

# INTRODUCTION TO SOFTWARE BUSINESS PRODUCT MANAGEMENT

**Week 1 Day 3**

Led by: Emily Crose  
for  
Oakland University



# DAY 2 RECAP





The background features a blue diagonal overlay from the top-left to the bottom-right. Underneath this overlay, there are numerous light blue question marks scattered across the surface. In the corners, outside the blue overlay, are several pieces of light brown paper, each with a large black question mark. On the right side, there are several thin, white, parallel diagonal lines.

QUESTIONS FROM  
DAY 2?



# SECURING & ENCRYPTING DATA



# CLEARTEXT VS. CIPHERTEXT

# *Cryptography*



The background is a solid dark red color. It is covered with a dense, repeating pattern of various black geometric shapes. These shapes include circles, triangles, squares, rectangles, and lines of different lengths and orientations. Some shapes are simple outlines, while others are more complex, like zig-zags or wavy lines. The overall effect is a busy, abstract, and somewhat chaotic pattern.

# HASHING



LAYER OF VALIDATION OF DATA

SECURES BOTH ENDS OF TRANSMISSION

ANYONE CAN VALIDATE!

PROTECTS ORIGINAL SECRET

IRREVERSIBLE

VALUE OF HASHING

Several thin, white, parallel diagonal lines are positioned in the bottom right corner of the slide, extending from the middle towards the bottom right edge.



A series of four parallel white diagonal lines in the bottom-left corner of the slide.

# POPULAR HASHING ALGORITHMS

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

# LET'S TRY SOME HASH!

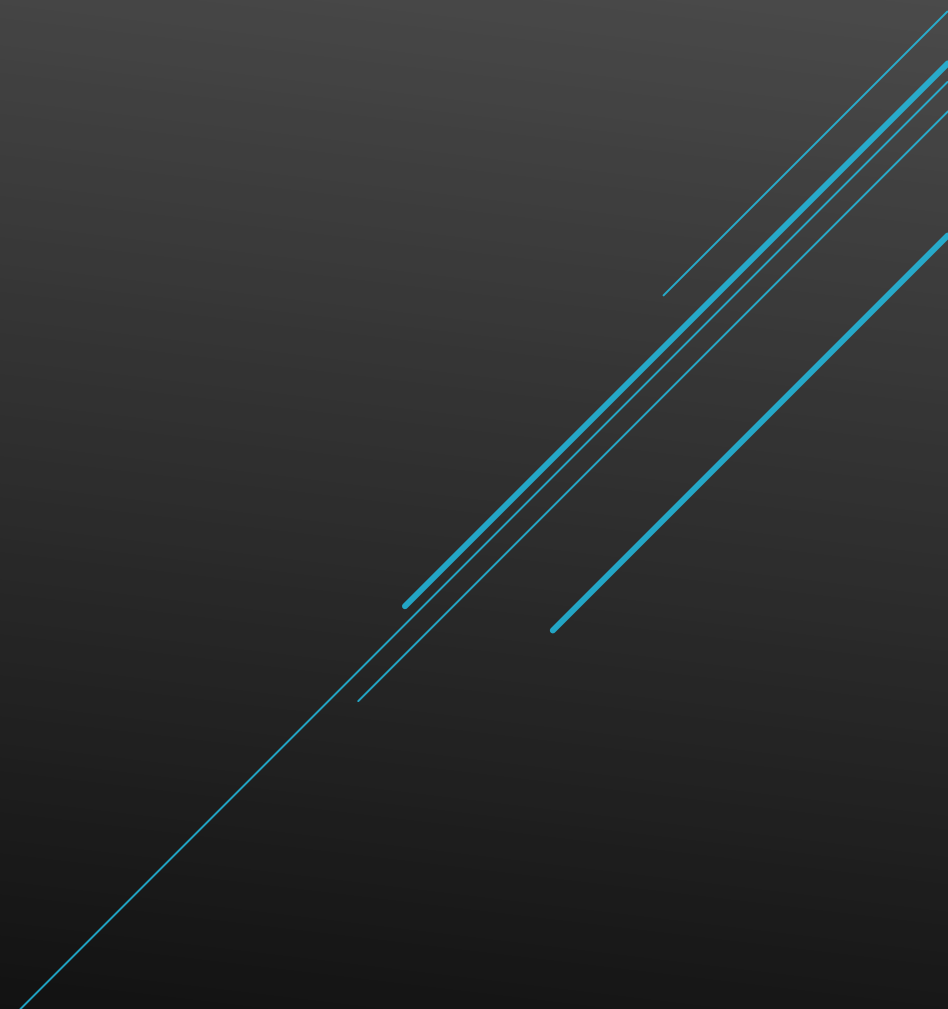
<https://gchq.github.io/CyberChef/>



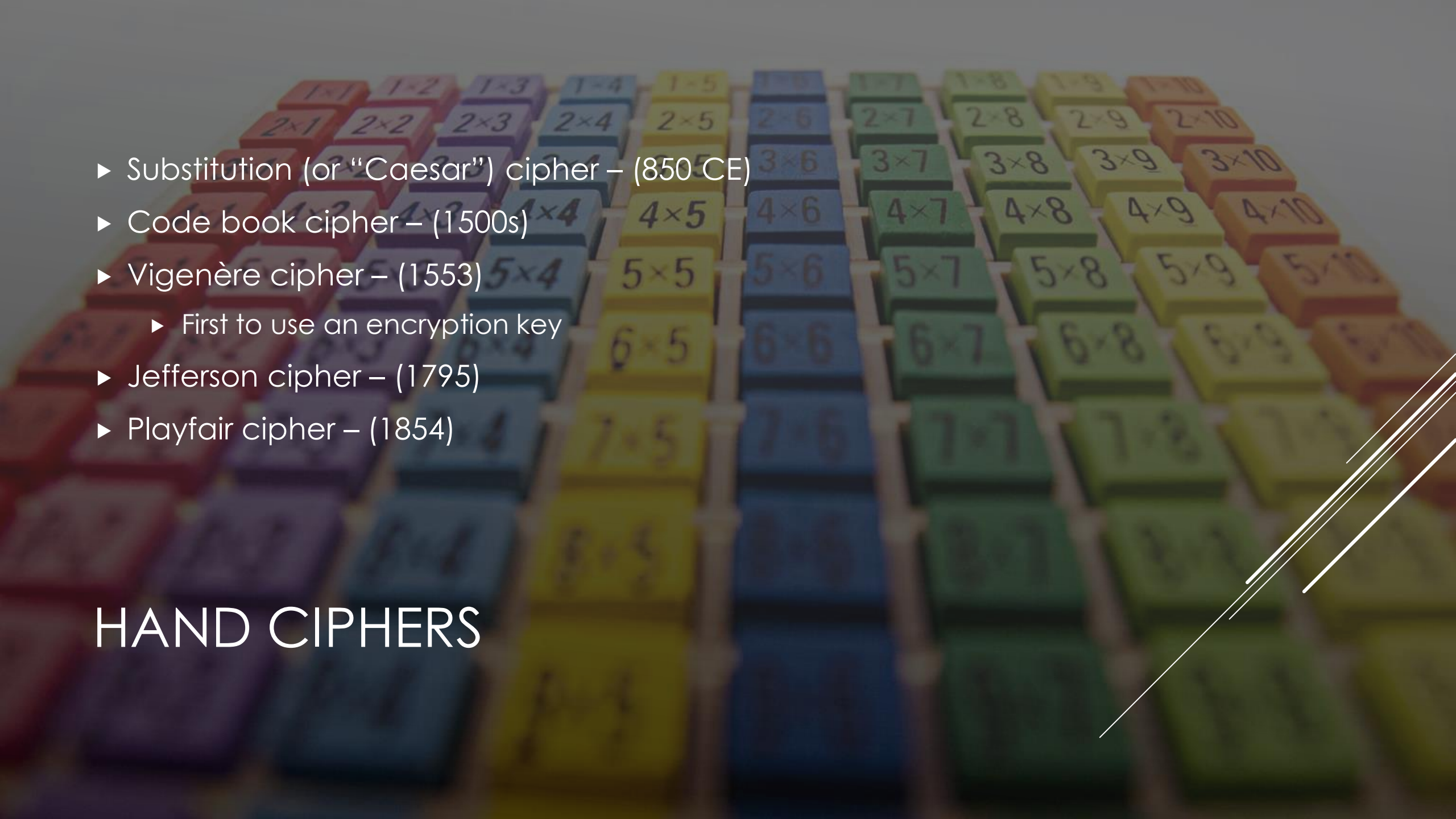
# WHAT IS ENCRYPTION?



# ENCRYPTION HISTORY

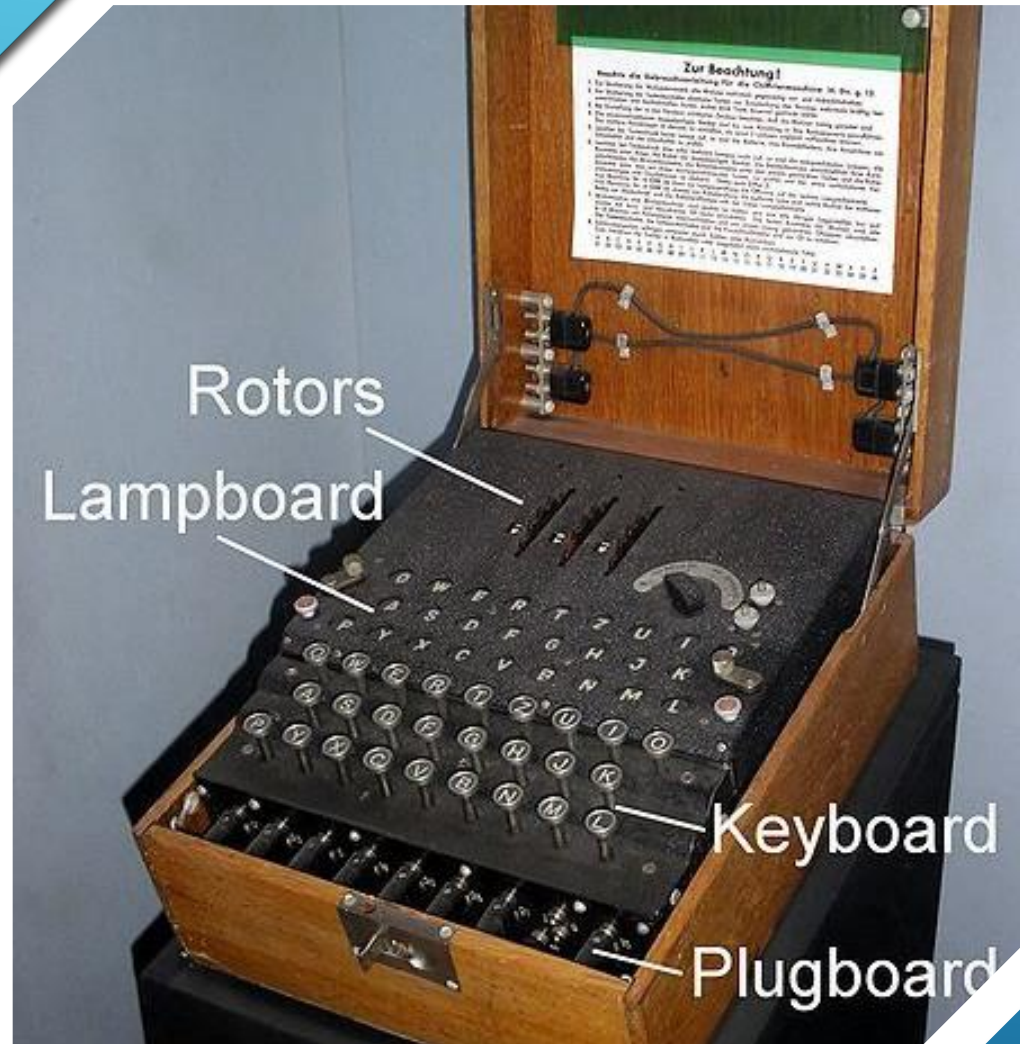




- 
- ▶ Substitution (or “Caesar”) cipher – (850 CE)
  - ▶ Code book cipher – (1500s)
  - ▶ Vigenère cipher – (1553)
    - ▶ First to use an encryption key
  - ▶ Jefferson cipher – (1795)
  - ▶ Playfair cipher – (1854)

# HAND CIPHERS

# WARTIME CRYPTOGRAPHY



MESSAGE HELLOWORLD

UNENCRYPTED LETTER

UKW

3rd Wheel

2nd Wheel

1st Wheel

ETW

STECKER

Index 6

Index 24

Index 10

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

18  
20  
14  
12  
7  
21  
16  
24  
17  
3  
5  
10  
13  
2  
19  
11  
4  
25  
15  
9  
6  
8  
26  
23  
22  
1

X

9  
22  
19  
1  
10  
16  
3  
26  
23  
18  
12  
6  
2  
4  
11  
15  
20  
25  
21  
17  
7  
5  
14  
8  
24  
13

X

26  
2  
5  
3  
11  
13  
20  
8  
24  
19  
12  
18  
9  
14  
17  
15  
10  
21  
23  
25  
7  
1  
4  
6  
16  
22

X

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

ENCRPYTED

ENCRYPTED LETTER #N/A



10 MINUTE BREAK

Three parallel white lines of varying lengths are positioned in the bottom right corner of the slide, angled upwards from left to right.



# PASSWORD CRACKING

A black and white photograph of a woman in a dark dress operating a large, complex mechanical cipher machine. The machine is composed of several tall metal cabinets filled with numerous rotors and electrical components. The woman is leaning over the machine, adjusting one of the rotors. The background shows more of the machine's structure and some cables. The overall tone is historical and technical.

# ONE-TIME PADS





# VENONA PROJECT



WHY DO WE ENCRYPT?





The background is a vibrant blue with various abstract patterns. There are large, irregular organic shapes in different shades of blue. Some areas have a fine dotted pattern, while others have a pattern of small white plus signs. On the right side, there are several parallel white diagonal lines. Small, light blue wavy lines are scattered throughout the composition.

WHAT DO WE ENCRYPT?

HOW DO WE  
ENCRYPT TODAY?

A series of several thin, white, parallel diagonal lines extending from the bottom right corner towards the center of the slide.

- ▶ 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

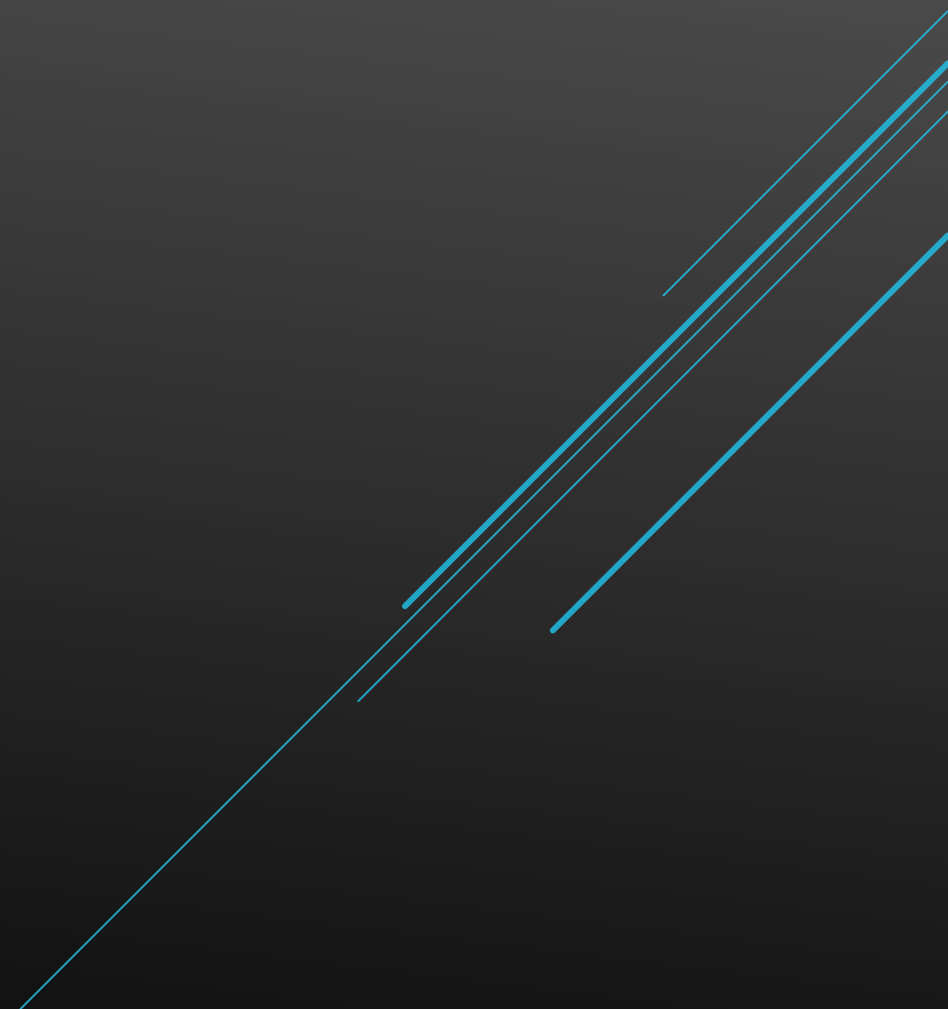
KEYSPACE/KEYLENGTH/KEYSIZE

A series of several parallel white lines of varying lengths and slopes, located in the bottom right corner of the slide, creating a modern, abstract graphic element.



# 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 AT REST

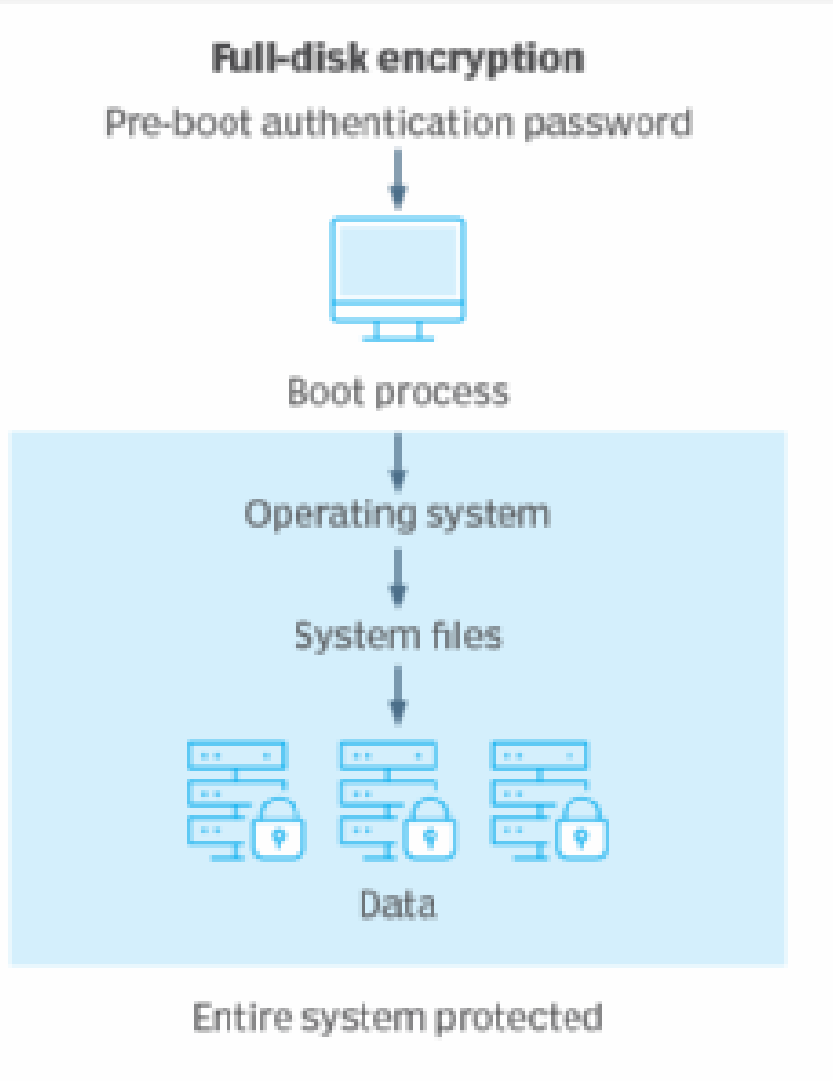


## DATA IN TRANSIT



# DATA SECURITY

# How the FDE process works



# FULL DISK ENCRYPTION





# SYMMETRIC KEY ENCRYPTION



# Symmetric encryption



**Secret key**



# ASYMMETRIC KEY ENCRYPTION

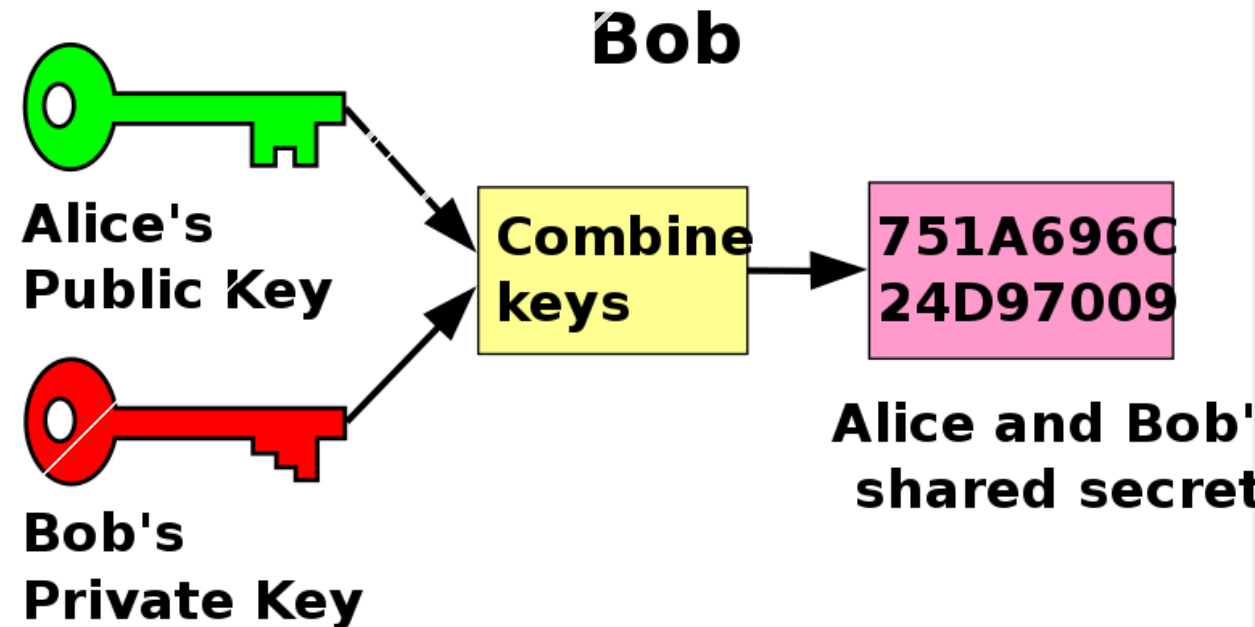
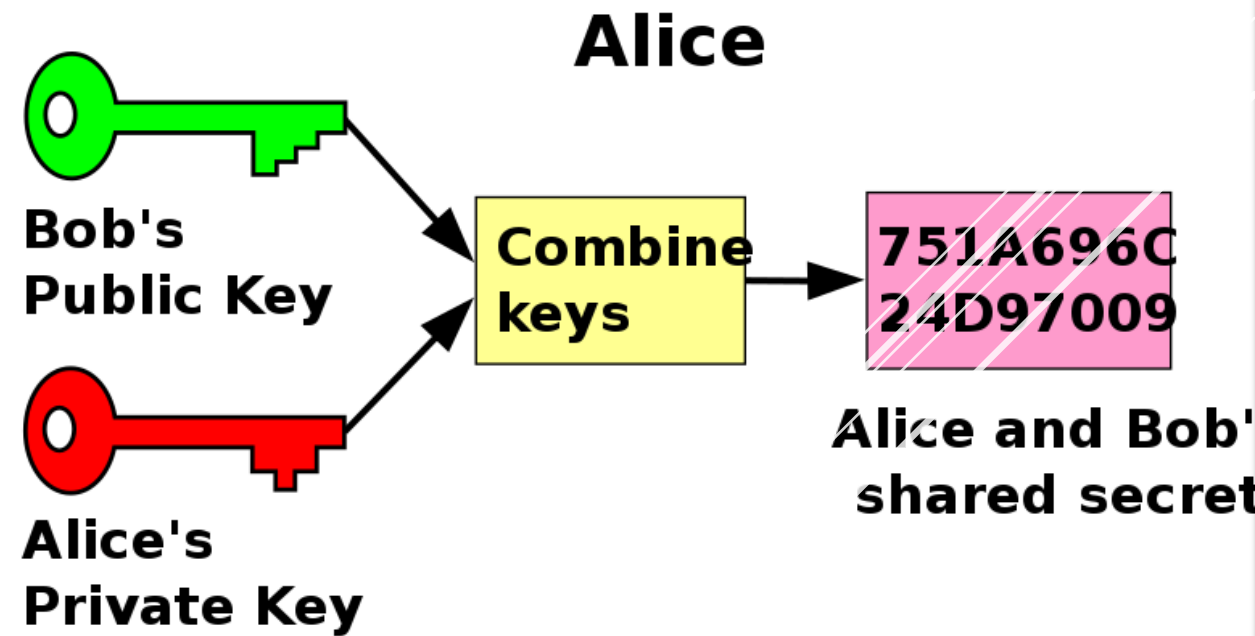




# SECURE KEY EXCHANGE?



# PUBLIC KEY CRYPTOGRAPHY



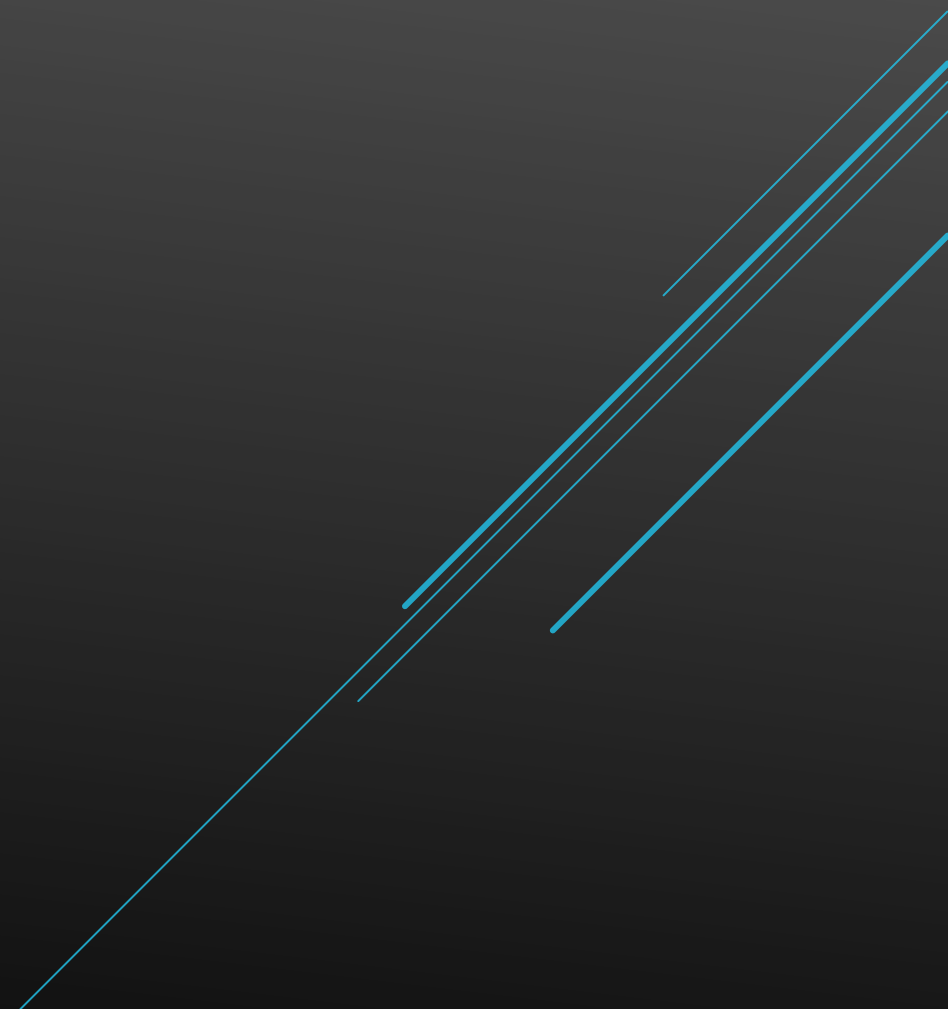




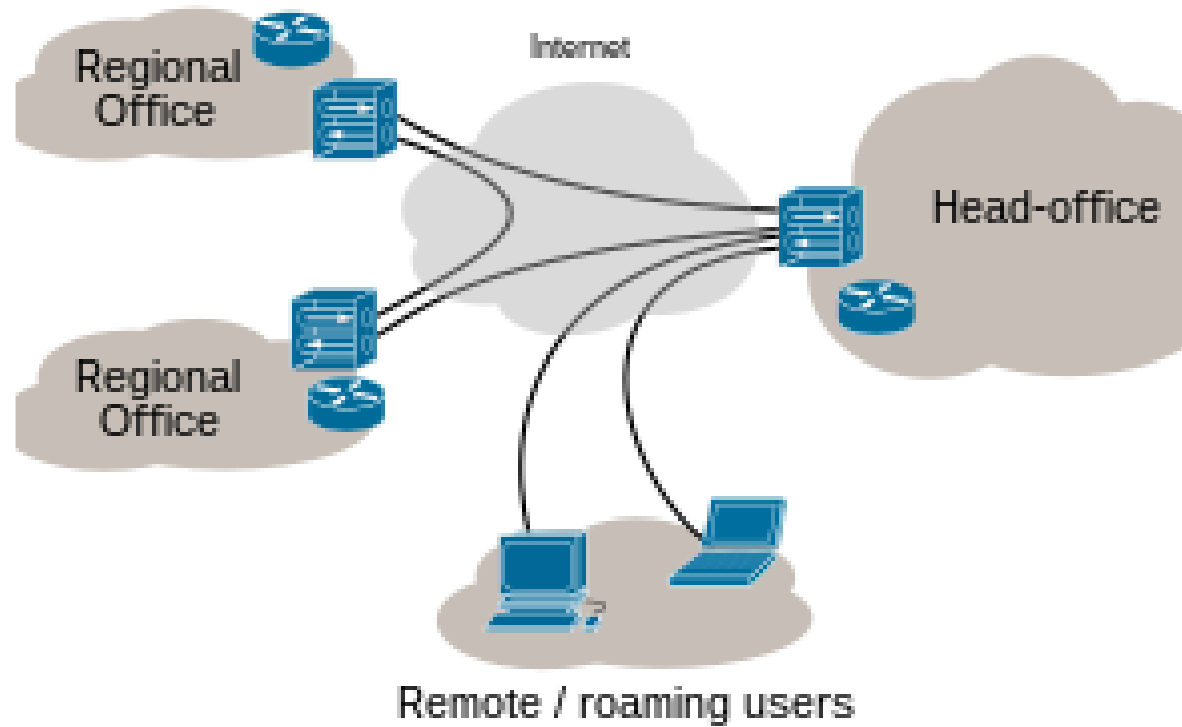
10 MINUTE BREAK

Three parallel white lines of varying lengths are positioned in the bottom right corner of the image, slanted diagonally upwards from left to right.

# SECURING NETWORK CONNECTIONS IN PRACTICE



## Internet VPN

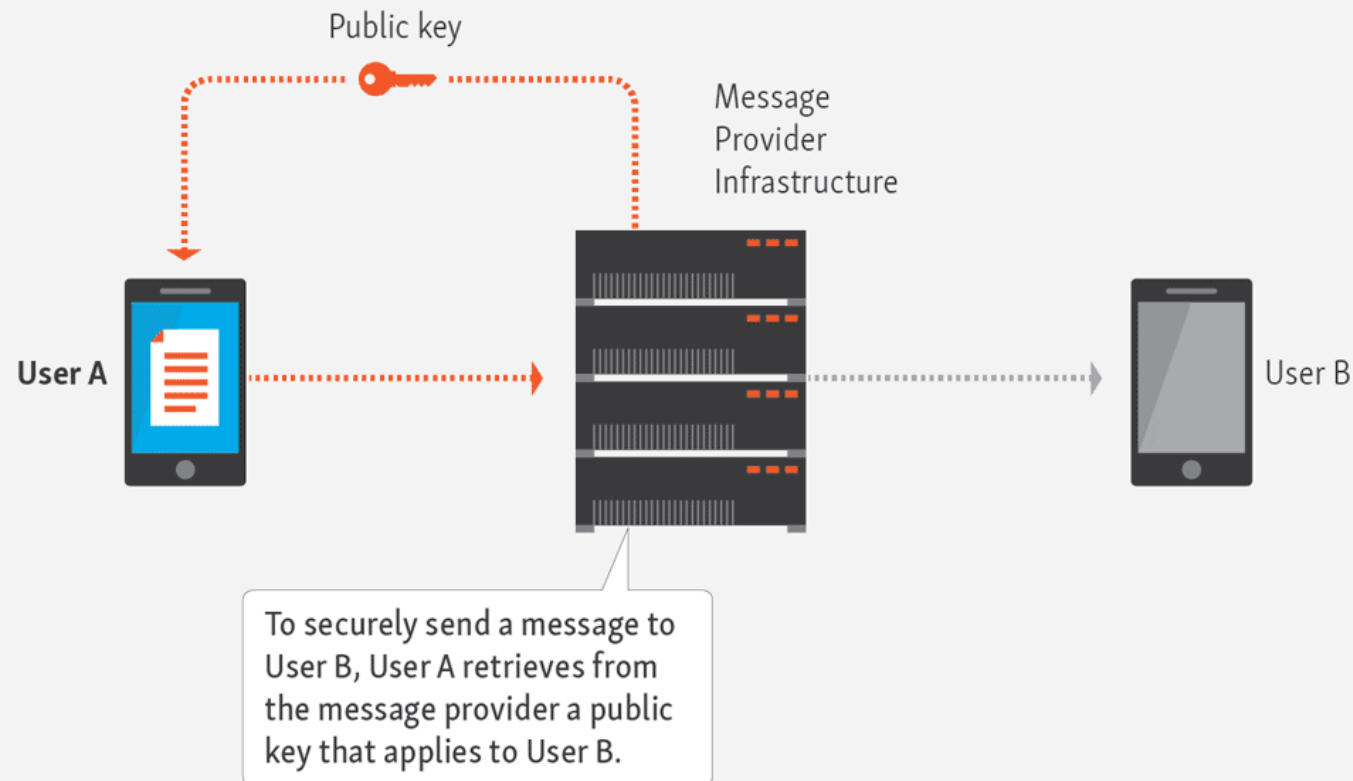


# VIRTUAL PRIVATE NETWORKS

# THIS IS HOW END-TO-END ENCRYPTION WORKS

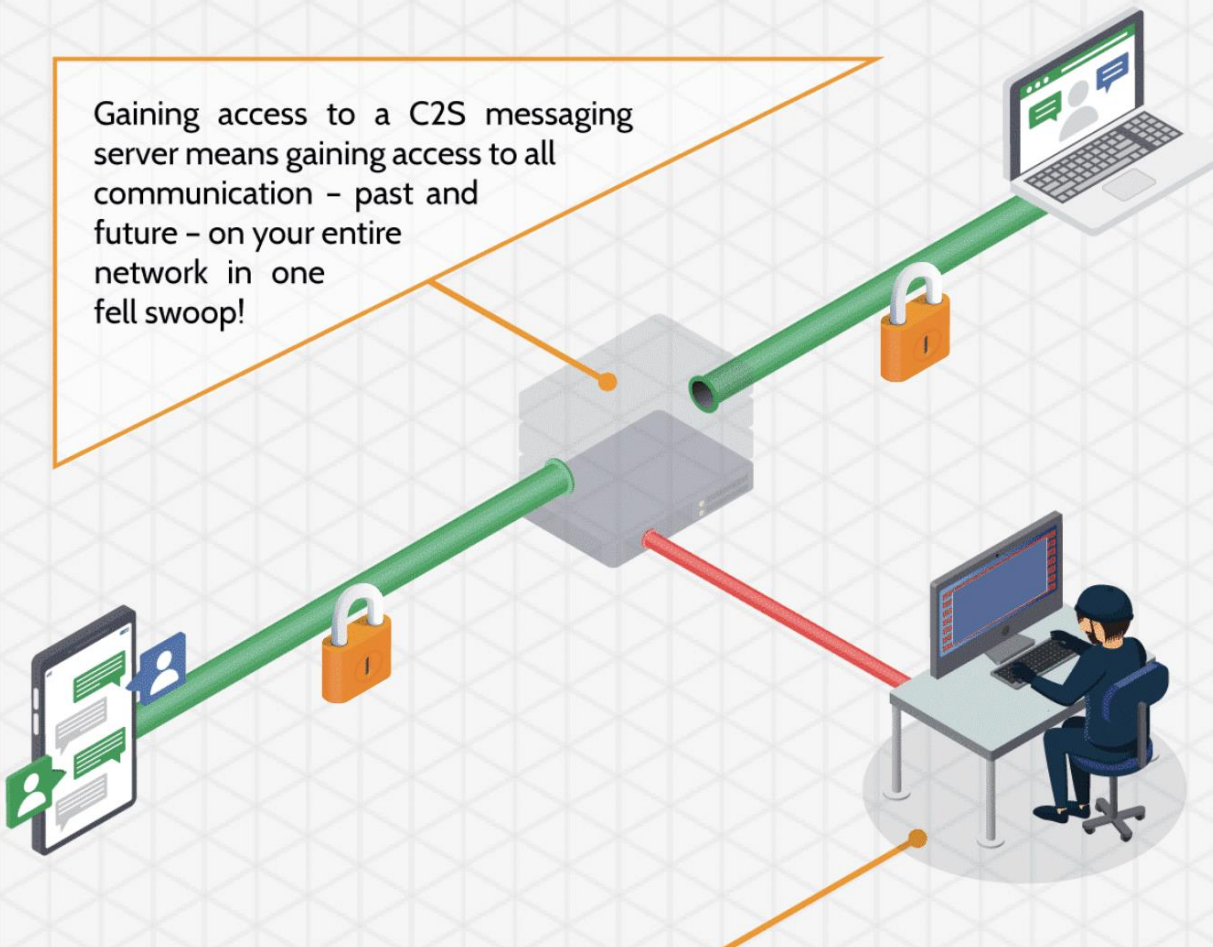


A major selling point for instant-messaging providers is some form of content encryption. But does this technology fully protect your privacy?



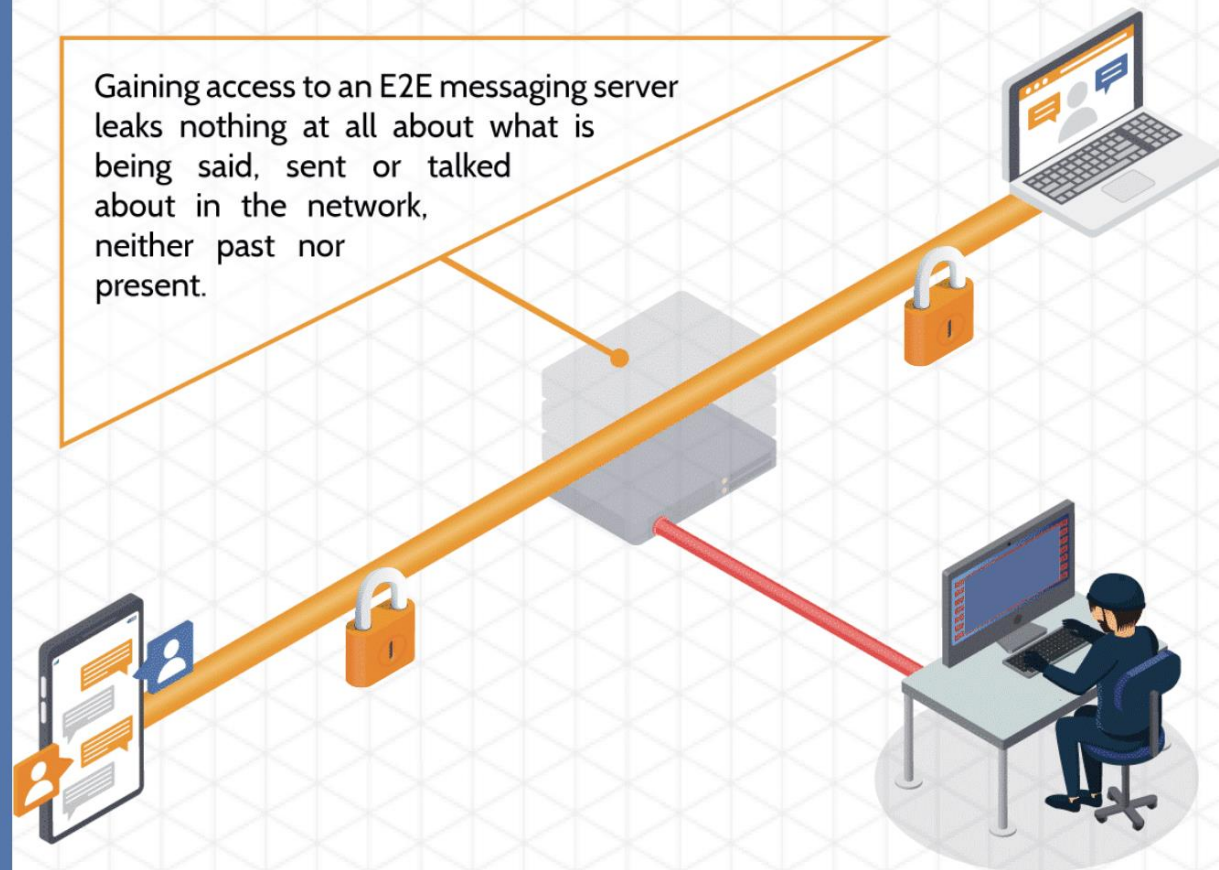
## CLIENT-TO-SERVER ENCRYPTION

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?



Provides trust



Allows a secure connection



Encrypts data



HTTPS

# WHAT DOES A SECURITY CERTIFICATE DO?

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

## CERTIFICATE AUTHORITIES



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



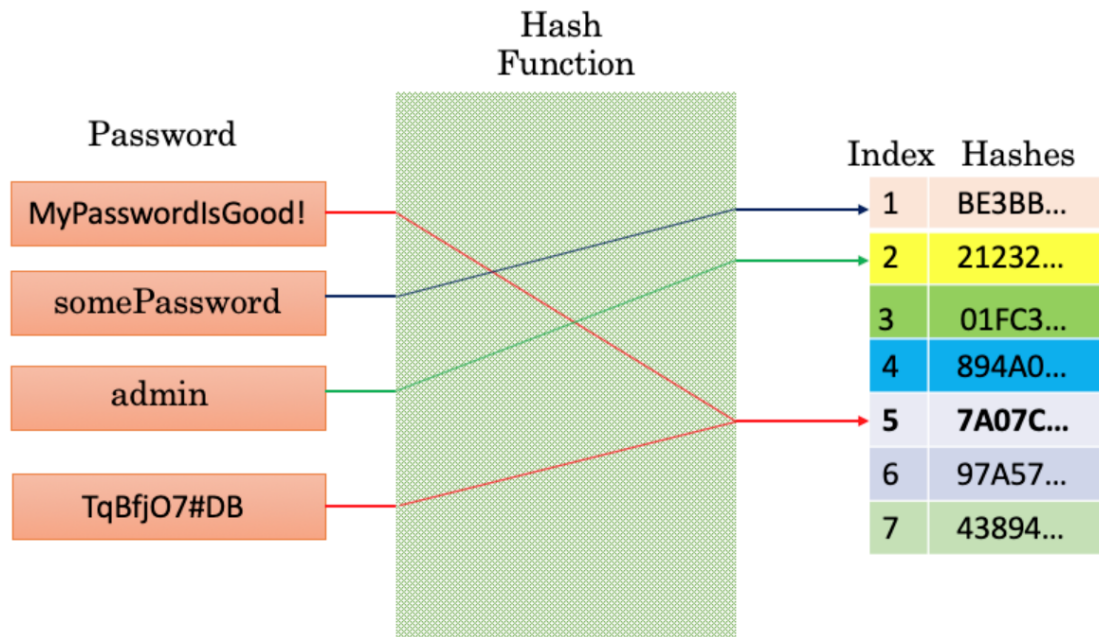
# AUDIT YOUR FAVORITE WEBSITE!

<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



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

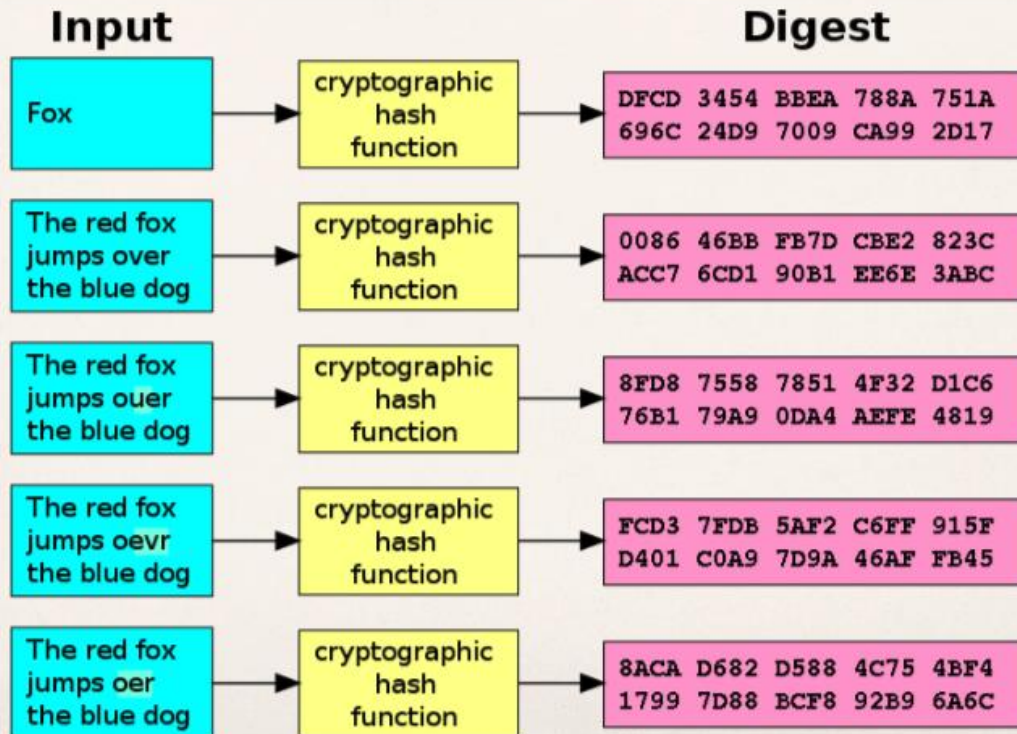
Master Key      : 98 8A F1 3B 6F 4B 4F 8B 98 6F 6B 22 C6 E5 70 0C
                  85 C4 08 89 78 59 B6 6D D3 F5 BD 86 B4 C9 5B B3

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 7F F9 CA B1 4E 20 32 73 4A 56 0F 08
```

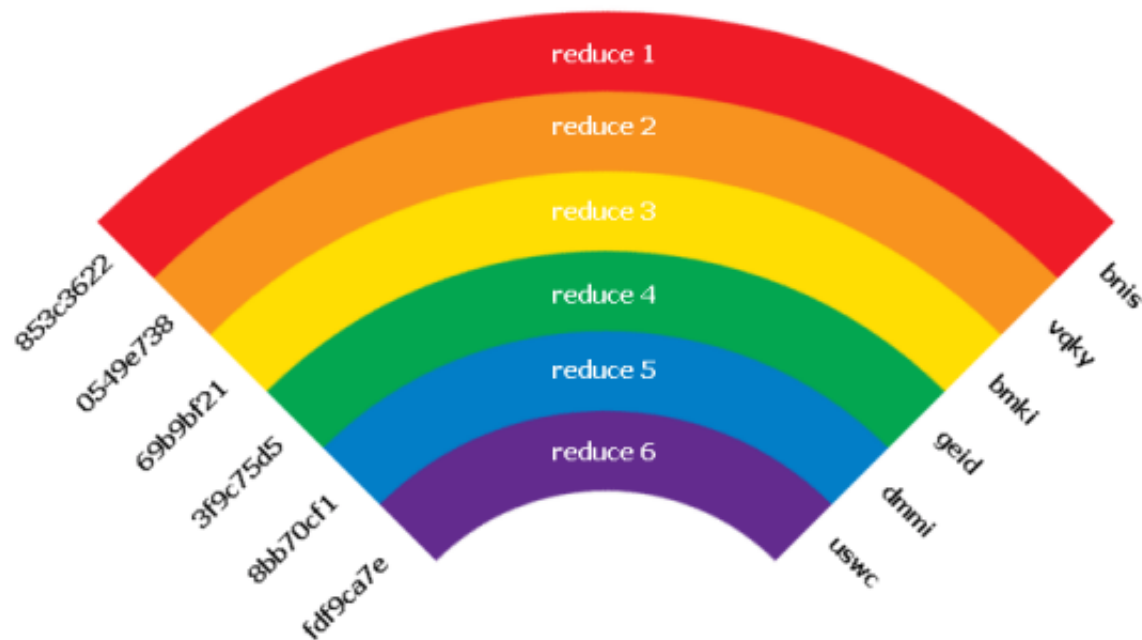
# REAL-LIFE PASSWORD CRACKING



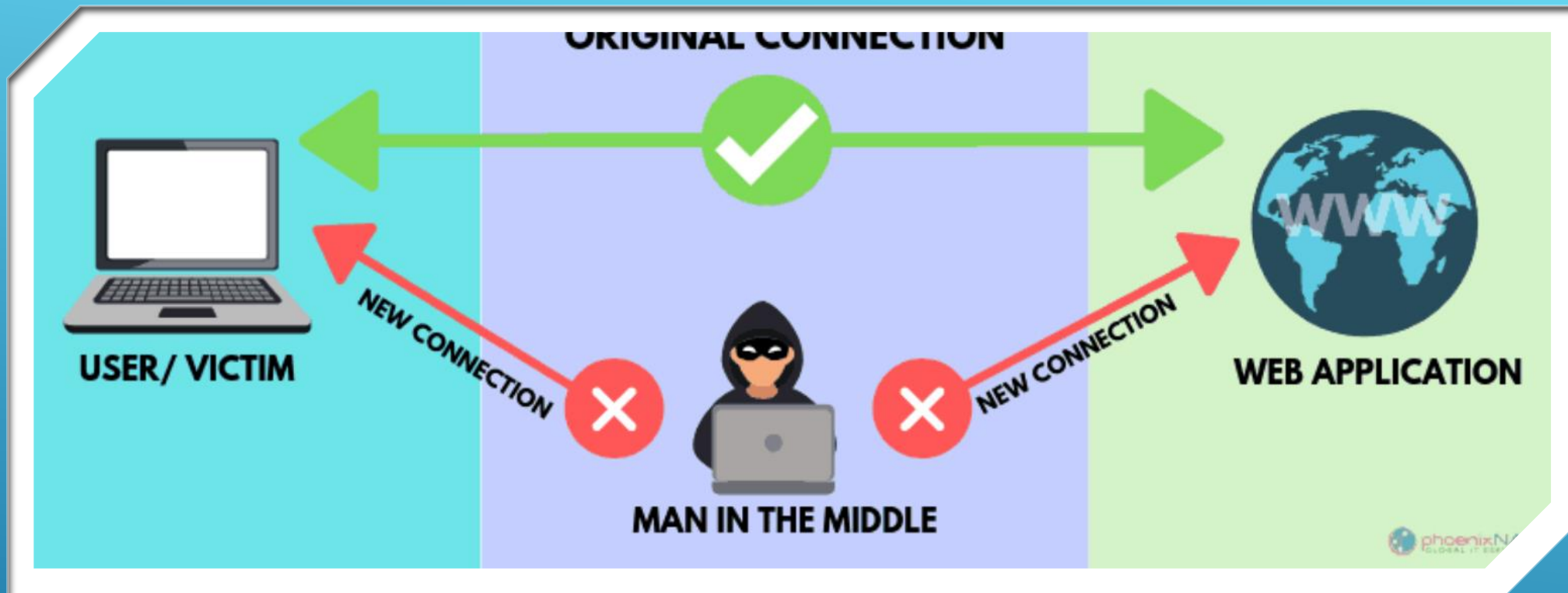
# What is a Hash?



# RAINBOW TABLES



# RAINBOW TABLES CONT'



# 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://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

# 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