INTRODUCTION TO SOFTWARE BUSINESS PRODUCT MANAGEMENT

Week 2 Day 1

Led by: Emily Crose

for

Oakland University

WEEK 1 RECAP

QUESTIONS FROM LAST WEEK?

SECURING & ENCRYPTING DATA

CLEARTEXT VS. CIPHERTEXT

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!

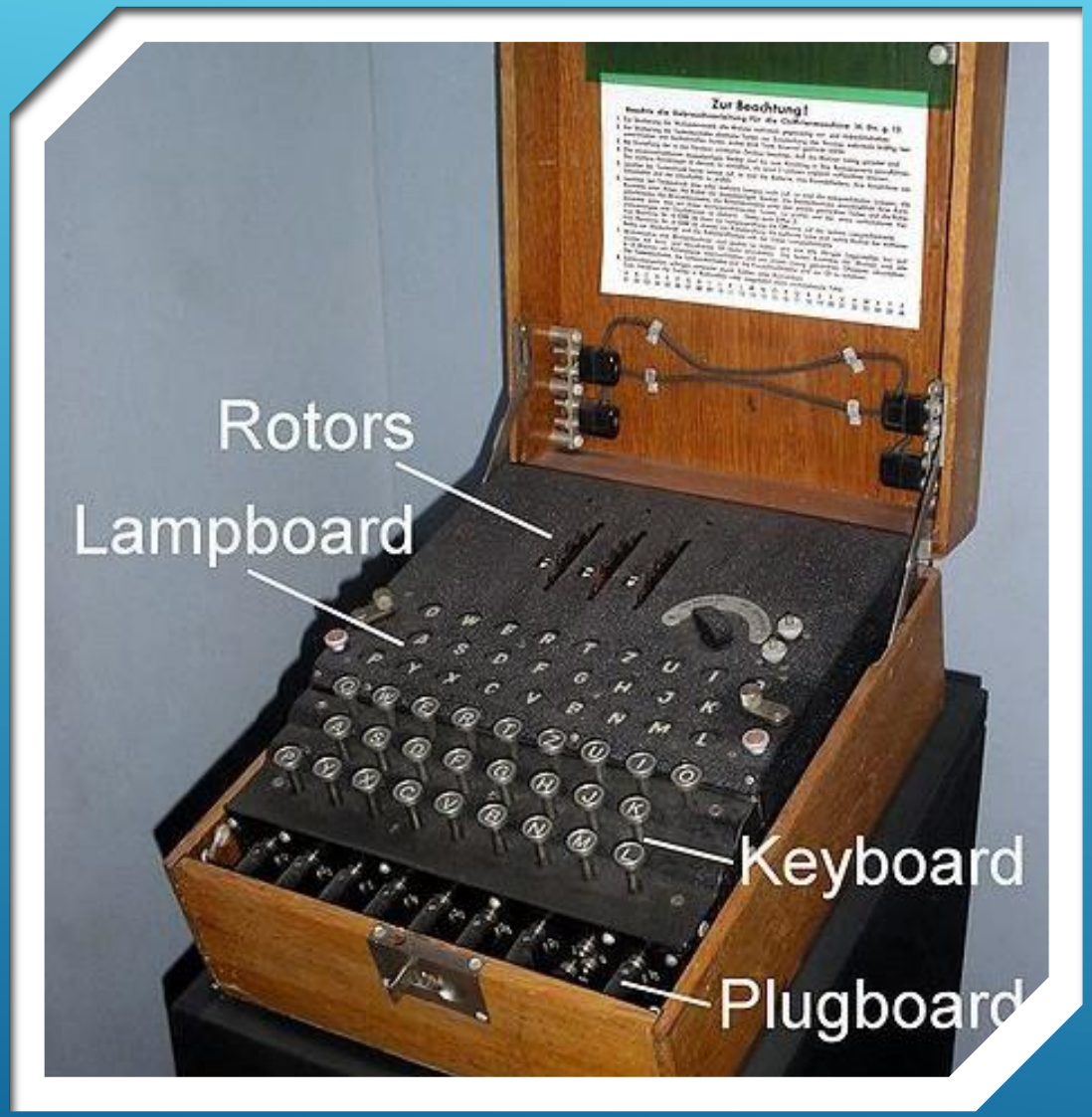
https://gchq.github.io/CyberChef/

WHAT IS ENCRYPTION?

ENCRYPTION HISTORY

HAND CIPHERS

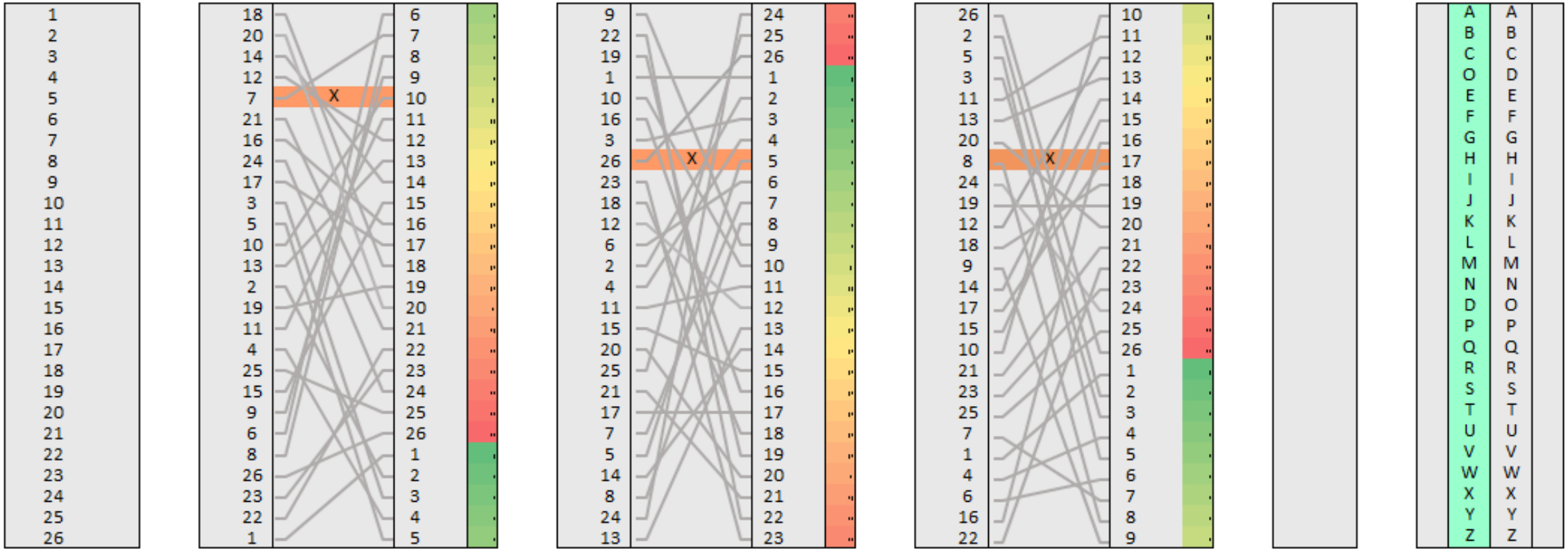
- Substitution (or "Caesar") cipher – (850 CE)
- Jefferson cipher – (1795)
- Vigenère cipher – (1553)
  - First to use an encryption key
- Code book cipher – (1500s?)
- Playfair cipher – (1854)



WARTIME CRYPTOGRAPHY

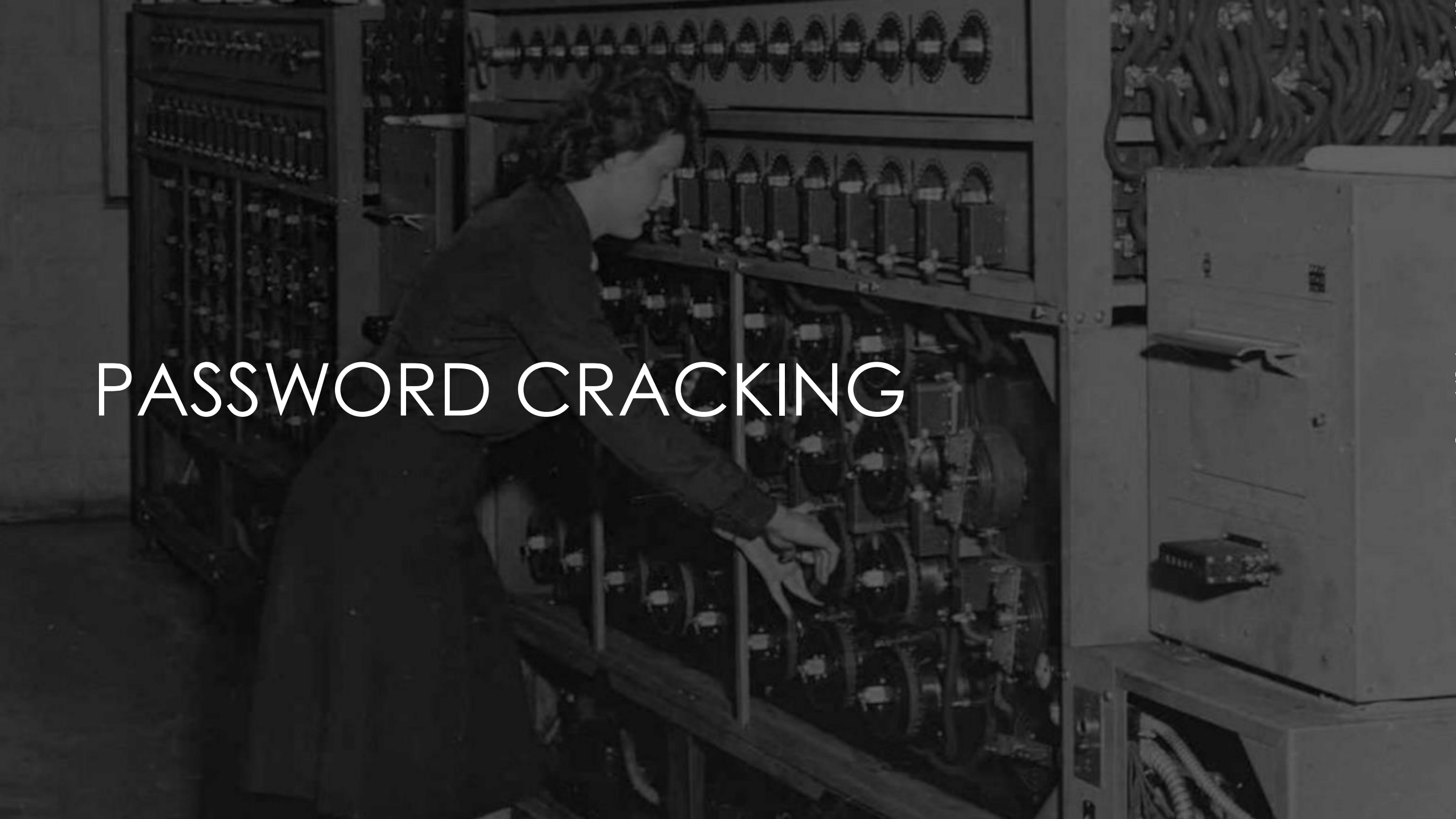
MESSAGE	HELLOWORLD	UNENCRYPTED LETTER	

UKW	3rd Wheel	2nd Wheel	1st Wheel	ETW	STECKER
	Index 6	Index 24	Index 10		



ENCRPYTED		ENCRYPTED LETTER	#N/A

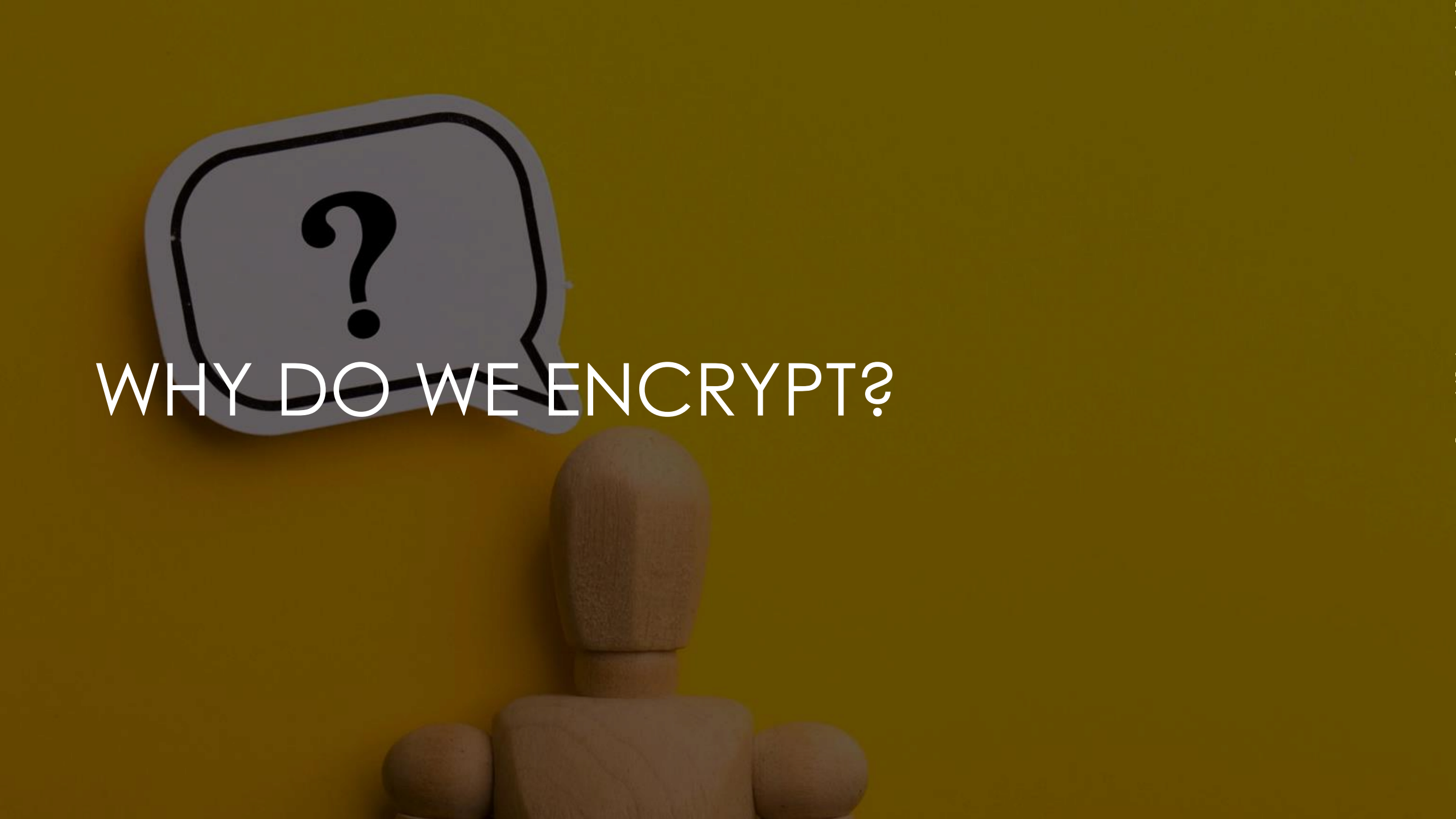
10 MINUTE BREAK



PASSWORD CRACKING

ONE-TIME PADS

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

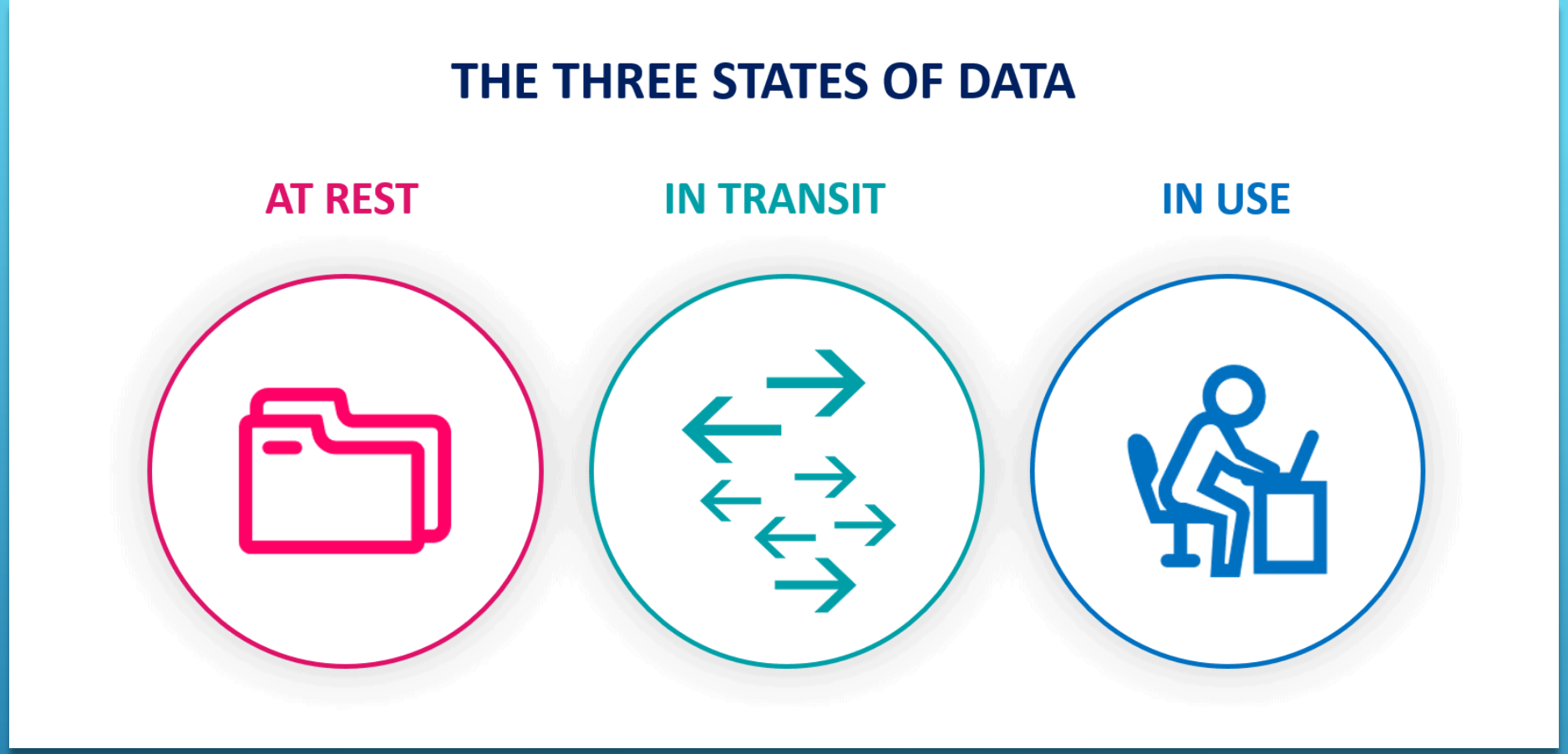
POPULAR MODERN CRYPTOGRAPHY ALGORITHMS

KEYSPACE/KEYLENGTH/KEYSIZE

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

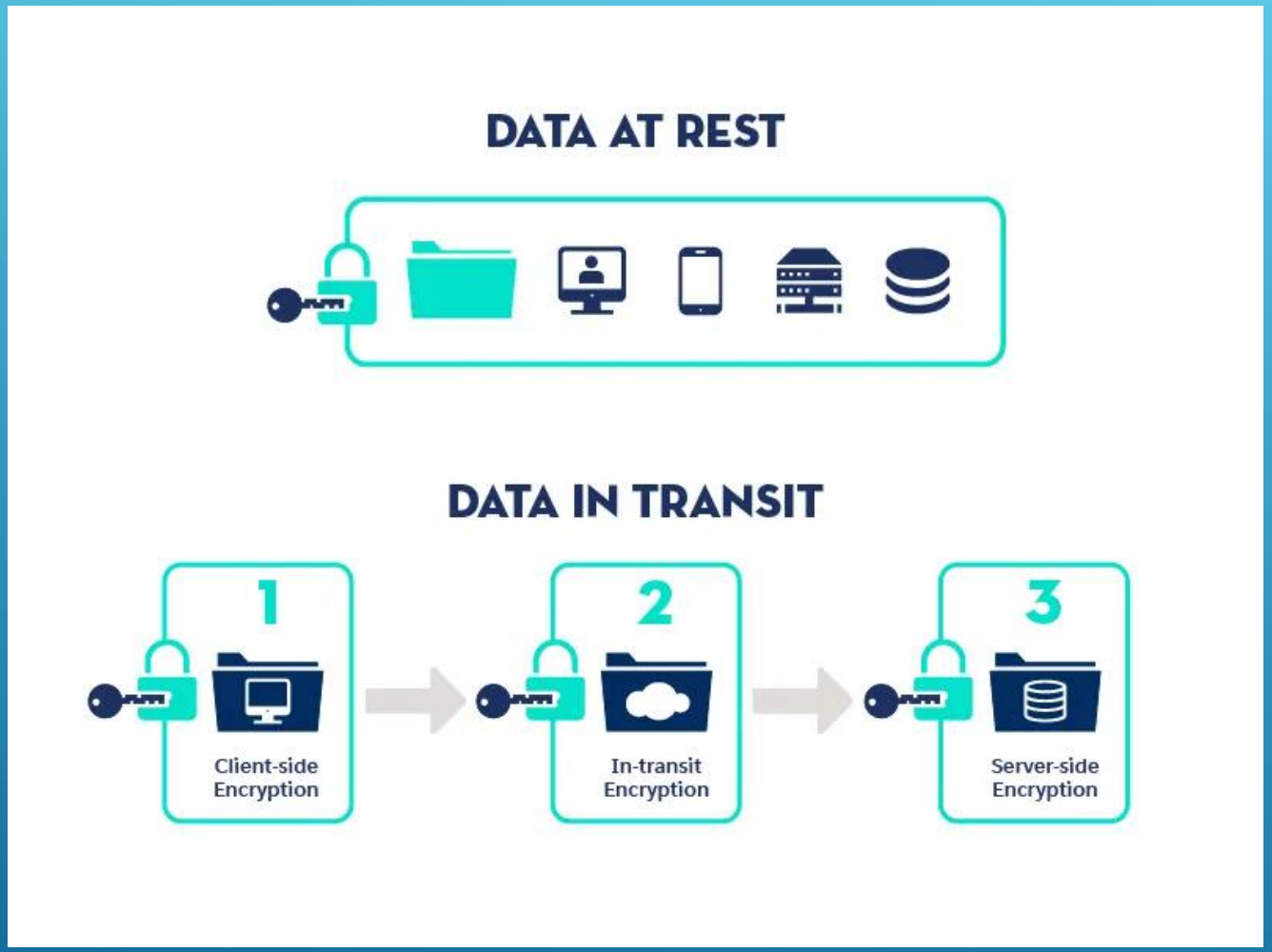
CRYPTOGRAPHIC STANDARDS

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

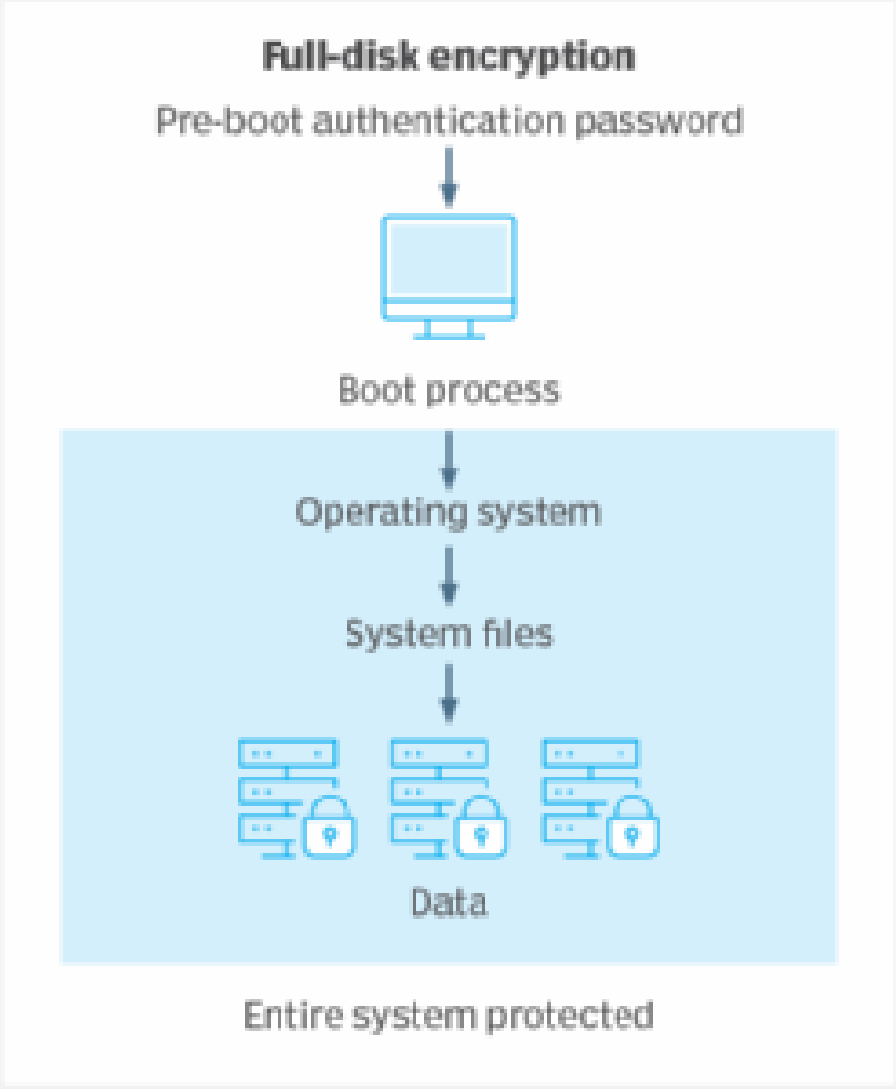


STATES OF DATA

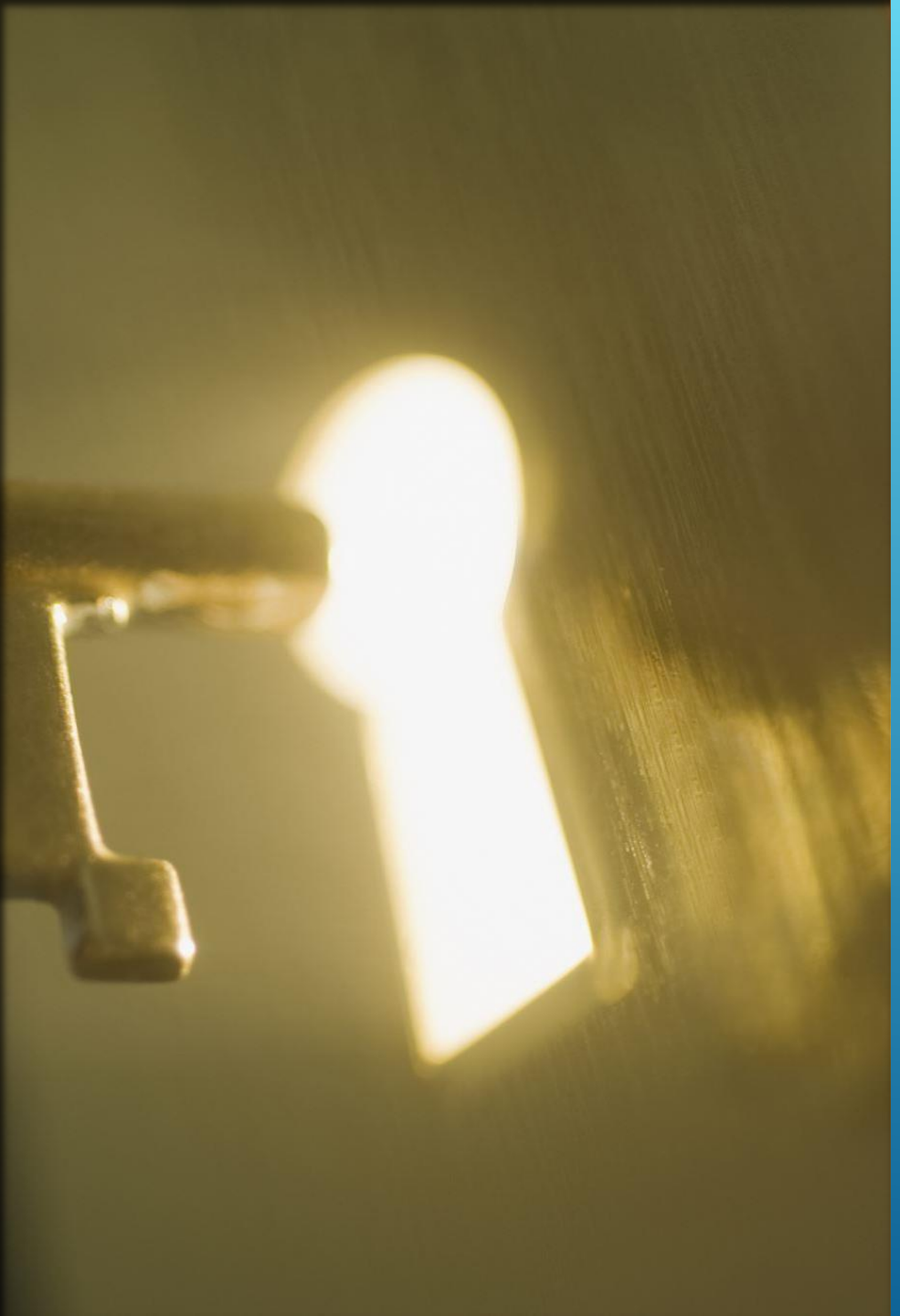
DATA SECURITY



How the FDE process works



FULL DISK ENCRYPTION



SYMMETRIC KEY ENCRYPTION

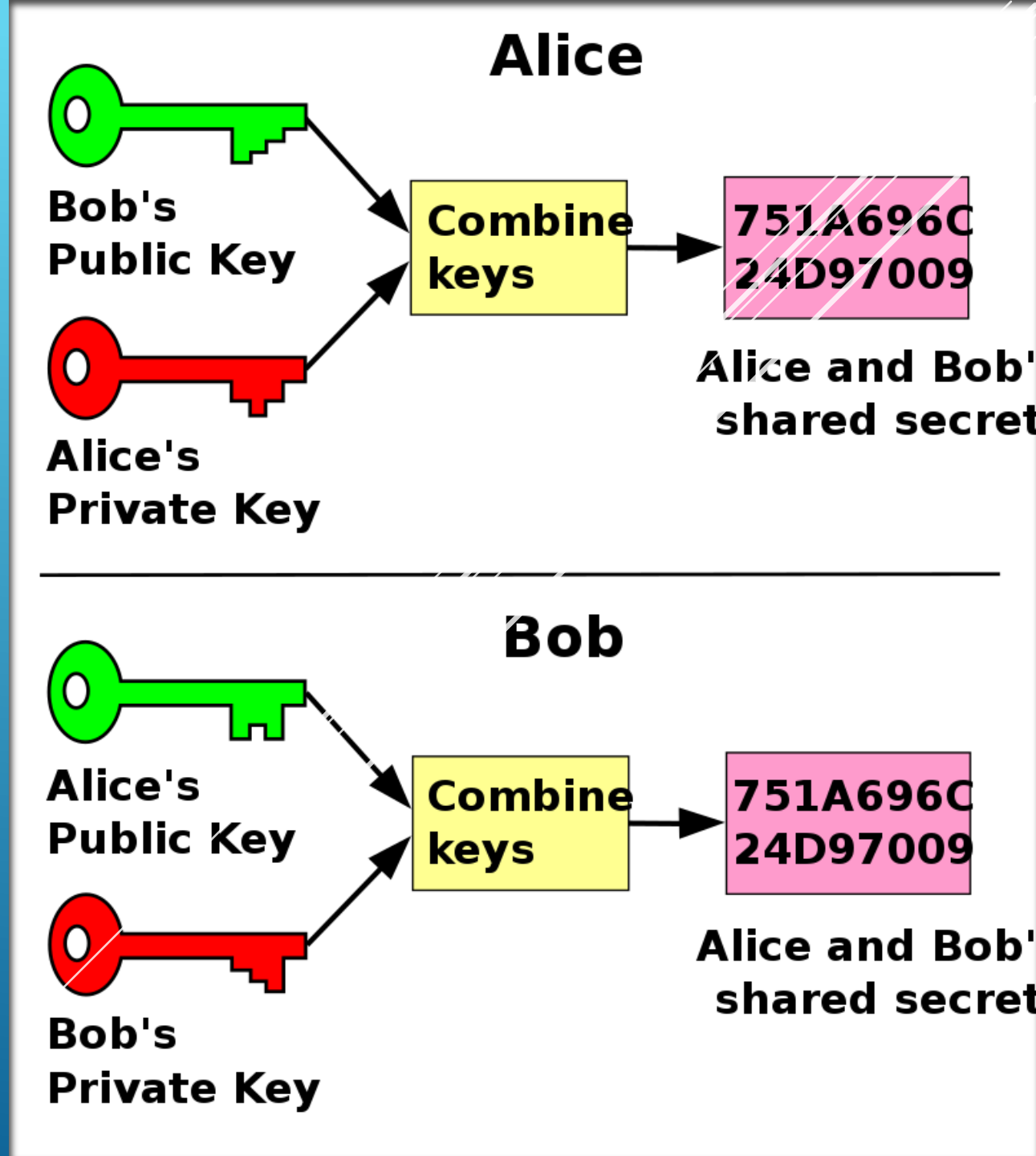
Symmetric encryption

Secret key

ASYMMETRIC KEY ENCRYPTION

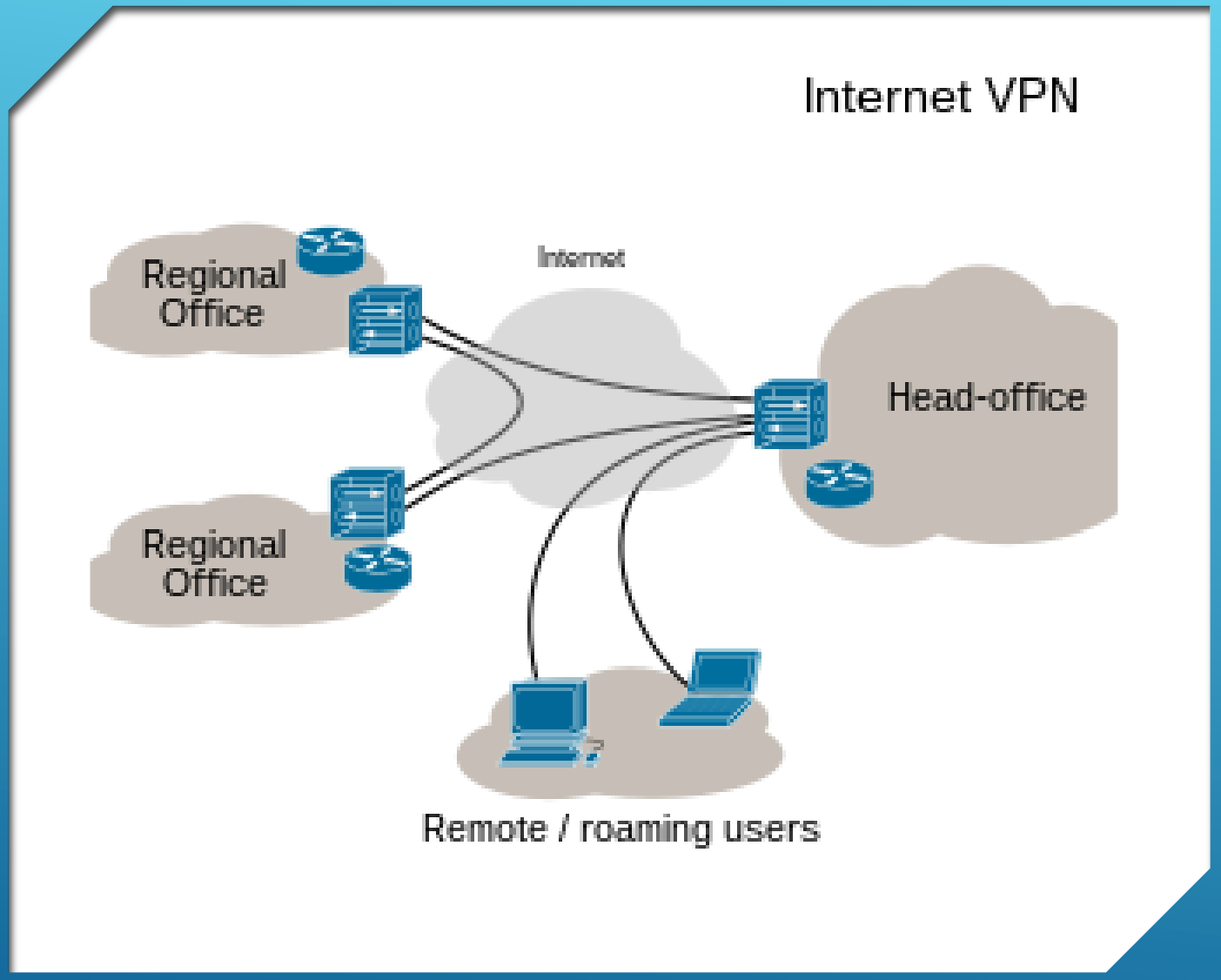
SECURE KEY EXCHANGE?

PUBLIC KEY CRYPTOGRAPHY



10 MINUTE BREAK

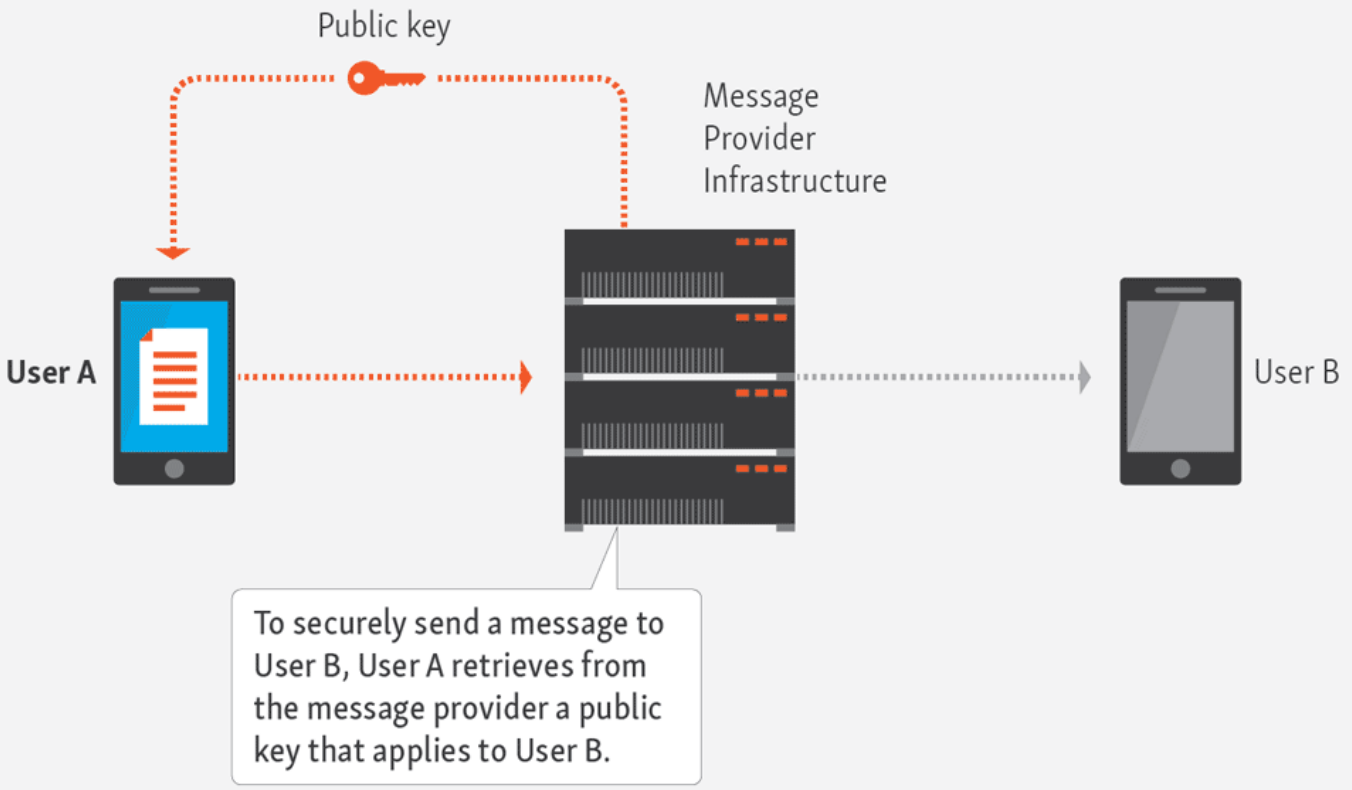
SECURING NETWORK CONNECTIONS IN PRACTICE



VIRTUAL PRIVATE NETWORKS

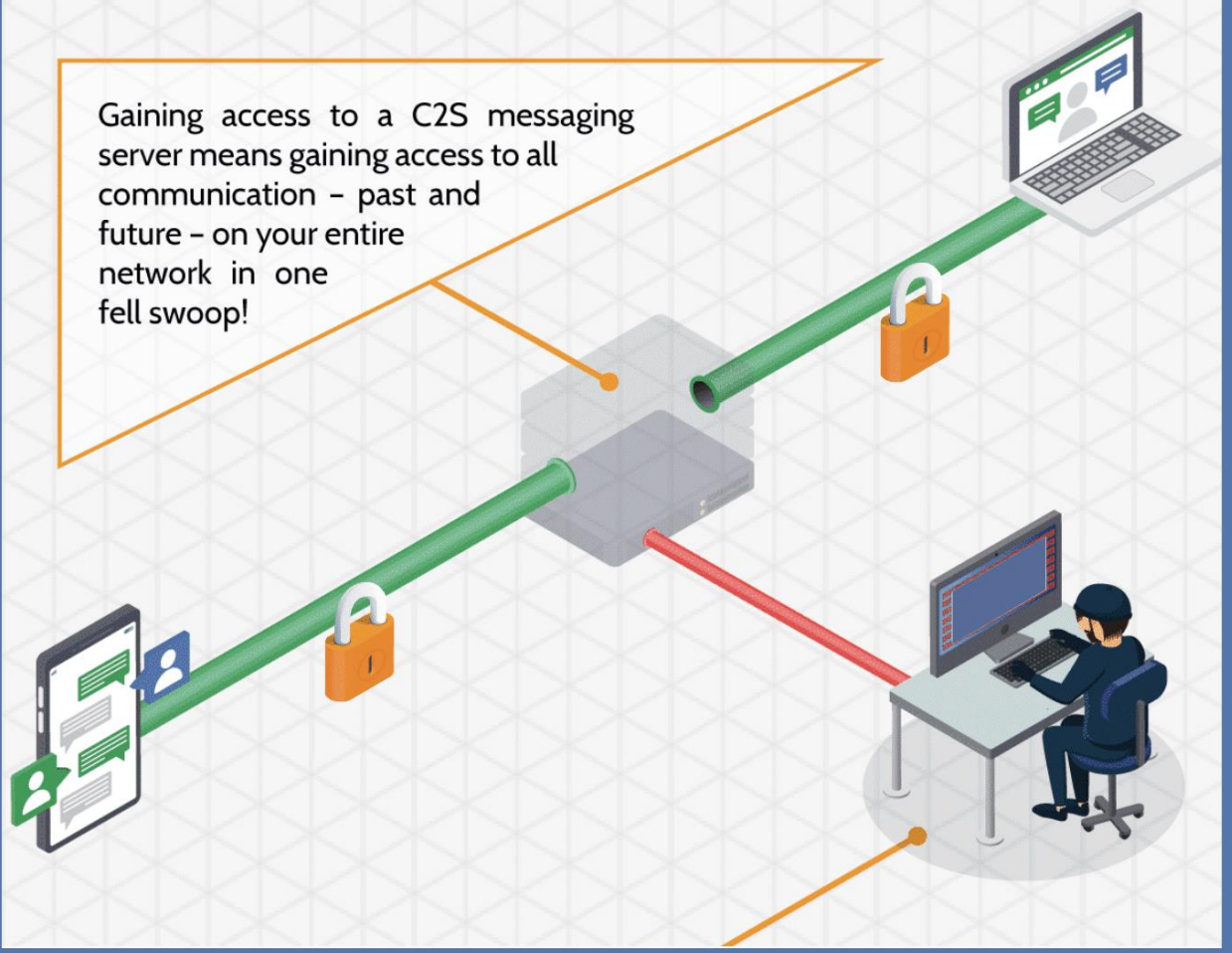
THIS IS HOW END-TO-END ENCRYPTION WORKS

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



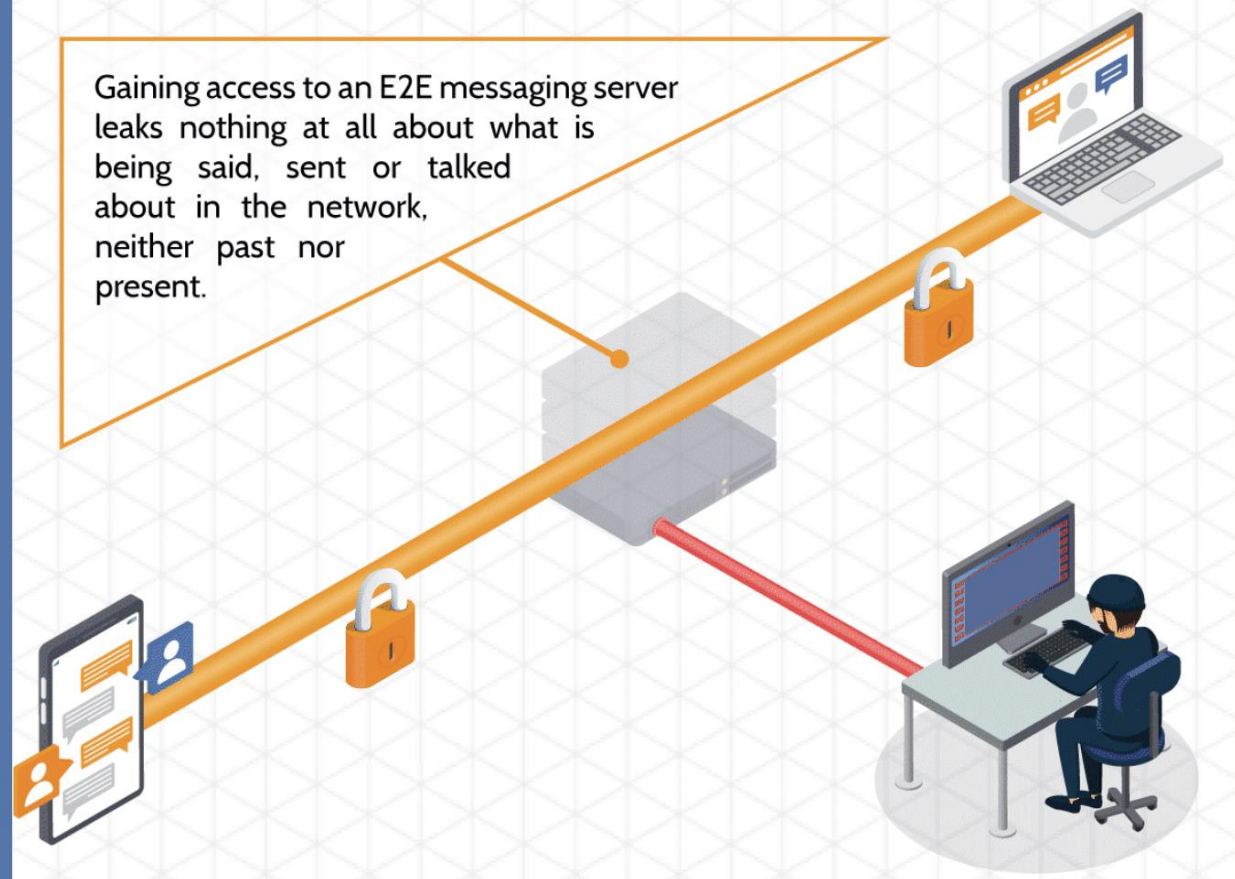
CLIENT-TO-SERVER ENCRYPTION

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

CERTIFICATE AUTHORITIES

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

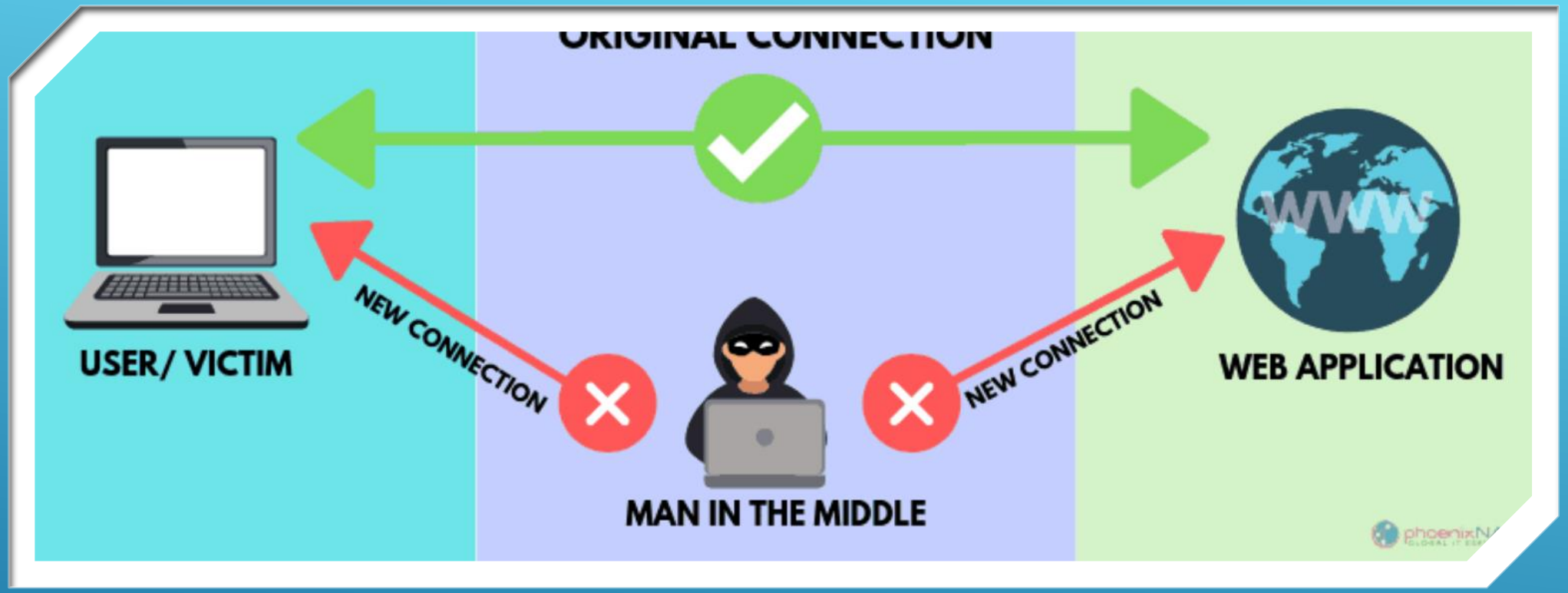
HOW DO WE KNOW WHO WE CAN AND CAN'T TRUST?

AUDIT YOUR FAVORITE WEBSITE!

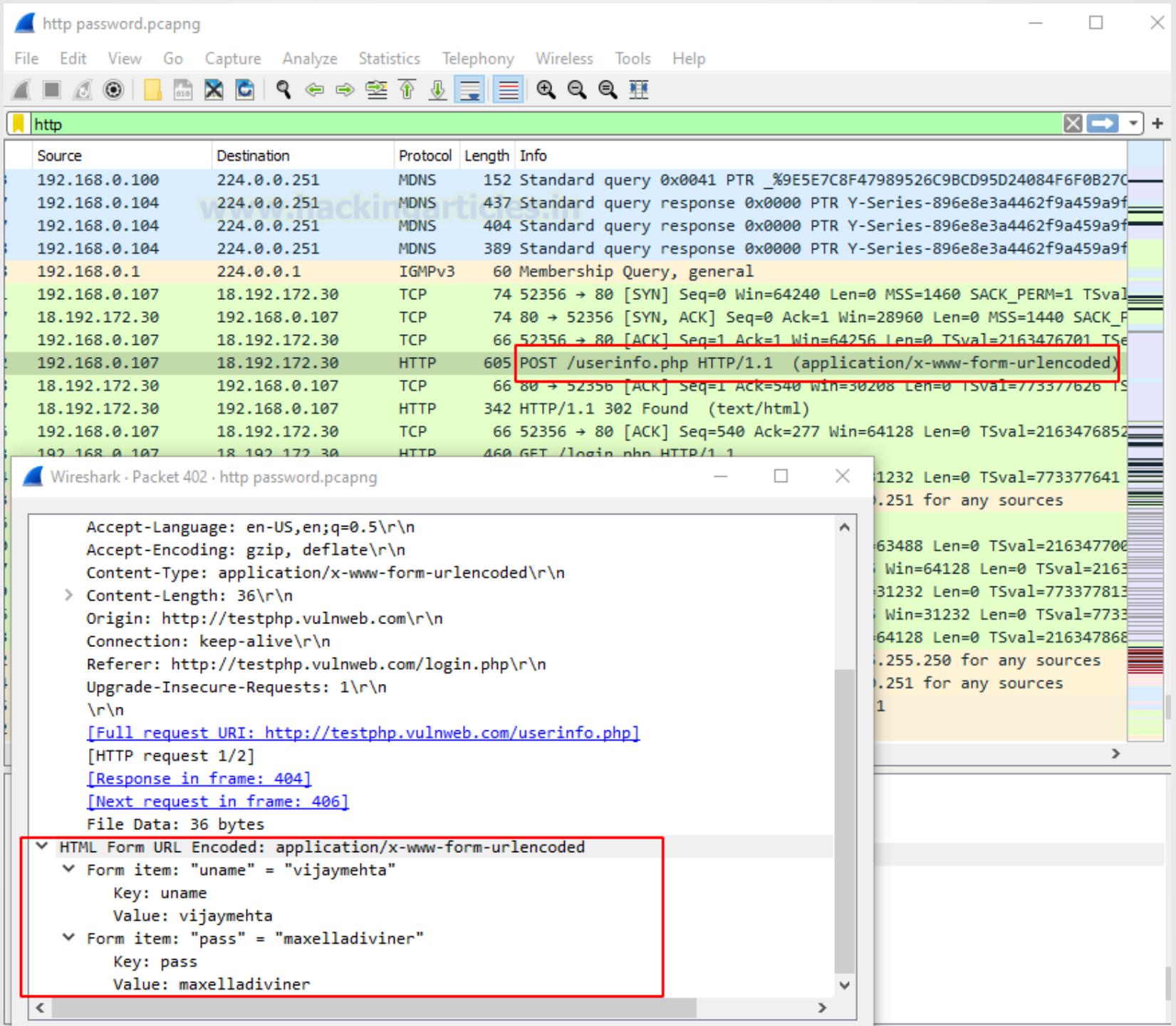
https://www.sslshopper.com/ssl-checker.html

THREATS TO POOR ENCRYPTION

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



MAN-IN-THE-MIDDLE


http password.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
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
Wireshark · Packet 402 · http password.pcapng
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
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "vijaymehta"
Key: uname
Value: vijaymehta
Form item: "pass" = "maxelladiviner"
Key: pass
Value: maxelladiviner

REAL-WORLD MITM ATTACK

REVIEW DAY 1

QUESTIONS?

PREVIEW DAY 2