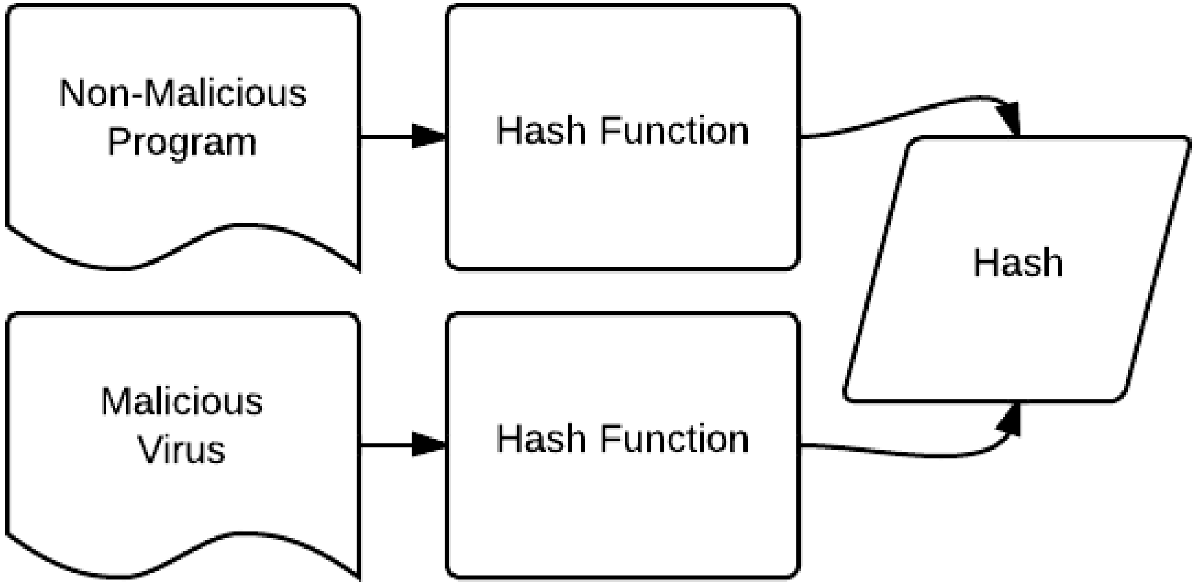
On the basis of that, the adversary will understand if there is a padding issue or mac issue

Older tls versions used to leak the type of error, and this resulted into manipulation of the cipher text by the attackers

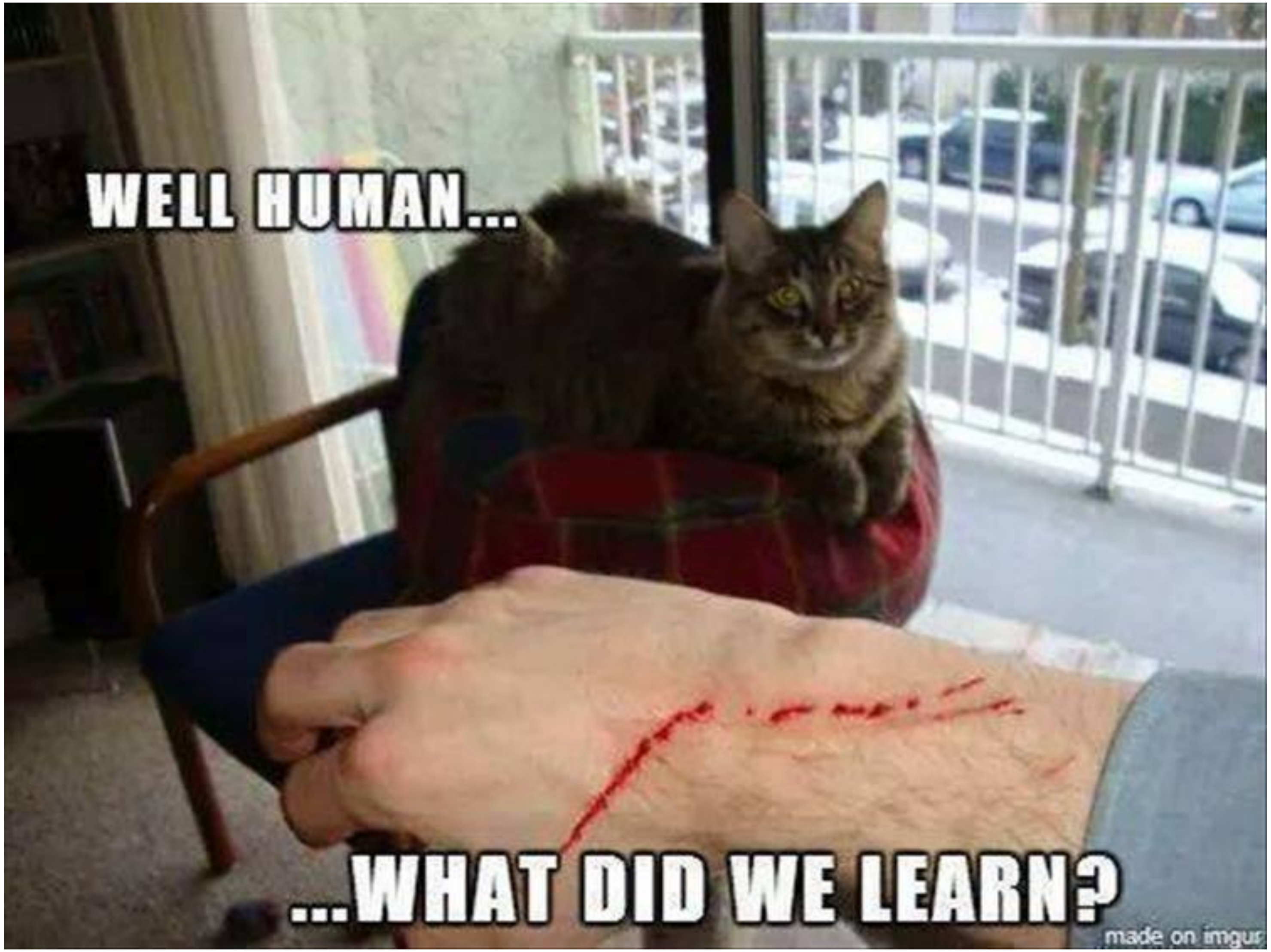
Padding attack also happened due to timing attacks when they had stopped showing the error messages, so when the pad is invalid, the error msg is sent out quickly and if the mac is invalid, it takes some time.

Use of weak secret key

Do we need to talk about cbc and ecb???



Lets talk about md5!!!


WELL HUMAN...
...WHAT DID WE LEARN?
made on imgur

https://medium.com/bugbountywriteup/idor-in-jwt-and-the-shortest-token-you-will-ever-see-uid-1234567890-4e02377ea03a

https://www.hackerone.com/zerodaily/2018-05-30

https://medium.com/101-writeups/hacking-json-web-token-jwt-233fe6c862e6

References

https://medium.com/@ranakhalil101/hack-the-box-brainfuck-writeup-w-o-metasploit-5075c0c55e93

https://blog.intothesymmetry.com/2020/01/the-curious-case-of-webcrypto-diffie.html

https://swcregistry.io/

https://attackdefense.com/freelabs

https://pentesterlab.com/exercises/padding_oracle/course

https://pentesterlab.com/exercises/ecb/course

https://sites.google.com/site/smxtilabz/products/lamma-watch

https://en.wikipedia.org/wiki/ROCA_vulnerability

https://blog.paradoxis.nl/defeating-flasks-session-management-65706ba9d3ce

https://heartbleed.com

https://www.valencynetworks.com/articles/cyber-attacks-cryptographic-attacks.html

Locate me

Twitter handle: @freak_crypt

Linkedin: shrutirupa-banerjiee

Thank You
THIS MUCH!