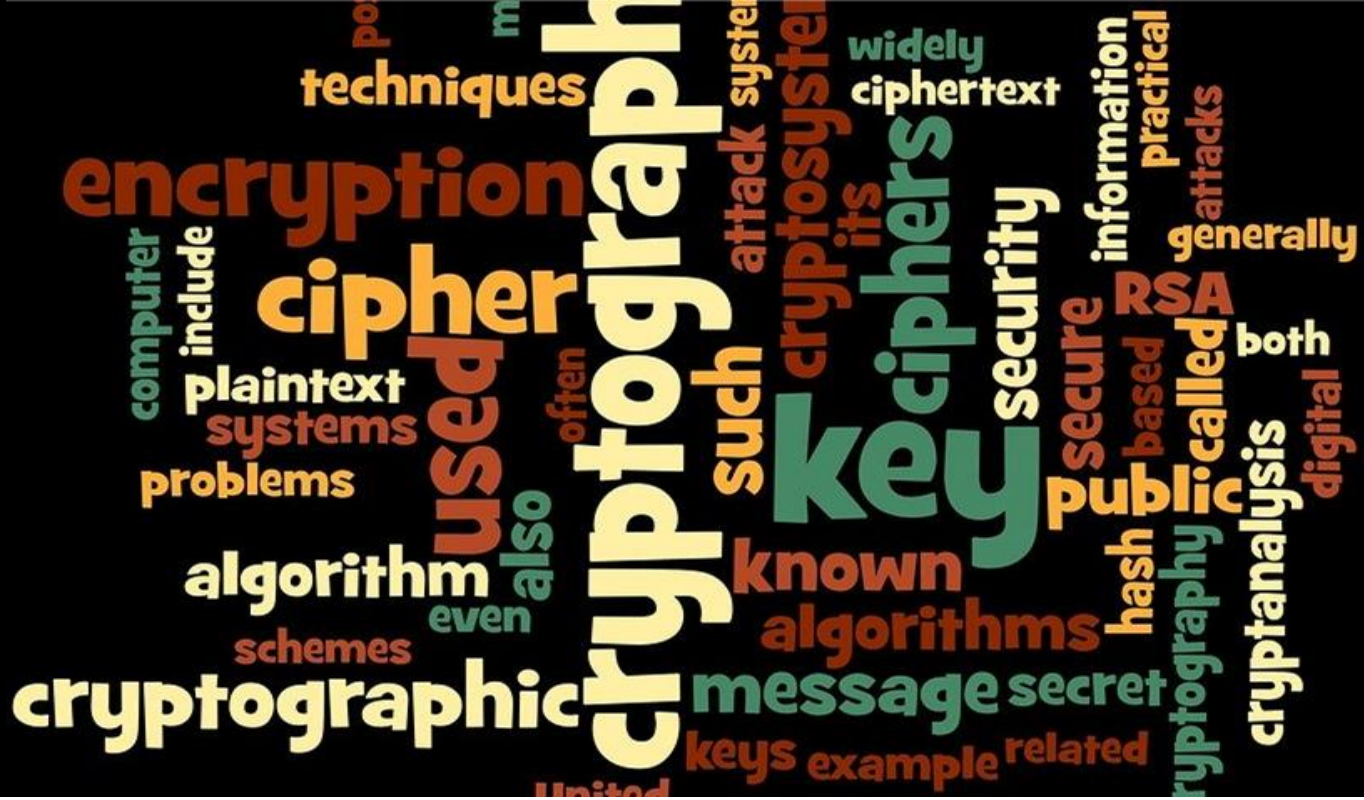
WARMUP



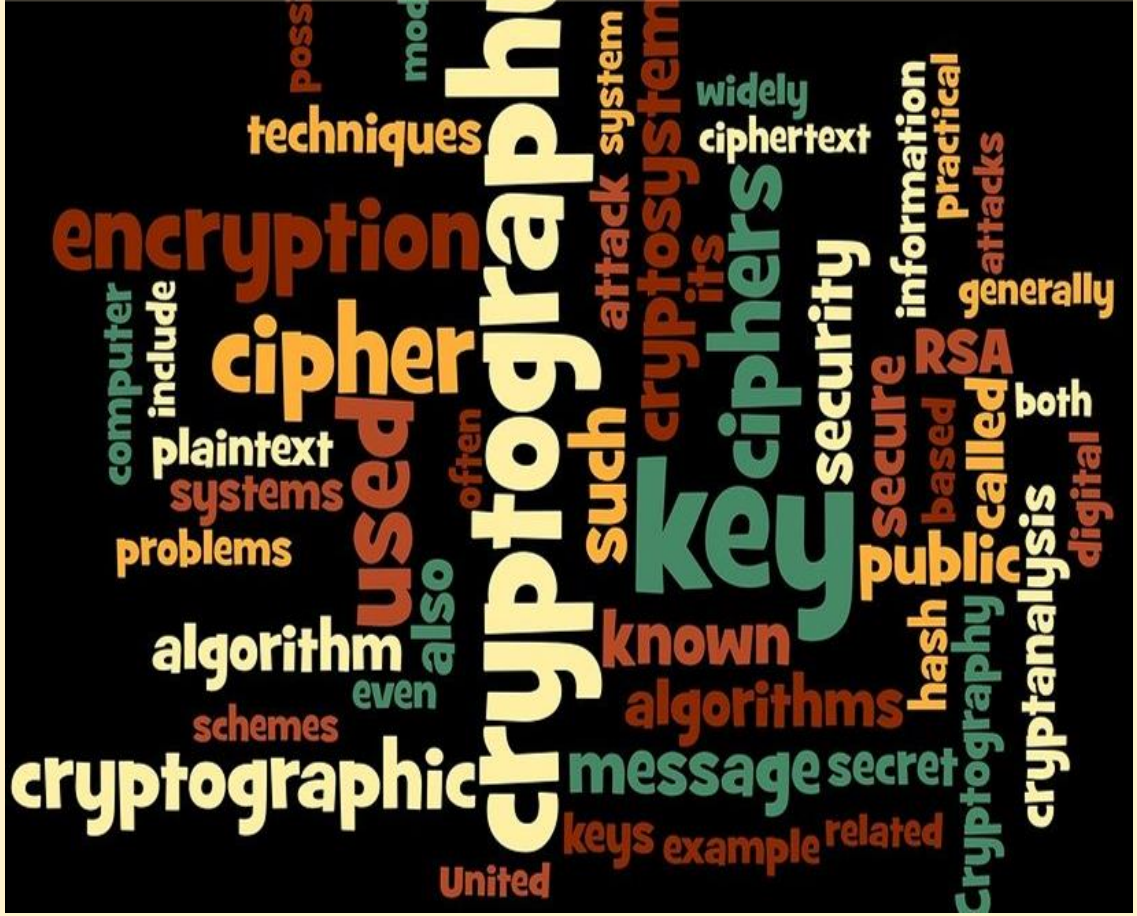
WARMUP

What does this message say?

G T Y O R J O T E O U I A B G T

Hint: Count the letters and try splitting the letters up into groups.

Brainteasers: https://www.braingle.com/brainteasers/22072/caesar-box.html



Data Encryption Awareness

- Michael Lieber (Lockport Schools)
- Suprabha Malhar-Jain (Oyster Bay Schools)

Lesson Title: Data Encryption Awareness
Grade Level: 7 - 12

Learning Objectives Outcomes :
6-8CY 4 , 9-12 CY 4, 6-8DL 5, 9-12 DL 5, 6-8 CY 1, 9-12 CY 1, 6-8 NDS 5, 9-12 NDS 5. Students will understand the vulnerabilities of the internet and how they came to be. Students will practice the use of encryption and decryption methods. Students will gain experience in coding, cracking passwords, social engineering and network attacks.

Facilitation of Learning: Warm up Cryptogram, slides, video, questions, discussion. Closure/Review is Edpuzzle video w/questions.

Summary: This lesson can be done in 15 minutes or 3 days depending on how much time students spend on Khan academy and Nova Labs. The information lends itself to the "big Picture" of how encryption works and the importance of it. Students will get a lot out of the Nova Labs and Khan academy.

Learning Types: Presentation, Observation, Oral Questioning, Problem Solving, Interactive Virtual models.

Materials List: Computer, Meet Software, Slides, Links to Khan Academy and Nova Labs, Nearpod

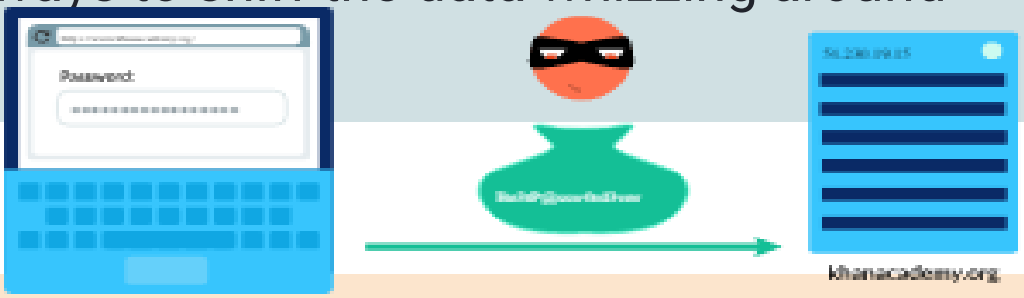
Accomodations: More time can be given to students that need it. Repeat any section. Captions can be used and changed to different languages.

Description of Activity:

- Students will complete the warm up share with class.
- Then students will read/watch the content and discuss/answer questions.
- Students will then spend time using Khan Academy and Nova Labs to solve puzzles.
- Students with then review the content by completing the edpuzzle.
  - Symmetric encryption | AP CSP (article) | Khan Academy
    a. Complete/Answer the questions
    b. Public Key Encryption
  - https://www.pbs.org/wgbh/nova/labs/
  - https://centralops.net/co/

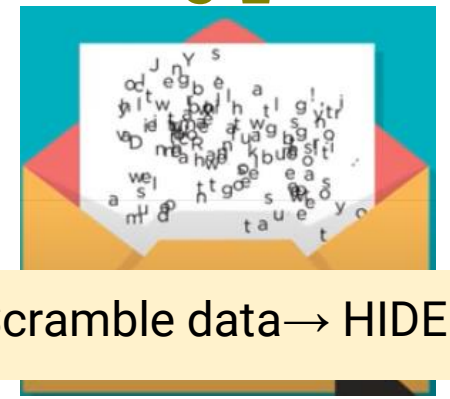
How Do Computers Send Private Data?

- TCP/IP protocols send private/sensitive data in packets on the same routes over the internet as other data
- Cybercriminals also formulate ways to sniff the data whizzing around the Internet.

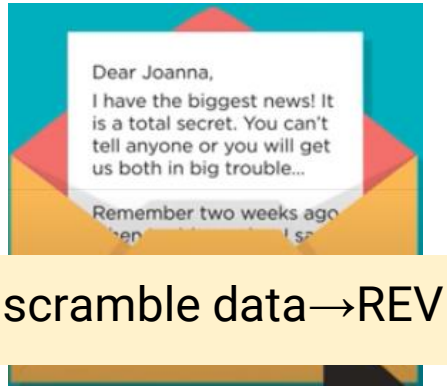


- **Encryption**: scramble the original data to hide the meaning of the text, while still making it possible for the data to be unscrambled using a secret key.
- Encryption enables two people (or computers!) to share private info over open networks
- TLS protocol adds a layer of encryption on top of TCP/IP, using both **symmetric and public key encryption** to send private data around the Internet.

Encryption ← → Decryption



Scramble data→ HIDE it



Unscramble data→REVEAL

Caesar Cipher Encryption

Simple substitution cipher which replaces each original letter with a different letter in the alphabet by shifting alphabet by a certain amount.

Caesar Cipher Decryption

Caesar always used a shift of 3 to DECODE the message.

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
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

Every letter shifts 6 letters over

SECRET MEETING AT THE PALACE → YKIXKZ SKKZOTM GZ ZNK VGRGIK

Encrypted Message for: Shift 6 -letters over ALEXANDRIA SOON **GRKDGTJXOG YUUT**

Vigenere Cipher

Is a polyalphabetic cipher. It Uses an **entire word as the shift key,** as opposed to Caesar Cipher's single shift amount. French cryptologists invented in mid-1500s.

1. Repeat the shift key to line up with each of the letters in the phrase
2. Replace each letter of the original text according to the Vigenère table:

Original	V	E	R	S	A	I	L	L	E	S
Shift key	C	H	E	E	S	E	C	H	E	E
Encrypted	X	L	?	?	?	?	?	?	?	?

Encryption:
Select the row that starts with "V"
Move to the column that has a header of "C"
Letter at the intersection of "V" row and "C" column is "X"

Encrypted	N	V	Y	Z	J	I
Shift key	C	H	E	E	S	E
Original	L	O	?	?	?	?

Decryption:
Select the row for the first letter in the shift key "C".
Move down that row until first encrypted letter "N"
Look up to see header of that column as "L"

	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

Cracking the Cipher

Three techniques are used to "**crack**" the cipher **without** knowing the **shift**.

1. **Frequency Analysis**

analyze frequency of characters in the message and identify the most likely “E” and narrow possible shift amounts

1. **Known plain text**

Messages tend to start with similar beginnings. In WWII, messages always started with weather report,

1. **Brute Force**

Only 25 possible shifts (not 26 — why not?). The enemy could take some time to try out each of them and find one that yielded a sensible message. Attacker submits many passwords or passphrases with the hope of eventually guessing correctly.

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
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

Send Private Data → Encryption

Modern Ciphers RSA

RSA-Cipher: (**R**ivest **S**hamir **A**dleman)

Easy: $m^e \bmod N \rightarrow c$

Hard: given $(e,N) \rightarrow m$

- Asymmetric key algorithm $m^e \bmod N \rightarrow c$
- Based on a one-way function -- i.e., a function that is easy in one direction and hard in the other.
- TLS key exchanges for connecting to a secure HTTPS website.
- Uses 2 different keys (Public key and Private key) for encryption and decryption.
  - Public key open and available to all, used for public encryption
  - Private key is possessed by owner; authentication of owner's Digital Signatures
  - RSA's strength and weaknesses lies in the factoring large integers

$m^{ed} \bmod N \rightarrow c$

public modulus

public key

private

m: message (a number)

e: public exponent

d: decryption key

N: public modulus

c: encrypted message

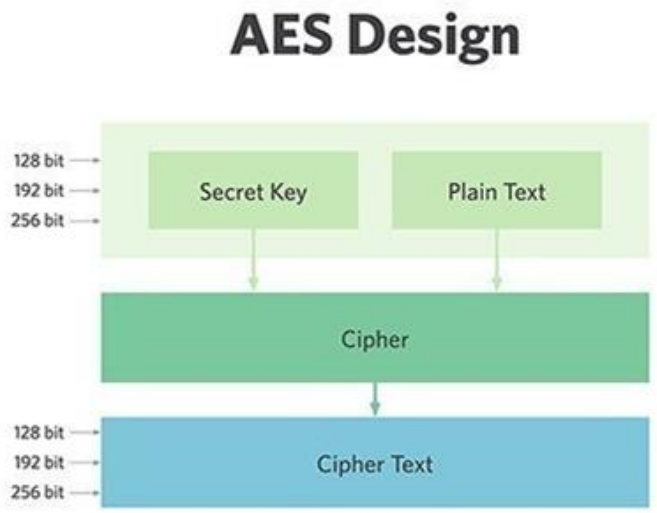
Modern Ciphers

AES-128: Advanced Encryption Standard

- symmetric key algorithm, also known by its original name Rijndael .
- Uses same key for encryption and decryption
- is a block cipher approved by the federal government and is often used for secure file transfer.
- less computational power, “1000 times faster” than asymmetric ones

AES includes three block ciphers: AES-128, AES-192 and AES-256.

- 128-bit key length to encrypt and decrypt a block of messages
- data divided into chunks of fixed length data(128 bits). Chunks are processed where each round is dependent on output of its predecessor.
- AES-192 uses a 192-bit key length and
- AES-256 a 256-bit key length to encrypt and decrypt messages.



Why is AES -128 More Secure?

1. Each key is always 128 bits long i.e. 2^{128} possibilities = 340 x 10^{36} keys 340,000,000,000,000,000,000,000,000,000,000,000
2. AES cipher requires applying a sequence of 10 mathematical operations for each bit of the key. Multiply that number above by 10, and that's the number of calculations a computer would need to do.
3. The fastest computer can calculate around 145 x10^{15}. The fastest computer would still take **500 trillion years** to try every possible 128-bit key!
4. Frequency analysis, won't work: AES cipher has the multi-step sequence of operations on blocks of bits, which does not reveal any information about the original text.

Use of strong passwords, password managers, multifactor authentication (MFA), firewalls and antivirus software is critical to enterprise security.

PBS NOVA LABS IS A GREAT TOOL FOR STUDENTS TO LEARN ABOUT CYBERSECURITY.

THERE ARE 4 MAJOR CHALLENGES :

CODING

PASSWORD CRACKING

SOCIAL ENGINEERING

NETWORK ATTACKS

GAME PLAY LEARNING. 75 MINUTES

https://www.pbs.org/wgbh/nova/labs/
https://centralops.net/co/
https://openspeedtest.com/?ref=logo

The EdPuzzle is designed for review of the "Big Picture"

https://edpuzzle.com/media/5f2bf8df7ec5741ea2a423dd

Thank You for your time and attention.

We hope you enjoyed our presentation.

We would be happy to answer any questions.

Symmetric Encryption Resources

1) Watch(Required):

a) Most of this lecture material including some images come from PBS Digital Video on Cryptography. https://www.youtube.com/watch?v=jhXCTbFnK8o

a) Answer Questions on Khan Academy

a) How bitcoin works(non technical) https://www.youtube.com/watch?v=l9jOJk30eQs

1) Optional:

a) How RSA works. This is technical with some math but still accessible. https://www.youtube.com/watch?v=wXB-V_Keiu8

b) How bitcoin works under the hood. Technical but still accessible. May need to rewatch, rewind several times. https://www.youtube.com/watch?v=Lx9zgZCMqXE

c) PBS Crash Course in Computer Science. Cryptography. Retrieved from https://www.youtube.com/watch?v=jhXCTbFnK8o

Symmetric Encryption

1. Join KHAN ACADEMY w/CODE: NEK4DD5U
2. The first substitution letters are the letters in the key word "ZESTILY", and the rest of the substitution letters are the remaining letters in the alphabet.
   With this key, how would you encrypt the word "ORANGE"?

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