INTRODUCTION TO SOFTWARE DEVELOPMENT

Week 1 Day 3

Led by: Emily Crose

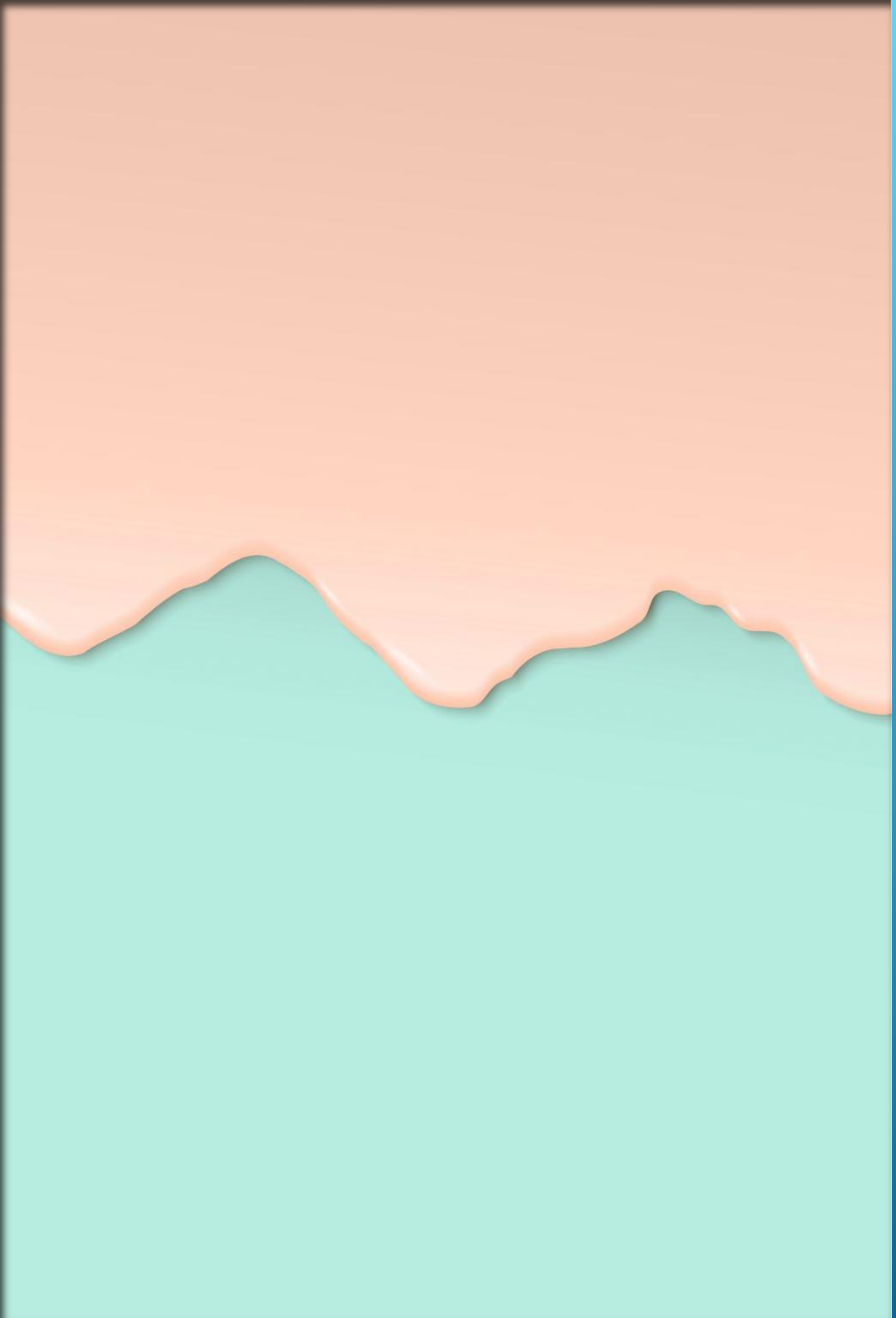
for

Oakland University

DAY 2 RECAP

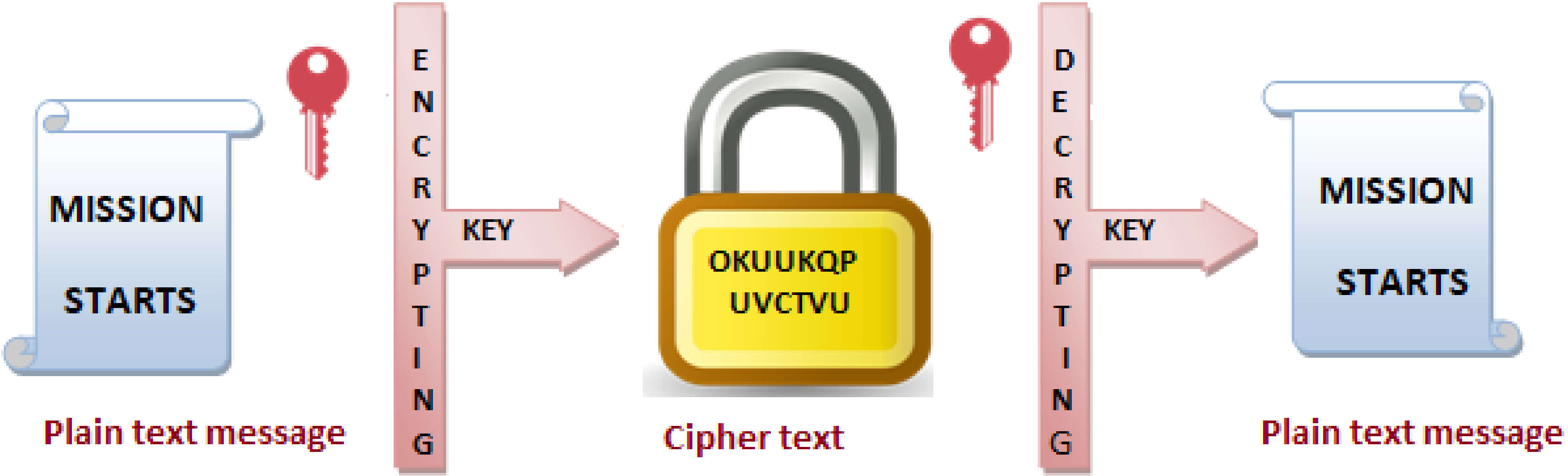
QUESTIONS FROM DAY 2?

SECURING & ENCRYPTING DATA



CLEARTEXT VS. CIPHERTEXT

Cryptography



MISSION STARTS

Plain text message

ENCRYPTING

KEY

OKUUKQP UVCTVU

Cipher text

DECRYPTING

KEY

MISSION STARTS

Plain text message

HASHING

VALUE OF HASHING

- LAYER OF VALIDATION OF DATA
- SECURES BOTH ENDS OF TRANSMISSION
- ANYONE CAN VALIDATE!
- PROTECTS ORIGINAL SECRET
- IRREVERSIBLE

POPULAR HASHING ALGORITHMS

- MD5
- SHA-1 (compromised)
- SHA-2
- SHA-3
- LM/NTLM hash (for Windows passwords)

LET'S TRY SOME HASH!

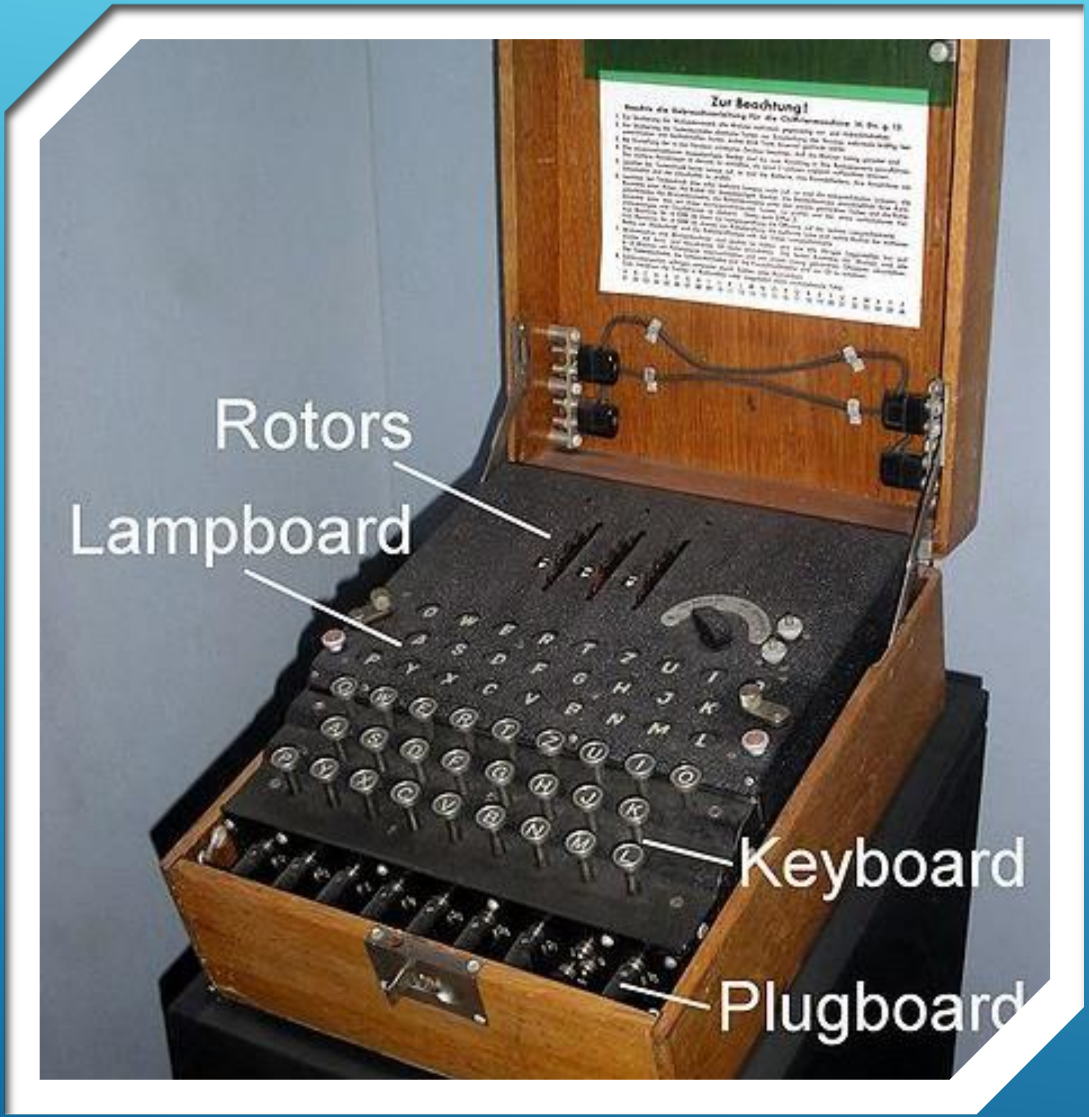
https://gchq.github.io/CyberChef/

WHAT IS ENCRYPTION?

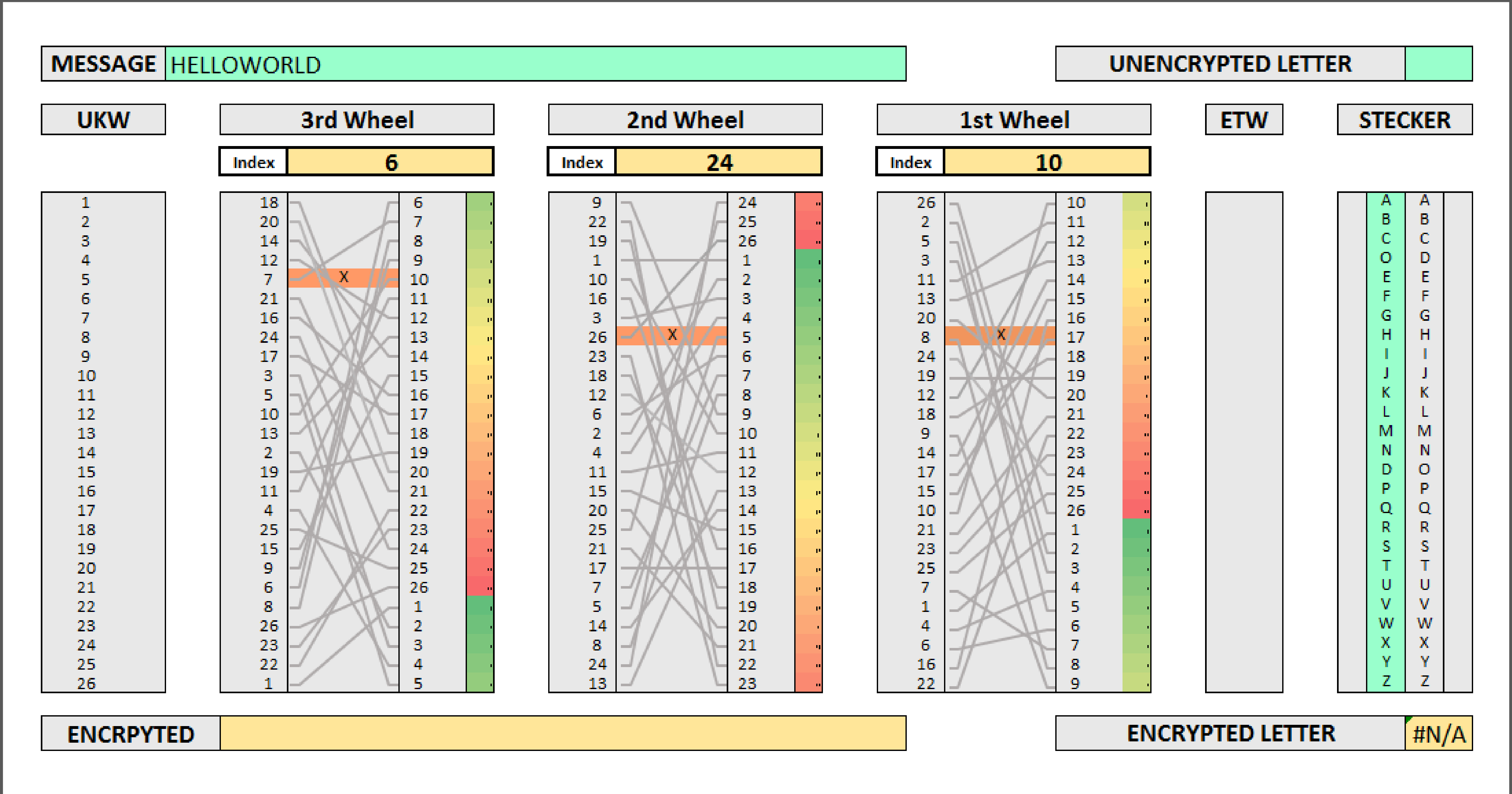
ENCRYPTION HISTORY

HAND CIPHERS

- Substitution (or “Caesar”) cipher – (850 CE)
- Code book cipher – (1500s)
- Vigenère cipher – (1553)
  - First to use an encryption key
- Jefferson cipher – (1795)
- Playfair cipher – (1854)



WARTIME CRYPTOGRAPHY



MESSAGE	HELLOWORLD

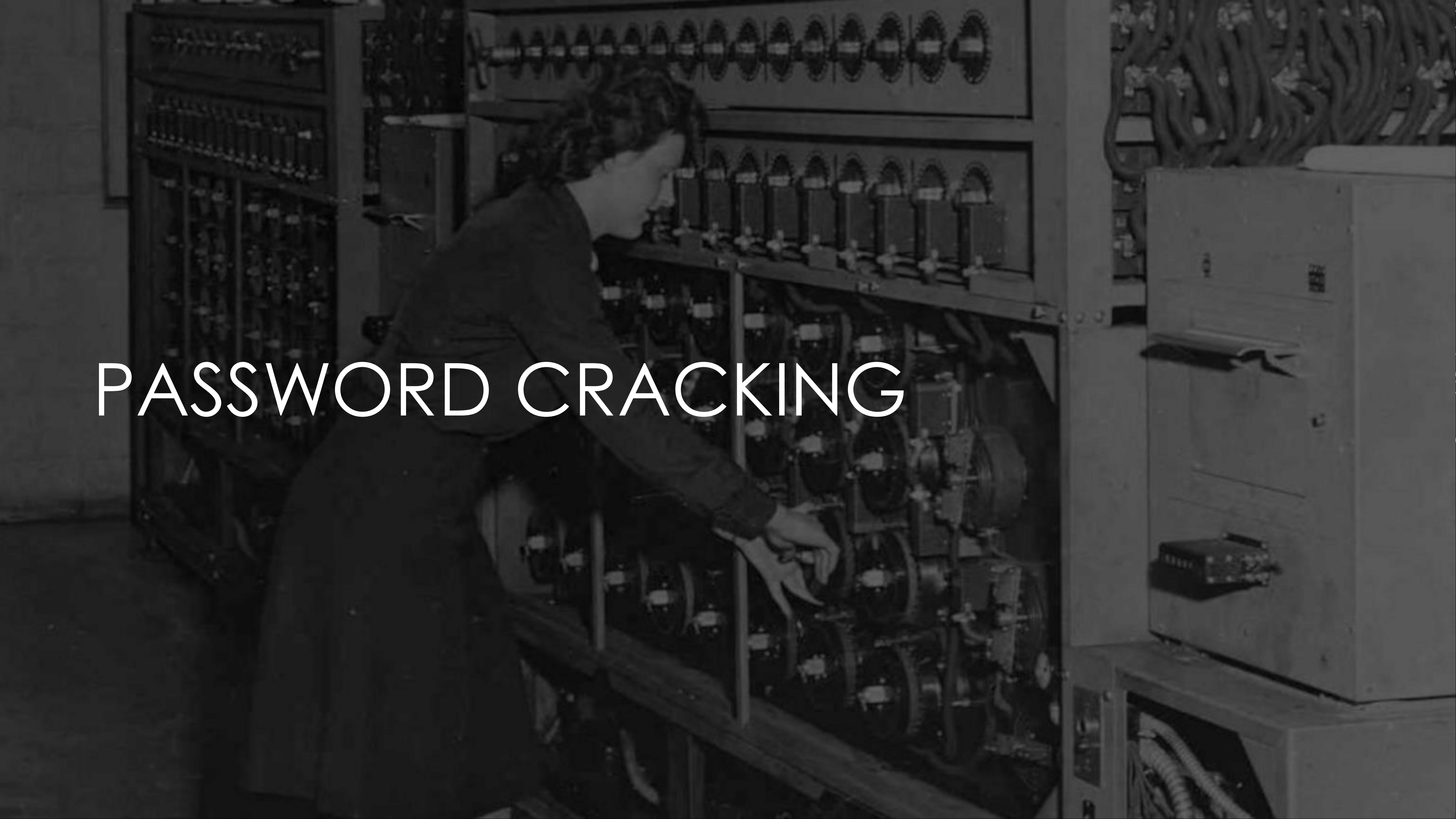
UNENCRYPTED LETTER	

UKW	3rd Wheel			2nd Wheel			1st Wheel			ETW	STECKER	
	Index	6		Index	24		Index	10				
1	18		6	9		24	26		10		A	A
2	20		7	22		25	2		11		B	B
3	14		8	19		26	5		12		C	C
4	12		9	1		1	3		13		O	D
5	7	X	10	10		2	11		14		E	E
6	21		11	16		3	13		15		F	F
7	16		12	3		4	20		16		G	G
8	24		13	26	X	5	8	X	17		H	H
9	17		14	23		6	24		18		I	I
10	3		15	18		7	19		19		J	J
11	5		16	12		8	12		20		K	K
12	10		17	6		9	18		21		L	L
13	13		18	2		10	9		22		M	M
14	2		19	4		11	14		23		N	N
15	19		20	11		12	17		24		D	O
16	11		21	15		13	15		25		P	P
17	4		22	20		14	10		26		Q	Q
18	25		23	25		15	21		1		R	R
19	15		24	21		16	23		2		S	S
20	9		25	17		17	25		3		T	T
21	6		26	7		18	7		4		U	U
22	8		1	5		19	1		5		V	V
23	26		2	14		20	4		6		W	W
24	23		3	8		21	6		7		X	X
25	22		4	24		22	16		8		Y	Y
26	1		5	13		23	22		9		Z	Z

ENCRPYTED	

ENCRYPTED LETTER	#N/A

10 MINUTE BREAK

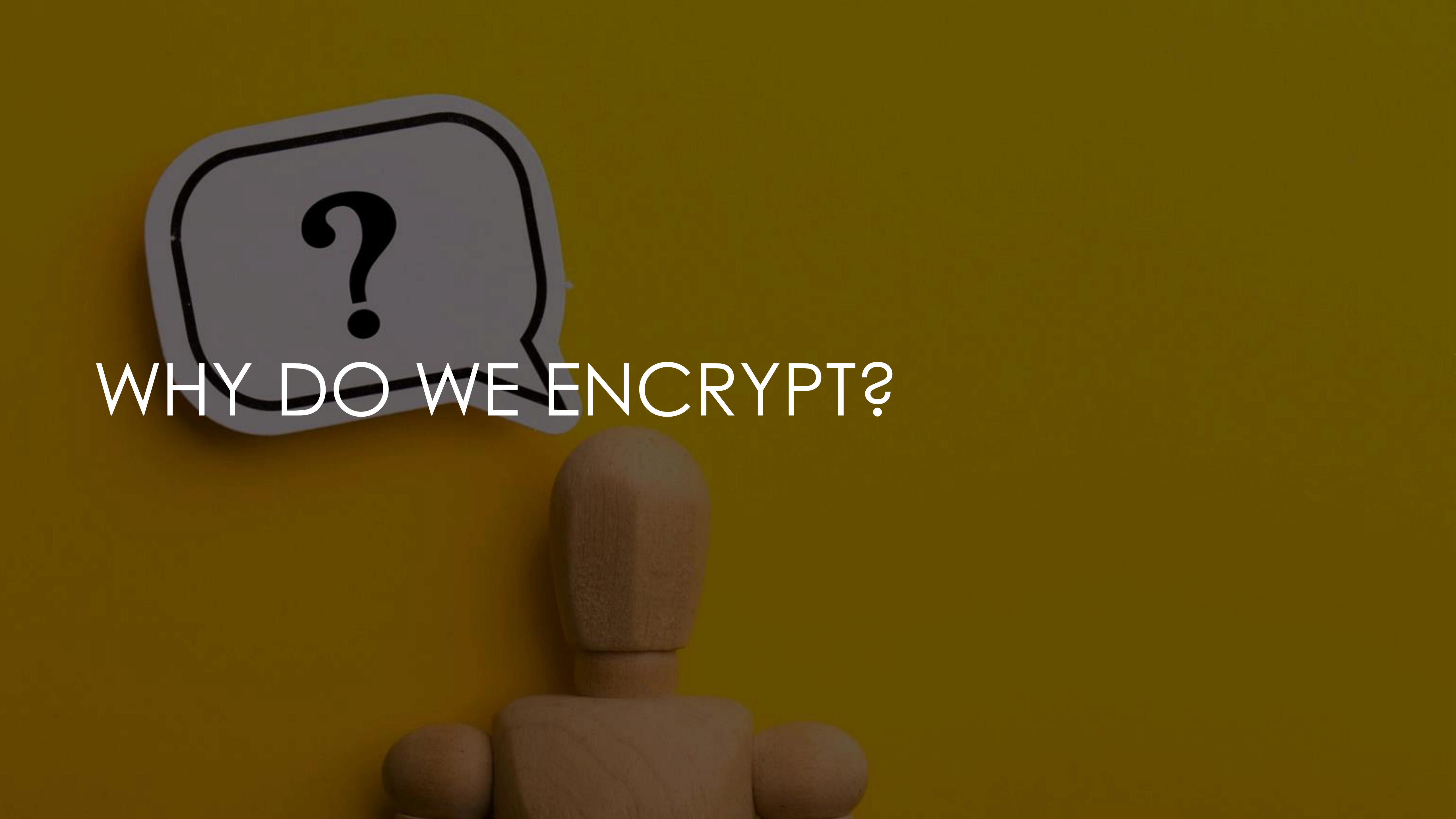


PASSWORD CRACKING

ONE-TIME PADS

Crypto Museum
cryptomuseum.com

VENONA PROJECT



WHY DO WE ENCRYPT?

WHAT DO WE ENCRYPT?

HOW DO WE ENCRYPT TODAY?

- Rivest-Shamir-Adleman (RSA) – (1977)
  - Based on prime number factorization
- Advanced Encryption Standard (AES) 256
  - Block cipher

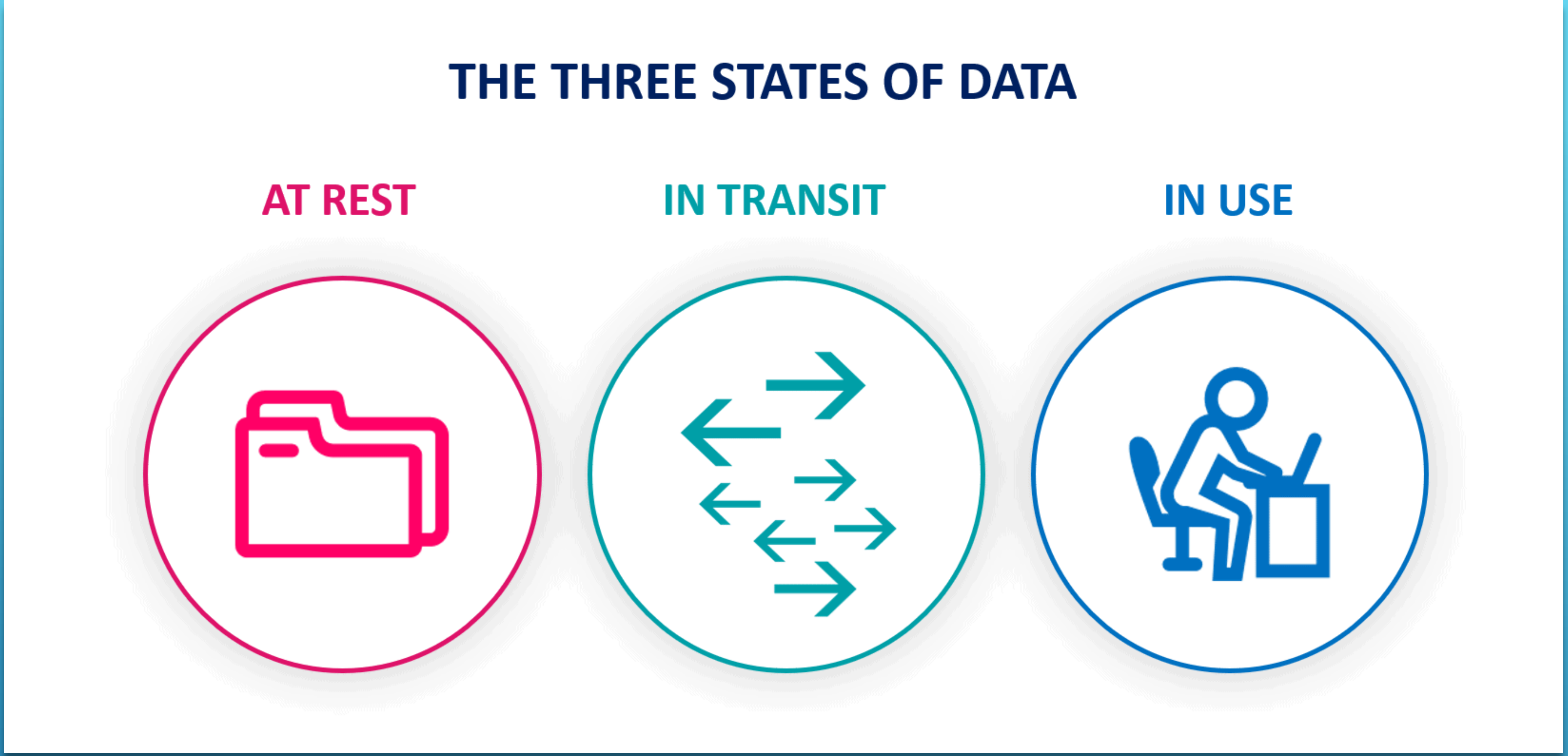
POPULAR MODERN CRYPTOGRAPHY ALGORITHMS

- AES
  - Supports key sizes of 128, 192, 256
- Key sizes improve the strength of cryptographic protection
- 2048 & 4096 key sizes
  - Large keys
  - Hard to brute force

KEYSPACE/KEYLENGTH/KEYSIZE

CRYPTOGRAPHIC STANDARDS

https://csrc.nist.gov/Projects/cryptographic-standards-and-guidelines



THE THREE STATES OF DATA

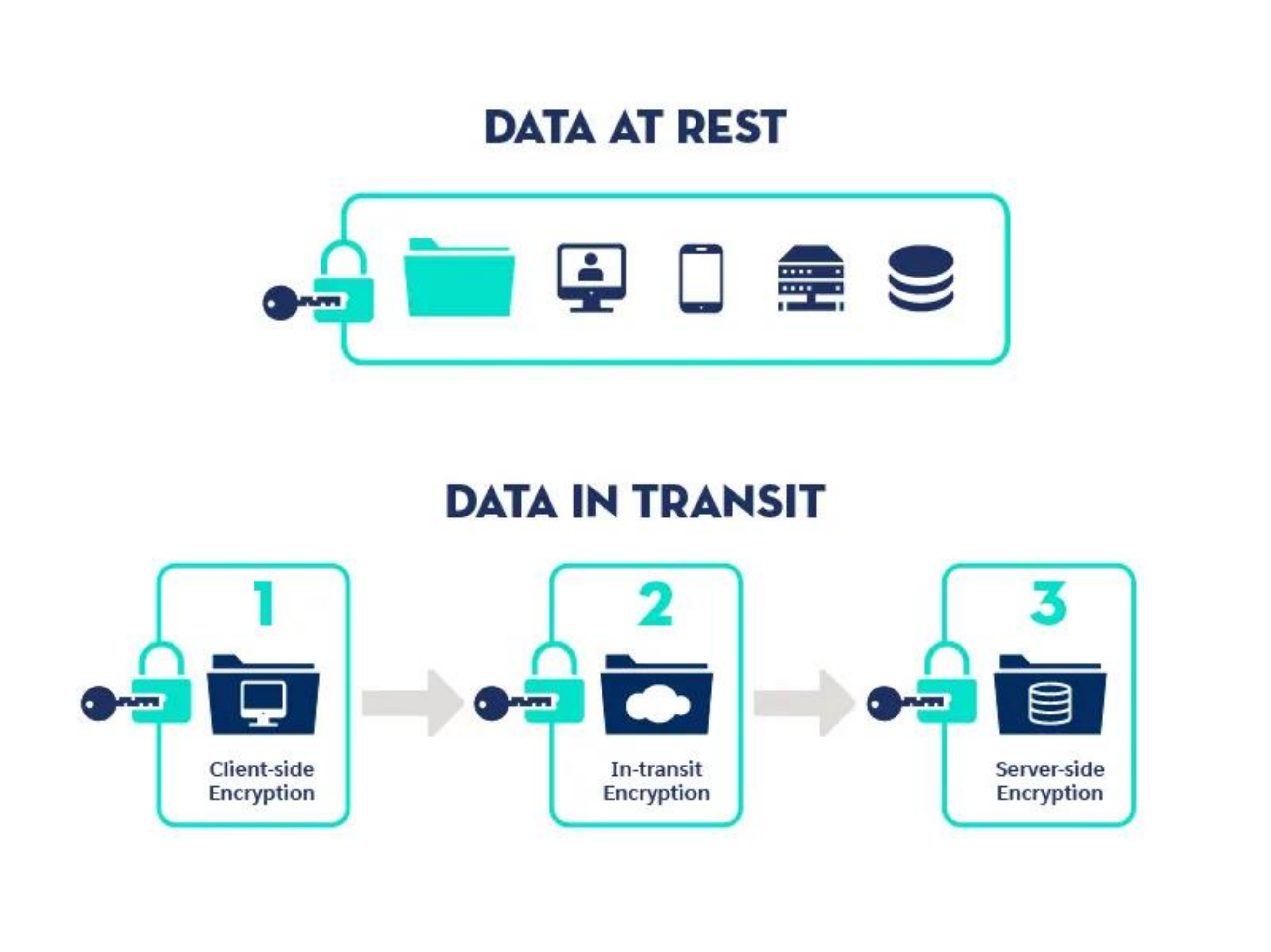
AT REST

IN TRANSIT

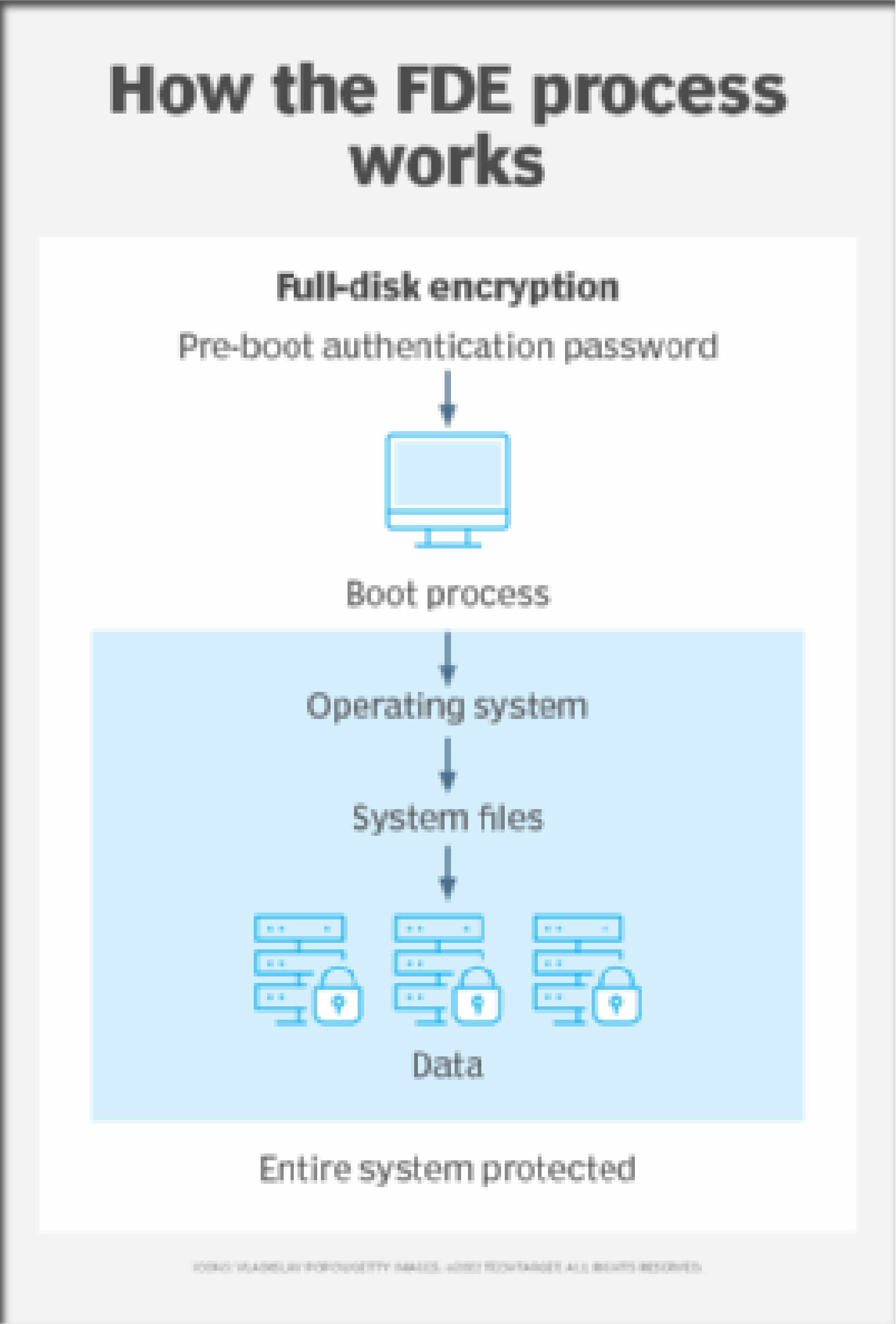
IN USE

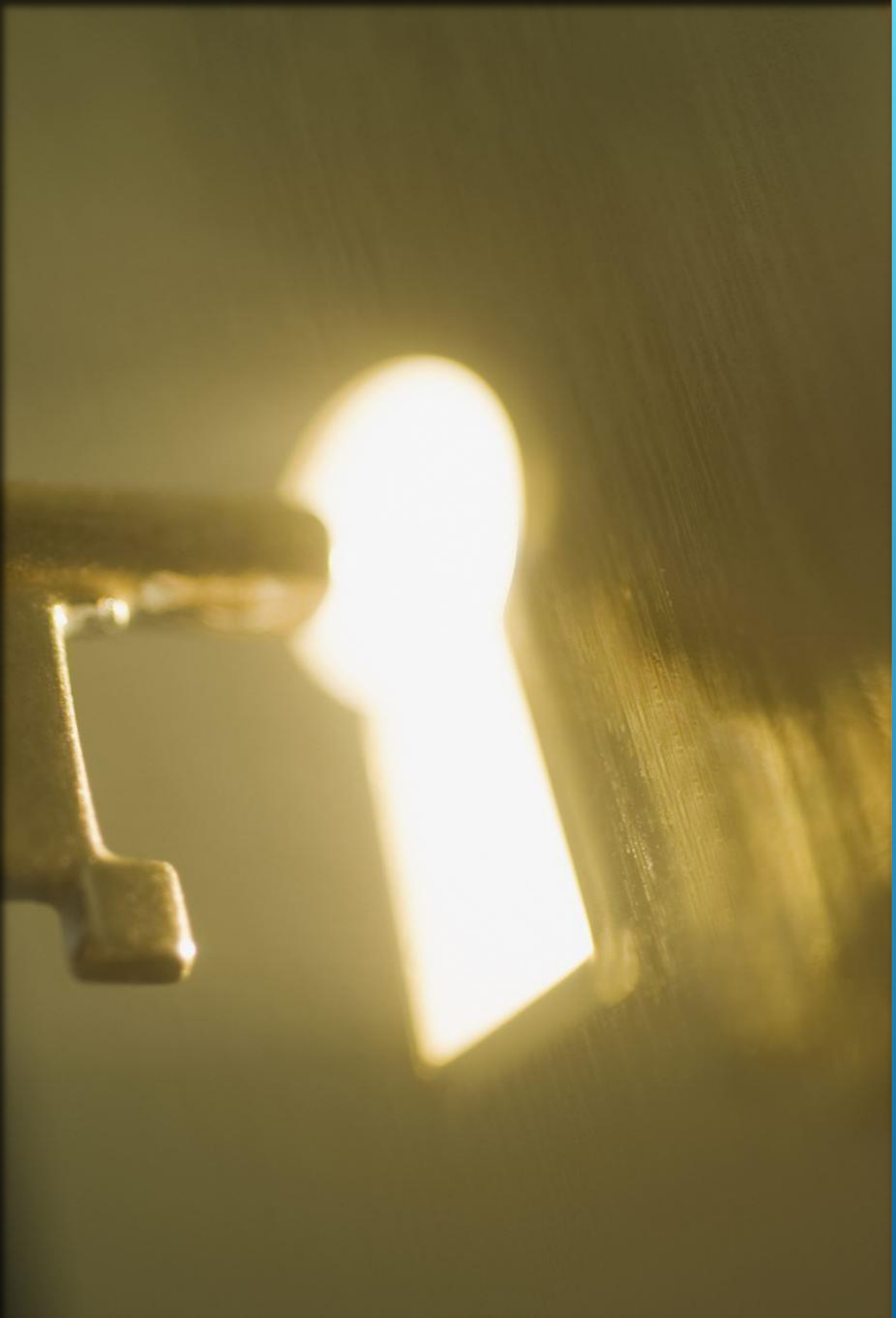
STATES OF DATA

DATA SECURITY



FULL DISK ENCRYPTION



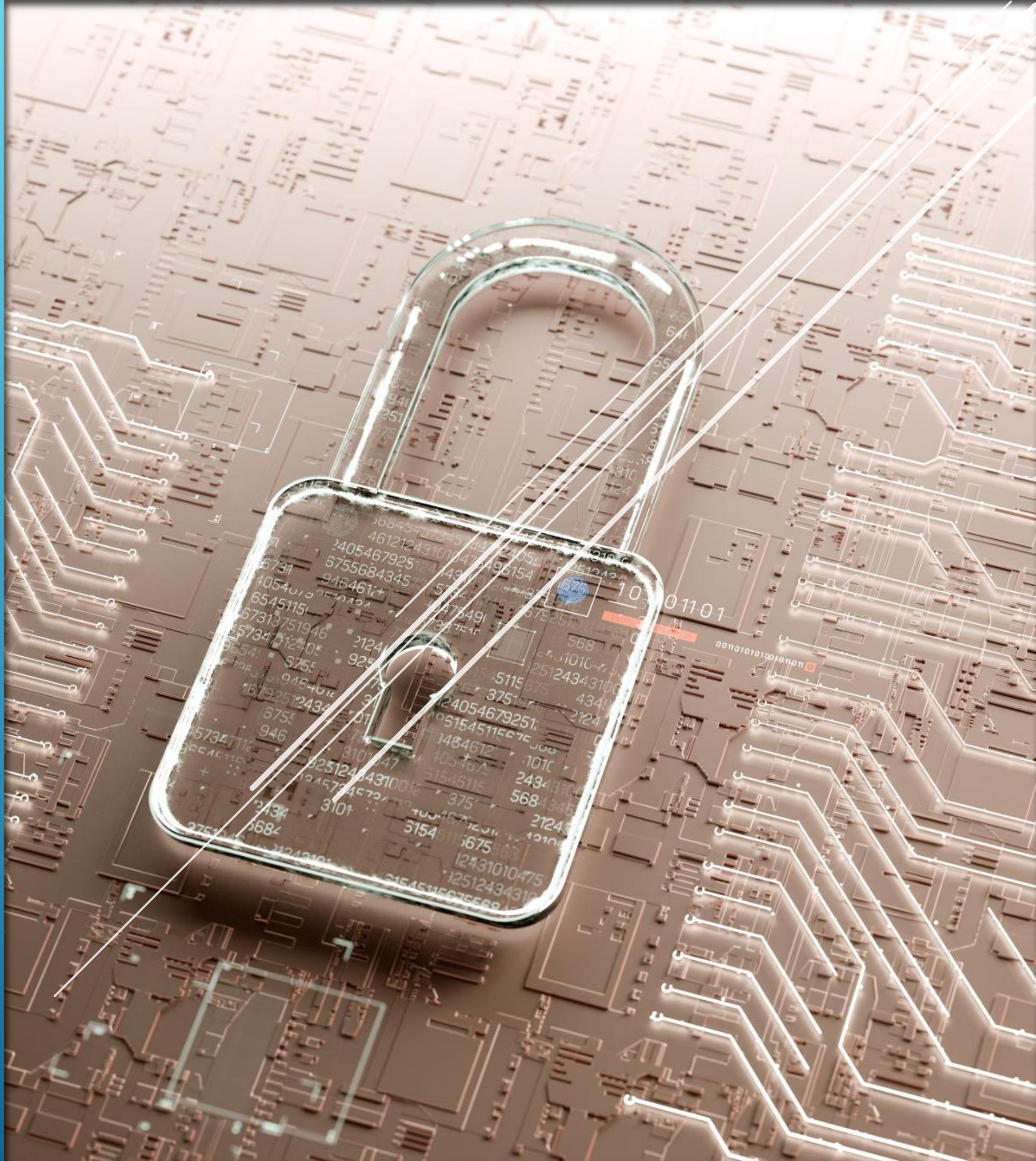


SYMMETRIC KEY ENCRYPTION

Symmetric encryption

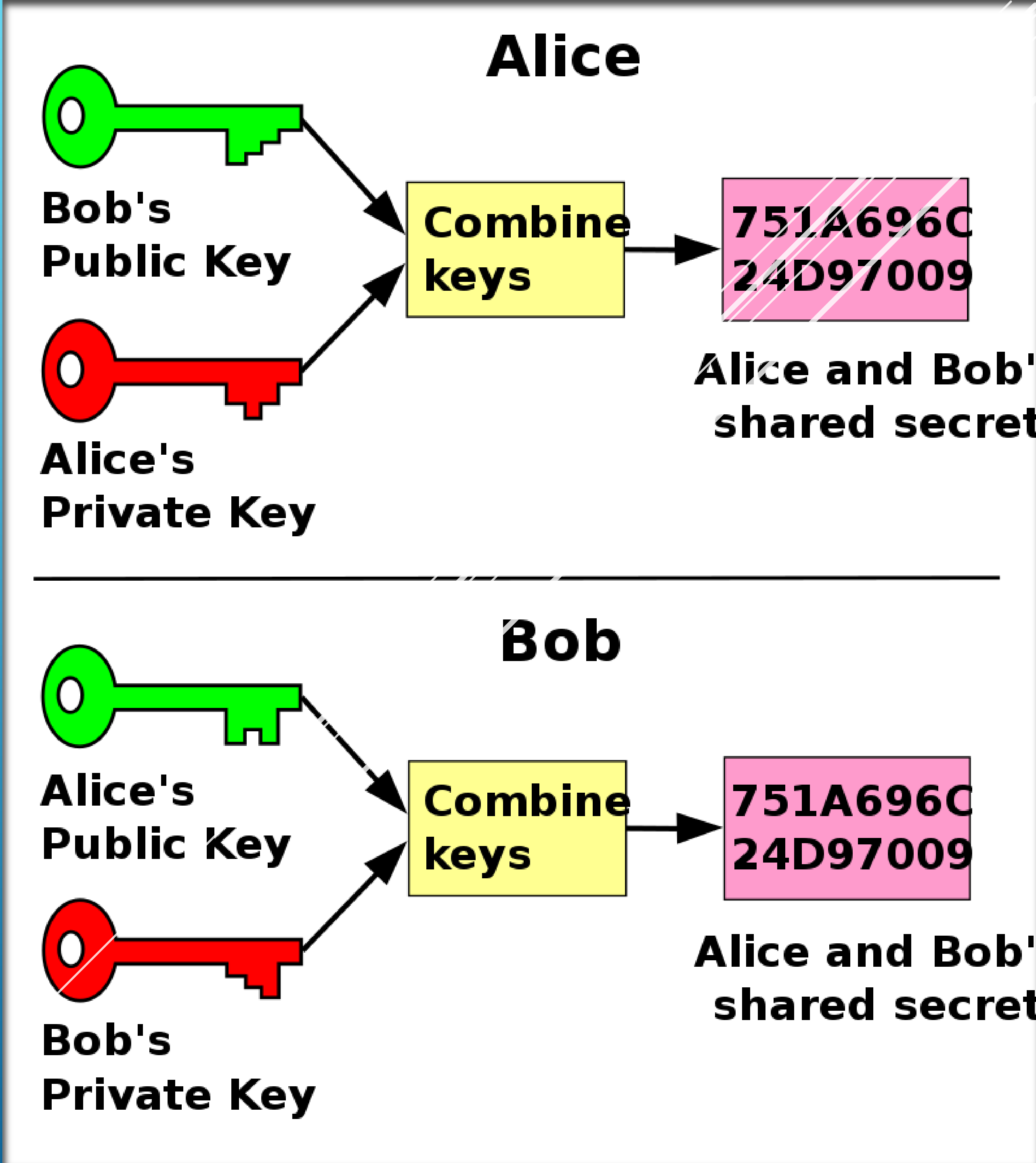
Secret key

ASYMMETRIC KEY ENCRYPTION



SECURE KEY EXCHANGE?

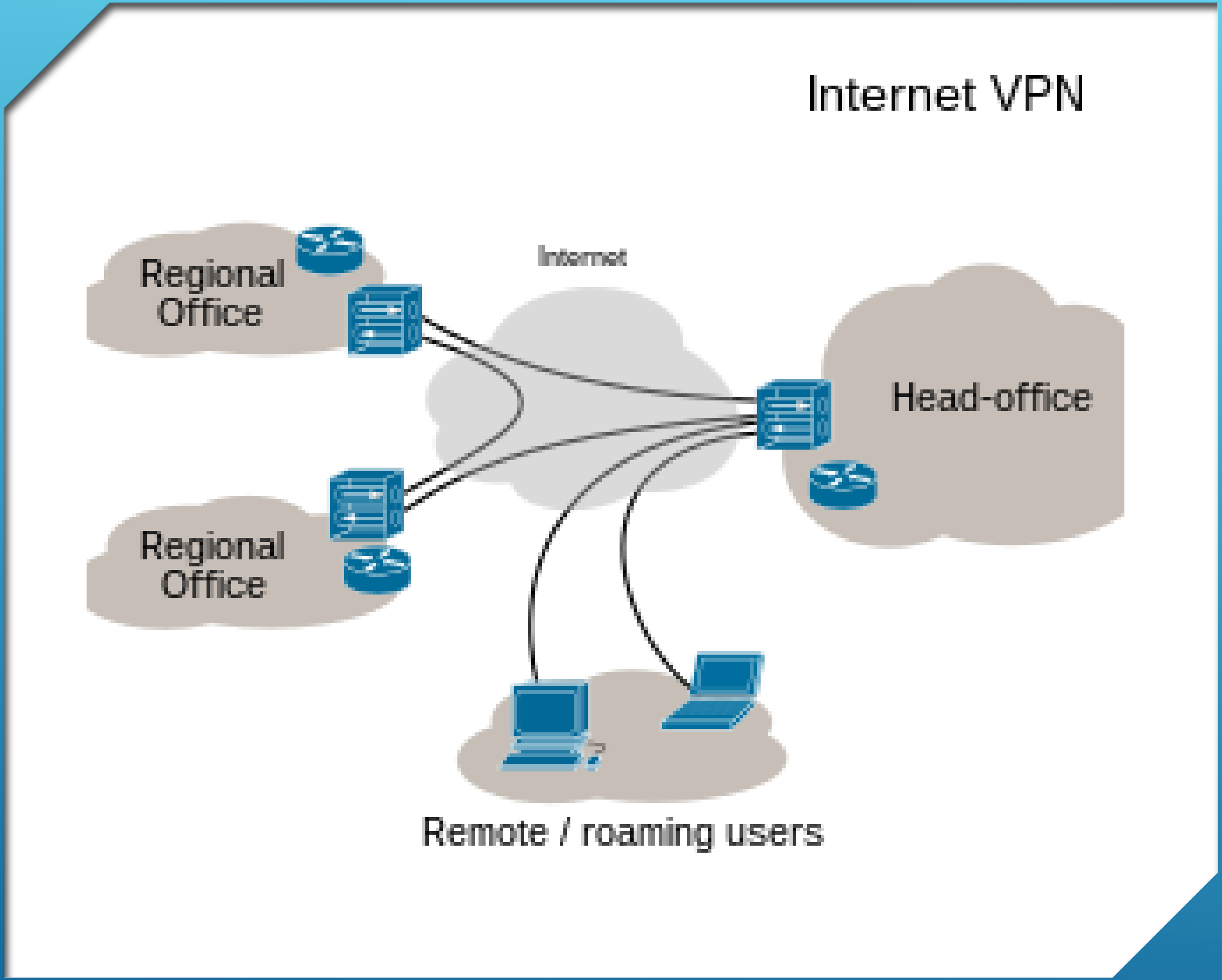
PUBLIC KEY CRYPTOGRAPHY



10 MINUTE BREAK

SECURING NETWORK CONNECTIONS IN PRACTICE

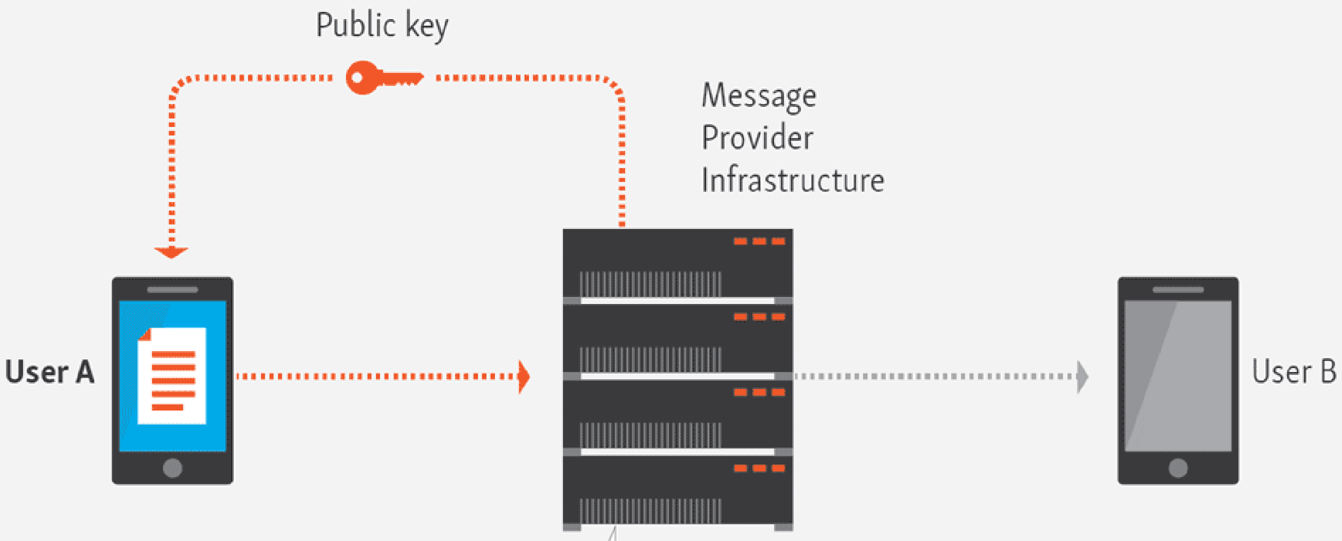
VIRTUAL PRIVATE NETWORKS



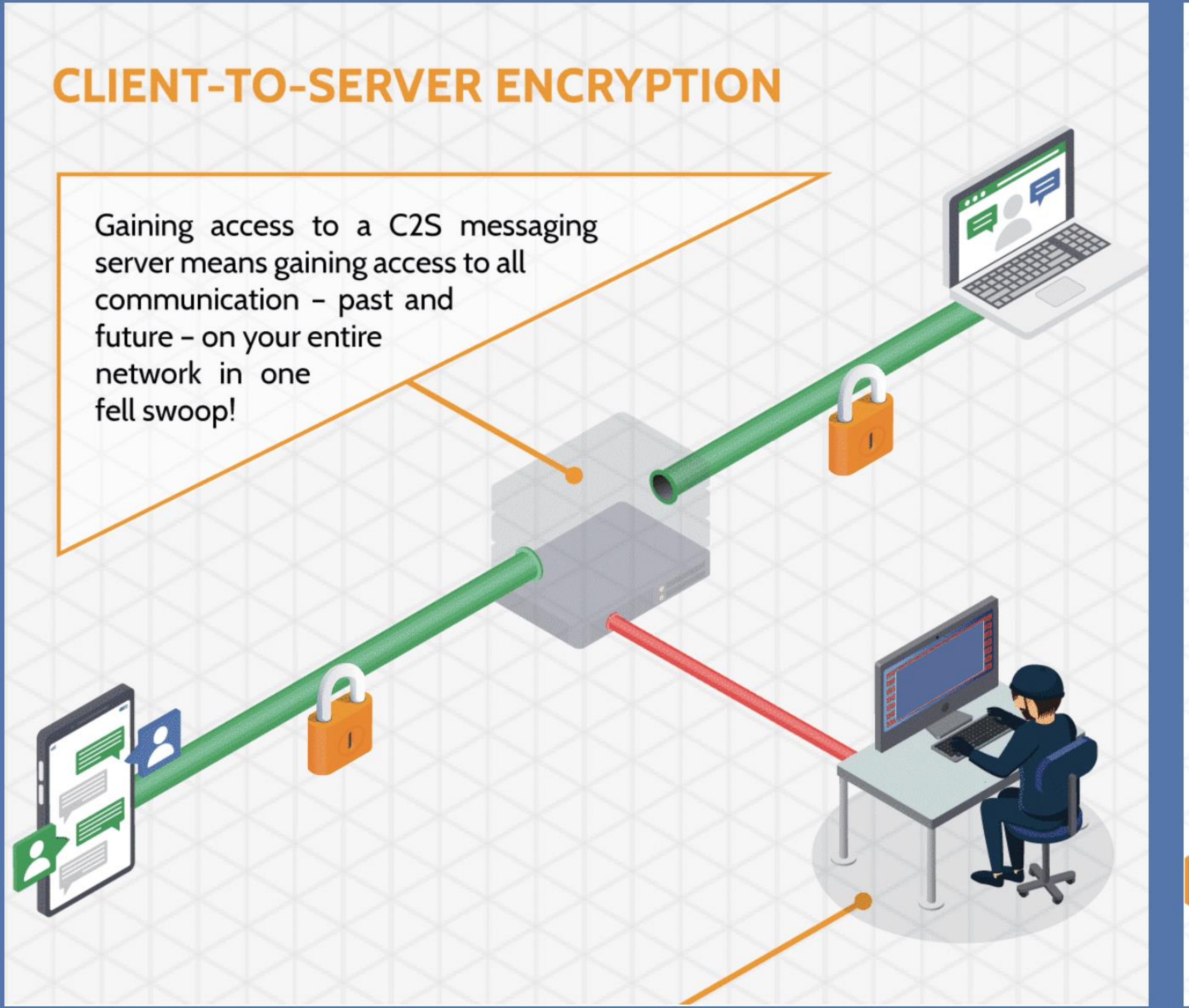
THIS IS HOW END-TO-END ENCRYPTION WORKS

● ● ● ● ● ●

A major selling point for instant-messaging providers is some form of content encryption. But does this technology fully protect your privacy?

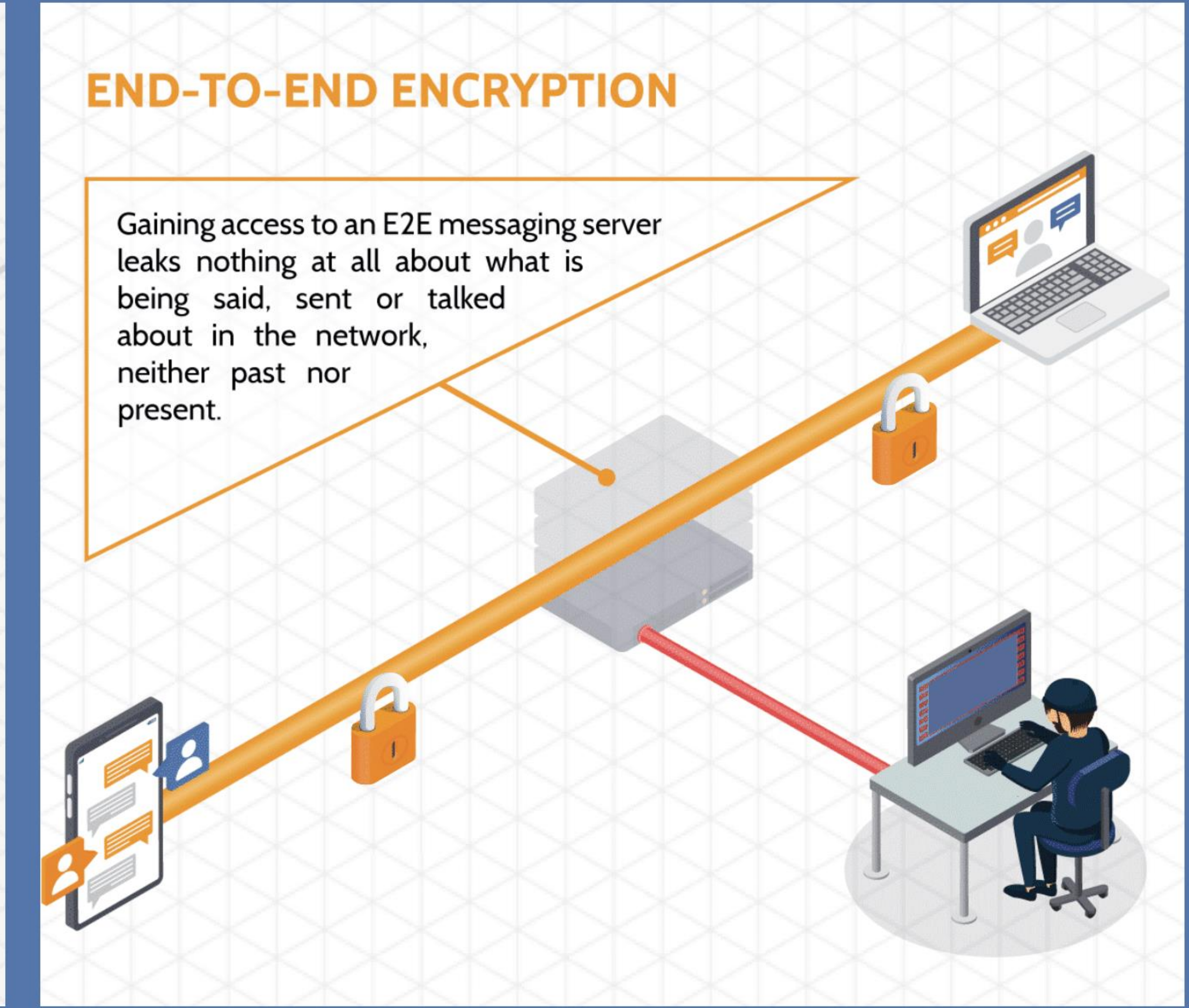


To securely send a message to User B, User A retrieves from the message provider a public key that applies to User B.



CLIENT-TO-SERVER ENCRYPTION

Gaining access to a C2S messaging server means gaining access to all communication – past and future – on your entire network in one fell swoop!



END-TO-END ENCRYPTION

Gaining access to an E2E messaging server leaks nothing at all about what is being said, sent or talked about in the network, neither past nor present.

WHY DO WE CARE ABOUT TRUST?

WHAT IS A SECURITY CERTIFICATE?

WHAT DOES A SECURITY CERTIFICATE DO?

- Provides trust
- Allows a secure connection
- Encrypts data
- HTTPS

- X.509 certificate
- Provides Transport Layer security
- Free!
- Trusted?

CERTIFICATE AUTHORITIES

HOW DO WE KNOW WHO WE CAN AND CAN'T TRUST?

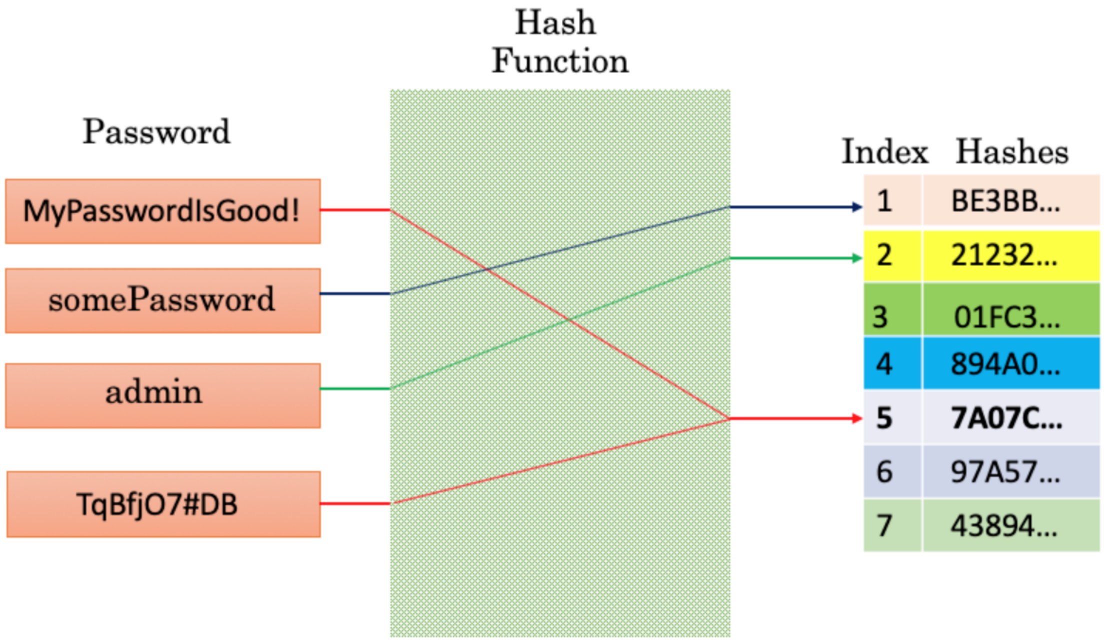
AUDIT YOUR FAVORITE WEBSITE!

https://www.sslshopper.com/ssl-checker.html

THREATS TO POOR ENCRYPTION

- Cleartext passwords
- Password cracking
- Man-In-The-Middle (MITM) attack
- Rainbow Tables
- Hash collisions

HASH COLLISIONS



Hash Function

Password

MyPasswordIsGood!

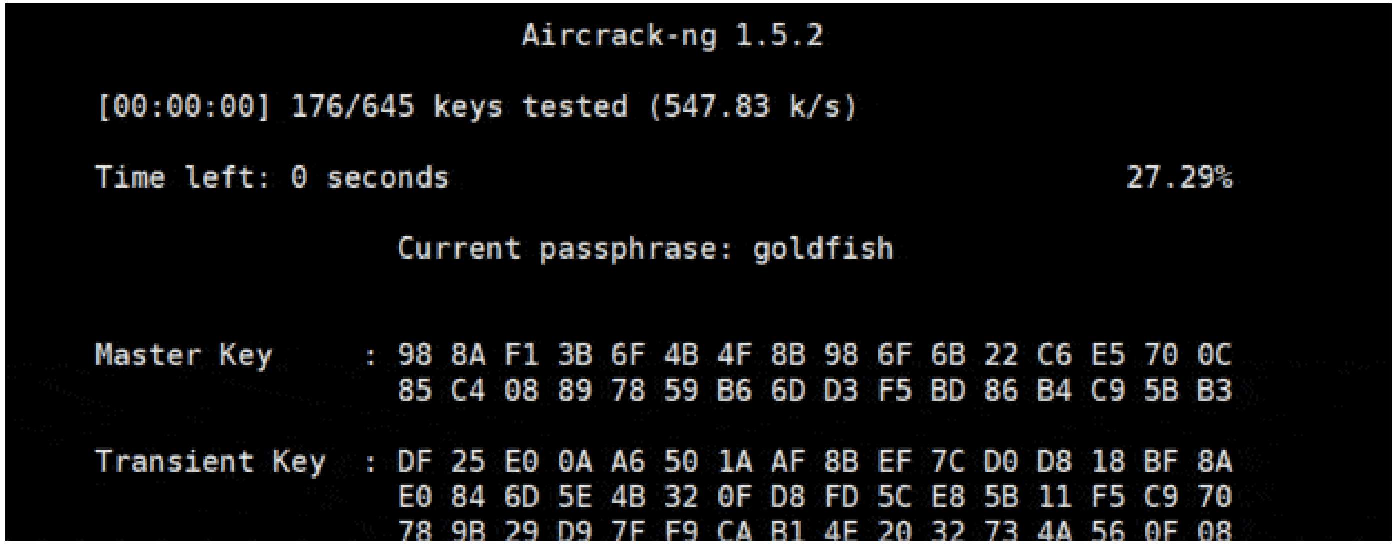
somePassword

admin

TqBfjO7#DB

Index	Hashes
1	BE3BB…
2	21232…
3	01FC3…
4	894A0…
5	**7A07C…**
6	97A57…
7	43894…

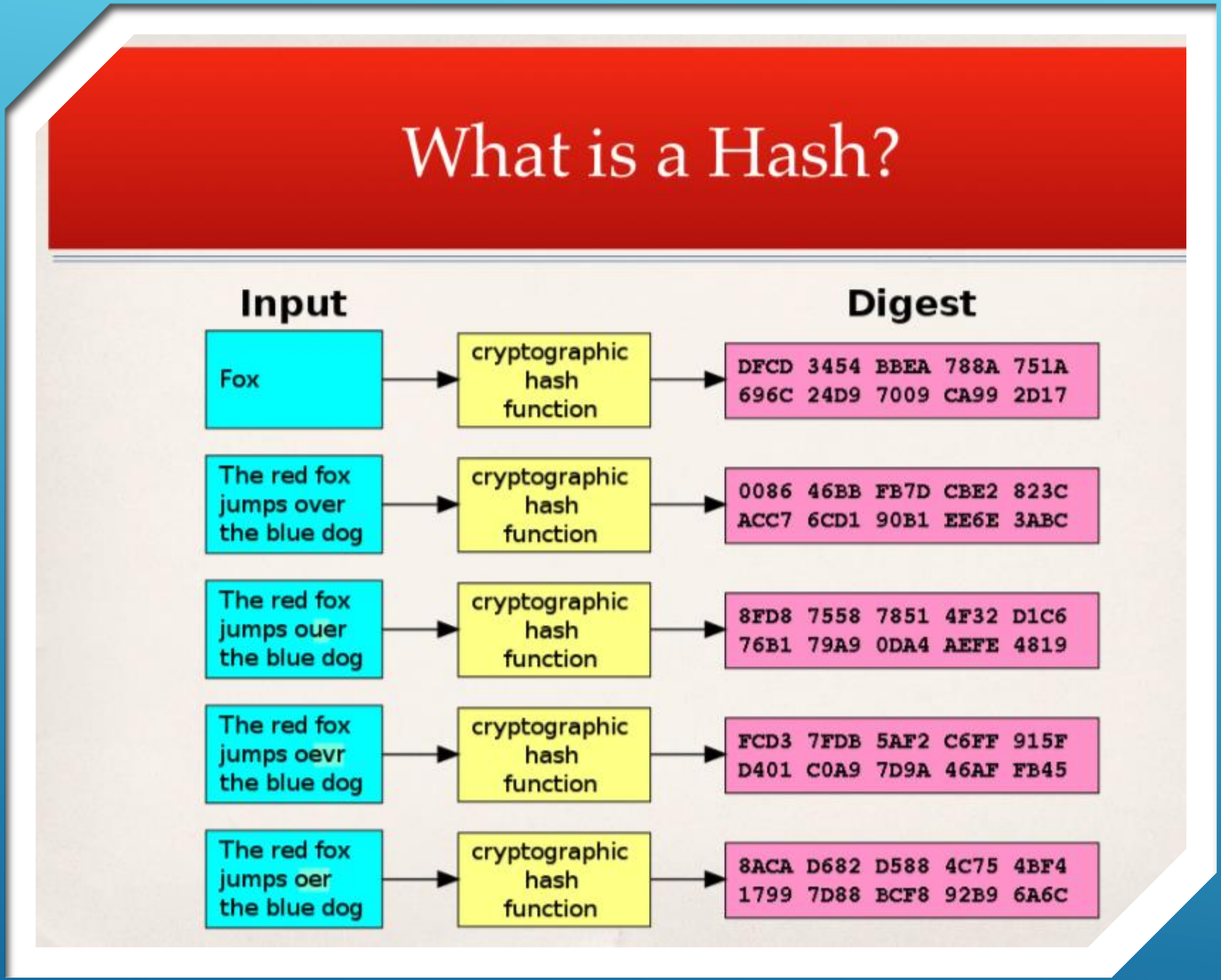
BRUTE FORCING



```
                              Aircrack-ng 1.5.2

     [00:00:00] 176/645 keys tested (547.83 k/s)

     Time left: 0 seconds                                      27.29%

                      Current passphrase: goldfish


     Master Key     : 98 8A F1 3B 6F 4B 4F 8B 98 6F 6B 22 C6 E5 70 0C
                      85 C4 08 89 78 59 B6 6D D3 F5 BD 86 B4 C9 5B B3

     Transient Key  : DF 25 E0 0A A6 50 1A AF 8B EF 7C D0 D8 18 BF 8A
                      E0 84 6D 5E 4B 32 0F D8 FD 5C E8 5B 11 F5 C9 70
                      78 9B 29 D9 7E F9 CA B1 4E 20 32 73 4A 56 0F 08
```

REAL-LIFE PASSWORD CRACKING

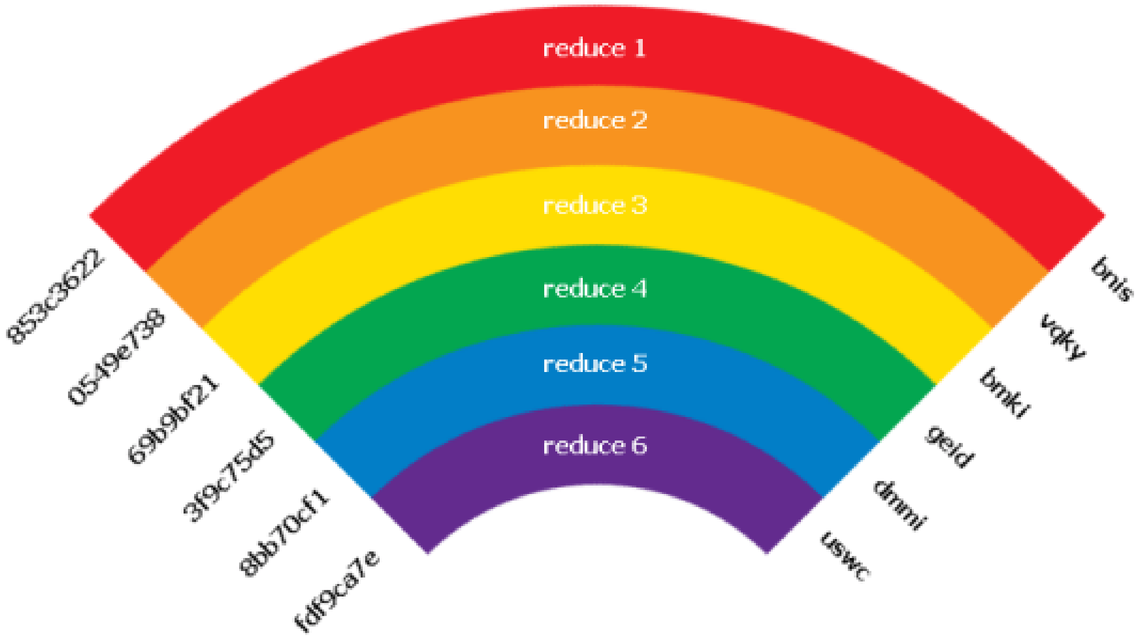
RAINBOW TABLES

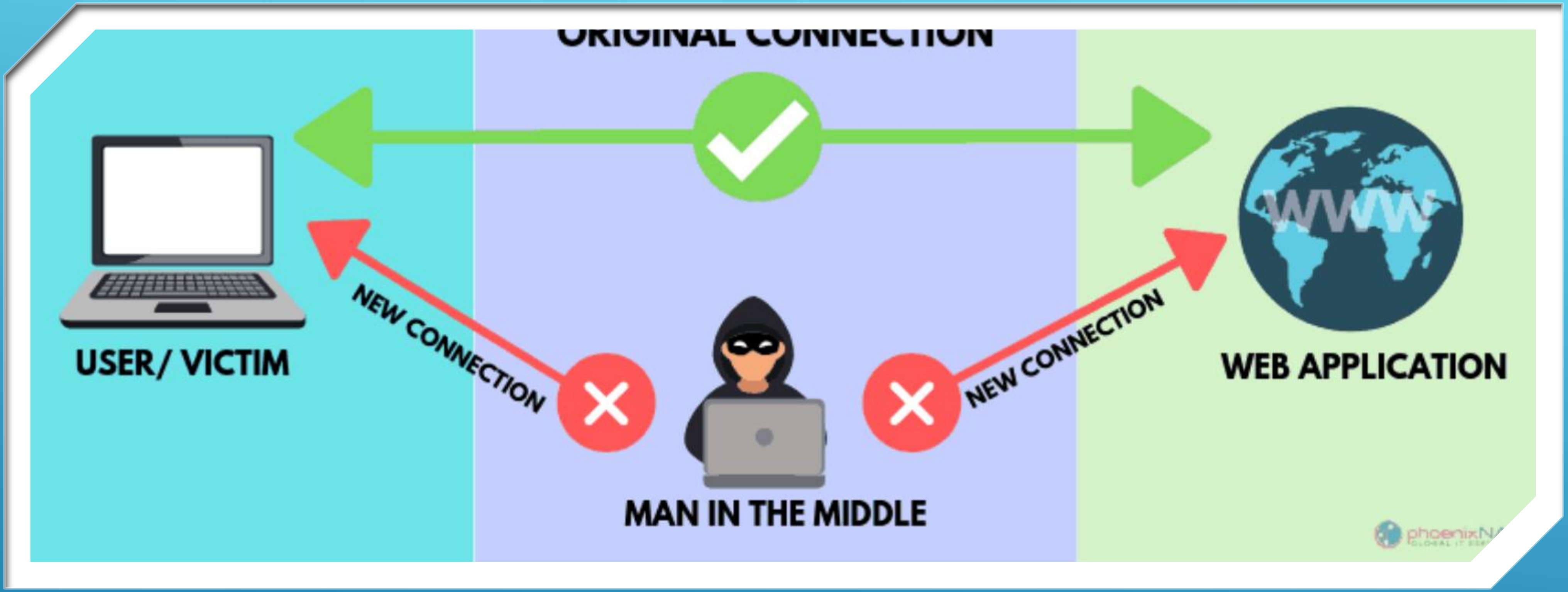


What is a Hash?

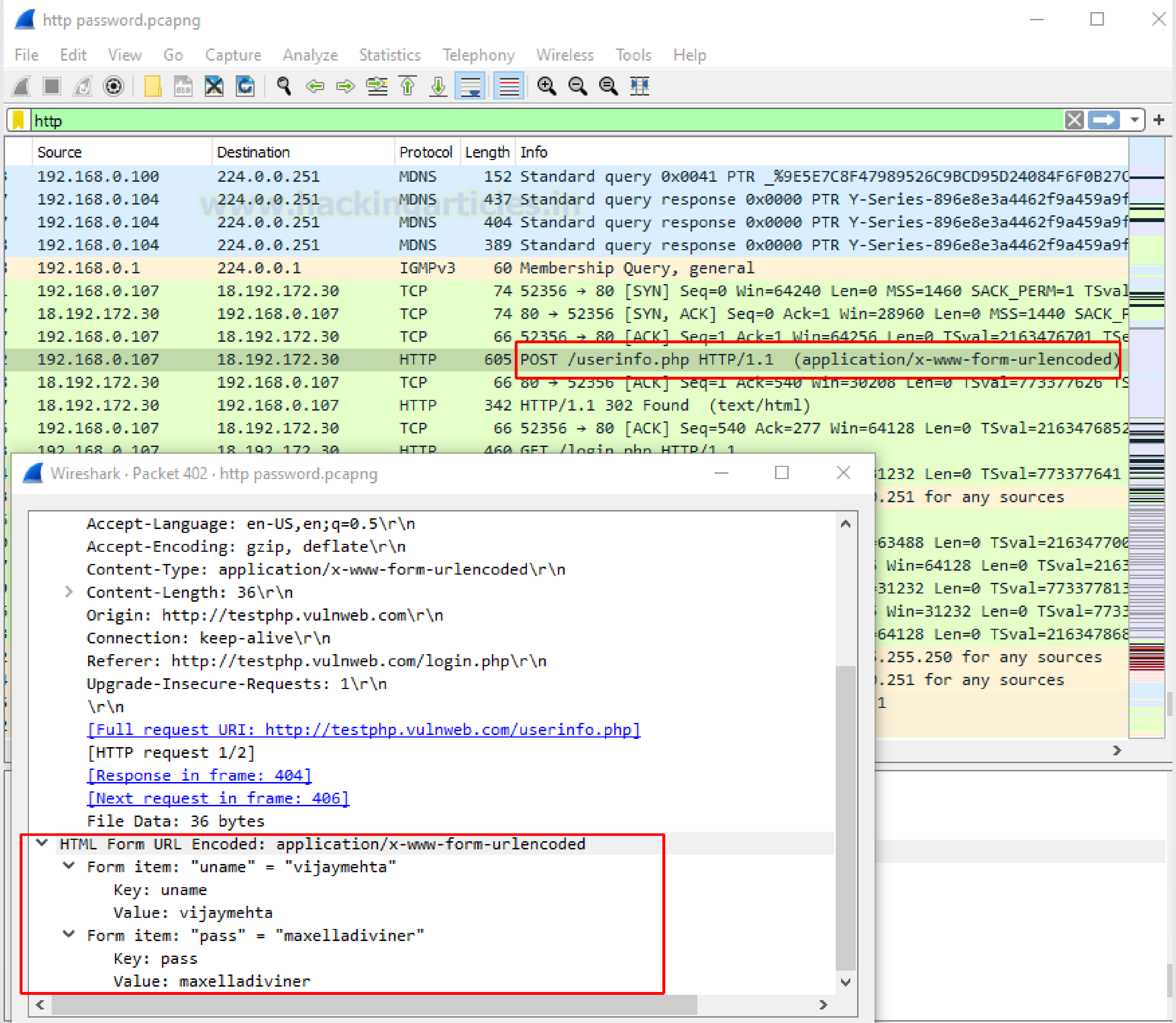
Input		Digest
Fox	cryptographic hash function	DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog	cryptographic hash function	0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog	cryptographic hash function	8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog	cryptographic hash function	FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog	cryptographic hash function	8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

RAINBOW TABLES CONT’





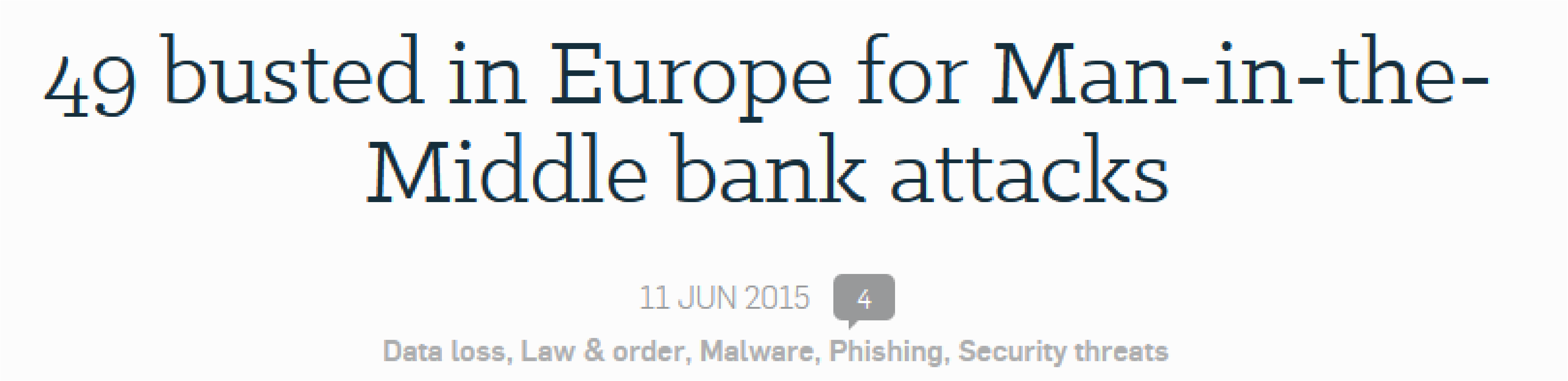
MAN-IN-THE-MIDDLE



www.hackingarticles.in

```
Source          Destination     Protocol Length Info
192.168.0.100   224.0.0.251     MDNS     152 Standard query 0x0041 PTR _%9E5E7C8F47989526C9BCD95D24084F6F0B27C
192.168.0.104   224.0.0.251     MDNS     437 Standard query response 0x0000 PTR Y-Series-896e8e3a4462f9a459a9f
192.168.0.104   224.0.0.251     MDNS     404 Standard query response 0x0000 PTR Y-Series-896e8e3a4462f9a459a9f
192.168.0.104   224.0.0.251     MDNS     389 Standard query response 0x0000 PTR Y-Series-896e8e3a4462f9a459a9f
192.168.0.1     224.0.0.1       IGMPv3    60 Membership Query, general
192.168.0.107   18.192.172.30   TCP       74 52356 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval
18.192.172.30   192.168.0.107   TCP       74 80 → 52356 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1440 SACK_P
192.168.0.107   18.192.172.30   TCP       66 52356 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2163476701 TSe
192.168.0.107   18.192.172.30   HTTP     605 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
18.192.172.30   192.168.0.107   TCP       66 80 → 52356 [ACK] Seq=1 Ack=540 Win=30208 Len=0 TSval=773377626 TS
18.192.172.30   192.168.0.107   HTTP     342 HTTP/1.1 302 Found  (text/html)
192.168.0.107   18.192.172.30   TCP       66 52356 → 80 [ACK] Seq=540 Ack=277 Win=64128 Len=0 TSval=2163476852
192.168.0.107   18.192.172.30   HTTP     460 GET /login.php HTTP/1.1
                                             1232 Len=0 TSval=773377641
                                             .251 for any sources
                                             63488 Len=0 TSval=216347700
                                             Win=64128 Len=0 TSval=2163
                                             31232 Len=0 TSval=773377813
                                             Win=31232 Len=0 TSval=7733
                                             64128 Len=0 TSval=216347868
                                             .255.250 for any sources
                                             .251 for any sources
                                             1
```

```
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  > Content-Length: 36\r\n
    Origin: http://testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    [HTTP request 1/2]
    [Response in frame: 404]
    [Next request in frame: 406]
    File Data: 36 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  v Form item: "uname" = "vijaymehta"
      Key: uname
      Value: vijaymehta
  v Form item: "pass" = "maxelladiviner"
      Key: pass
      Value: maxelladiviner
```



49 busted in Europe for Man-in-the-Middle bank attacks

11 JUN 2015 4

Data loss, Law & order, Malware, Phishing, Security threats

REAL-WORLD MITM ATTACK

REVIEW DAY 3

QUESTIONS?

PREVIEW DAY 4