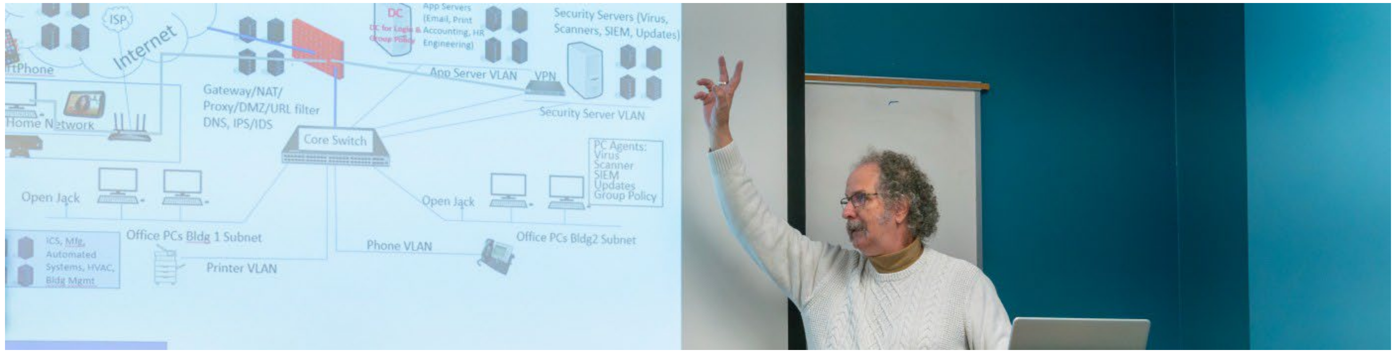
Download slides at
Bhudsoncissp.com



Cyber Encryption. A Hands-on Experience

Presented by Barry Hudson

bhudsoncissp@gmail.com

GCFIV IRGVCTXMSR E LERHW-SR IBTIVMIRGI

TVIWIRXIH FC FEVVC LYHWSR

What is Cyber Encryption

- Encryption is the process of converting readable data into an unreadable format to prevent unauthorized access.
- Plaintext to Ciphertext: Encryption takes original, readable information (plaintext) and uses a mathematical algorithm to scramble it into an unreadable format known as ciphertext.
- Ciphertext to Plaintext: Decryption takes unreadable format and restores it to the original, readable information (plaintext).
- The Role of the Key: The key, coupled with knowledge of the algorithm, enables you to run the process in reverse to decrypt.
- Without the correct key, the ciphertext remains a meaningless jumble of characters to anyone who intercepts it.
- The key must be protected.

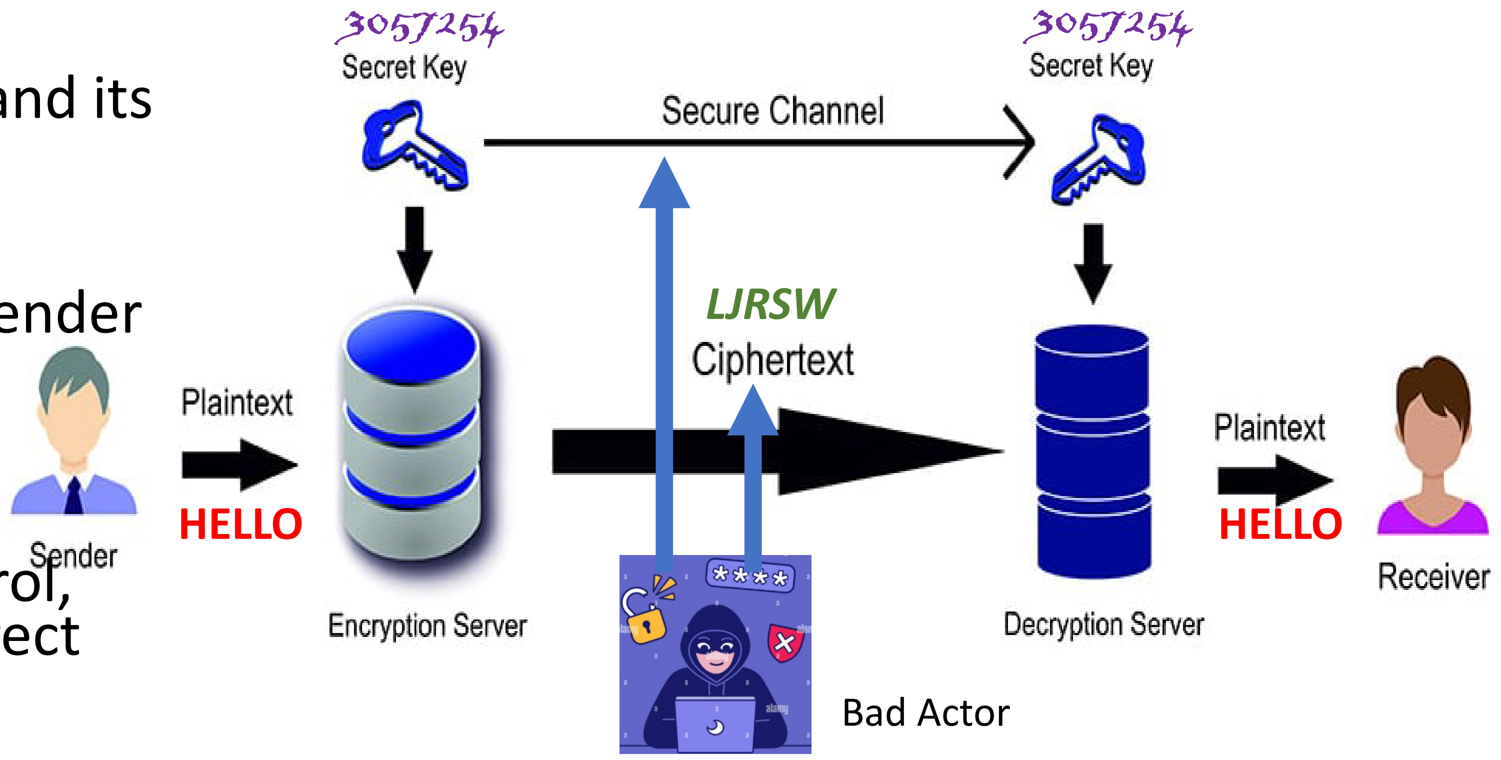
Who, ~~What~~, When Where, Why, and How

Who uses and How Encryption Works

- Sender and Recipient
  (Role can be reversed with the same key)
- Agree on an Encryption Key (and its transmission)
- Using the key & algorithm:

1. Plaintext to Ciphertext by sender
2. Restored to Plaintext by recipient

- Subject to Adversarial Attack
  (If Bad Actor gains some control, they can alter, delete, or redirect the message.)



Symmetric Cryptography

The Key is the sole secret, and must be kept secret.

The biggest problem is getting the keys to the recipient (key exchange)

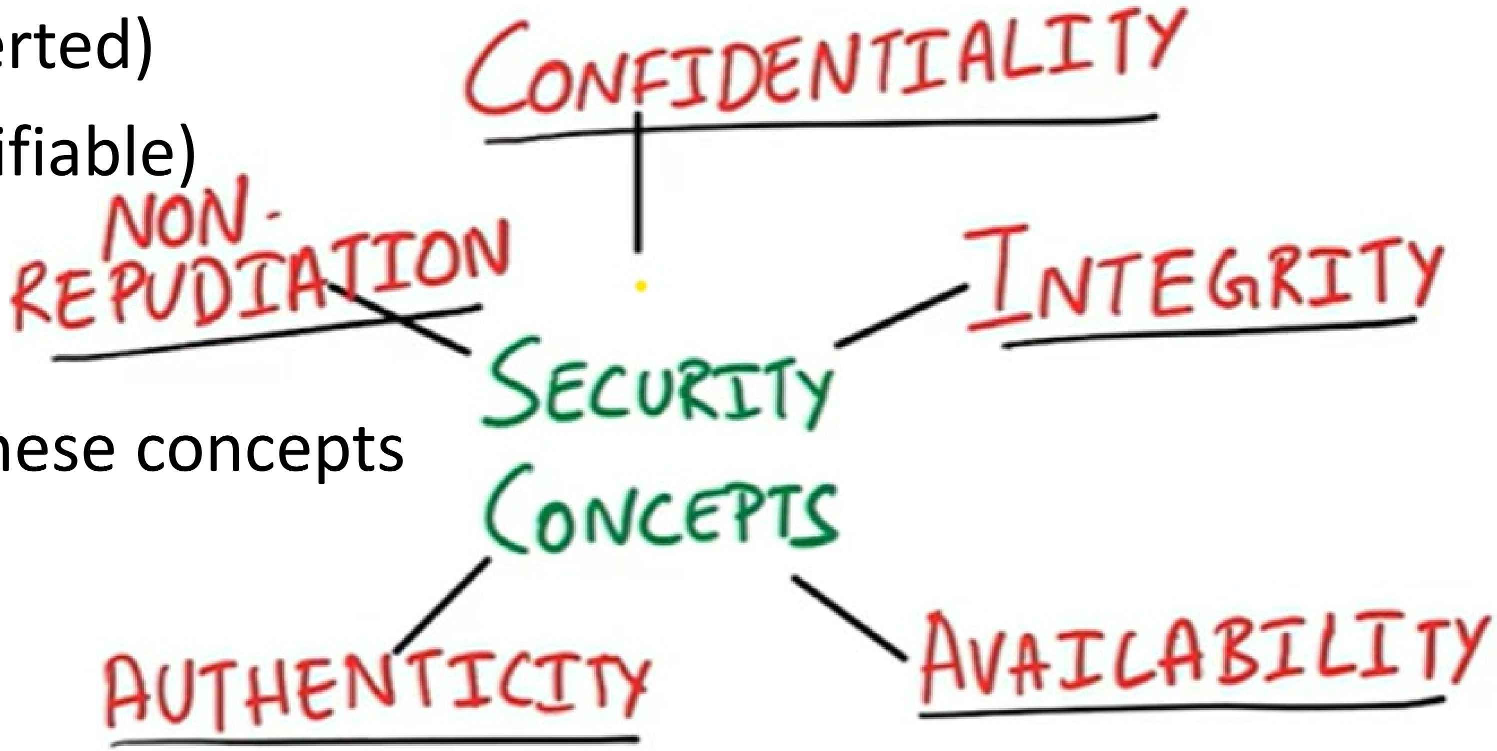
~~Who~~, ~~What~~, When Where, Why, and ~~How~~

Why and When is Encryption Useful

CIA Triad

1
CONFIDENTIALITY
INFORMATION SECURITY
2
INTEGRITY
3
AVAILABILITY

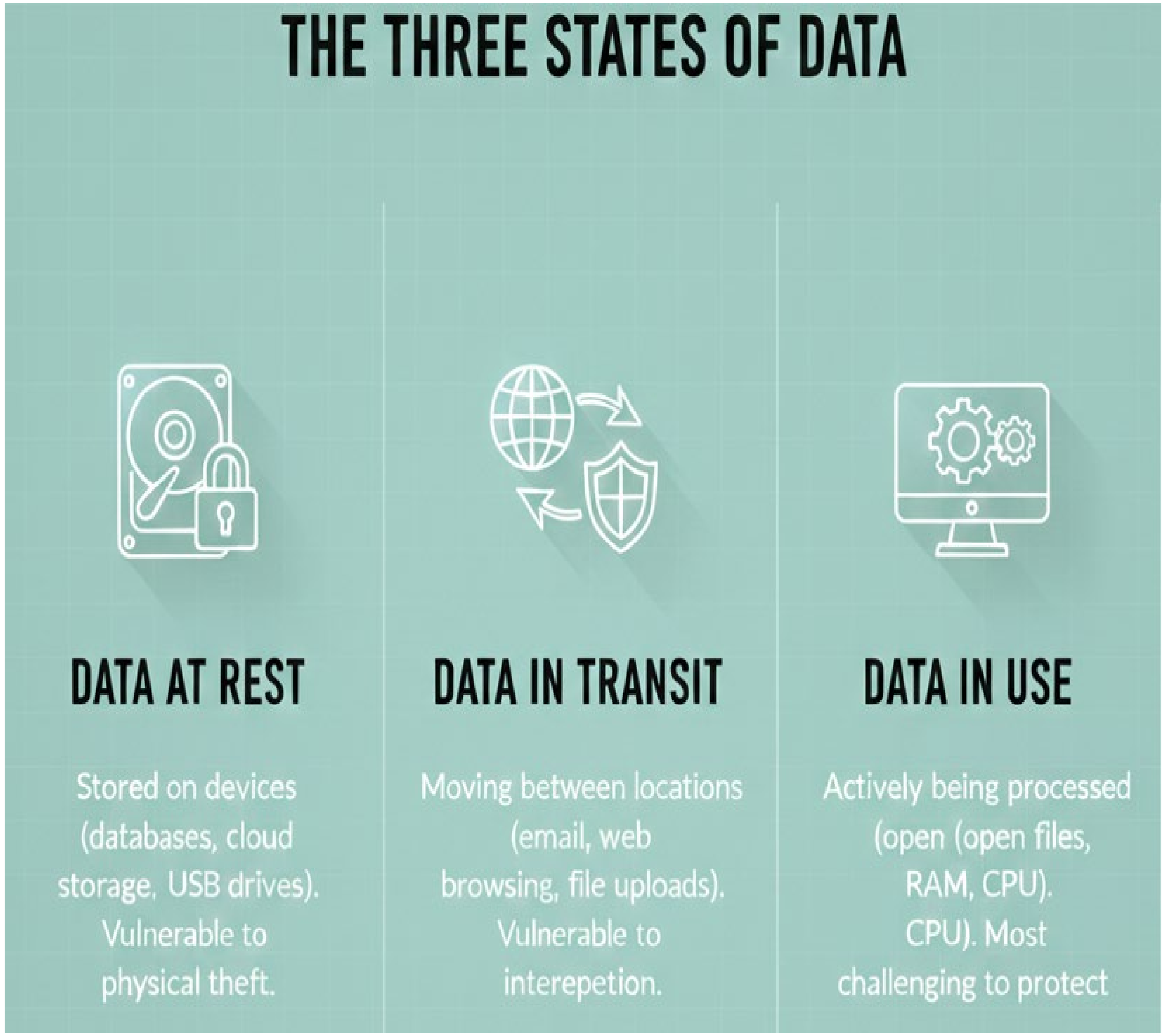
- **Confidentiality** (no snooping or interception)
- **Integrity** of Data (no alteration to data)
- **Availability** (not stolen or diverted)
- Authenticity (genuine and verifiable)
- Non-repudiation (verification of sender)
- Privacy Assured by combing these concepts (averting adversaries)



~~Who~~, ~~What~~, ~~When~~ Where, ~~Why~~, and ~~How~~

Where is Encryption Used

- Data at rest (on your PC, server, phone)
  Vulnerable to physical theft or ransomware
- Data In transit (email, text, Web activity)
  Vulnerable to “man-in-the-middle
- Data in use (being processed)
  Vulnerable to Virus and malware that intercepts and sends to collection points



THE THREE STATES OF DATA

DATA AT REST

Stored on devices (databases, cloud storage, USB drives). Vulnerable to physical theft.

DATA IN TRANSIT

Moving between locations (email, web browsing, file uploads). Vulnerable to interepetion.

DATA IN USE

Actively being processed (open (open files, RAM, CPU). CPU). Most challenging to protect

Introducing the CipherFidget

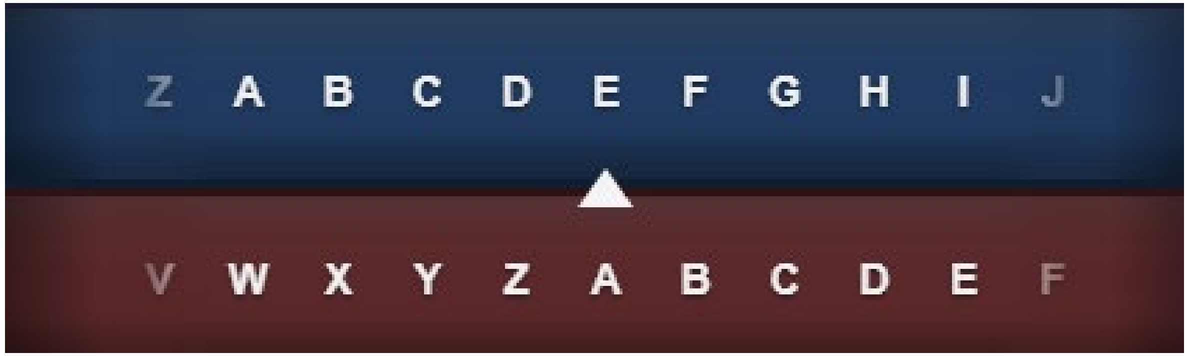
- A tactile “secret decoder ring” paired with interactive lessons.
- Contains 2 alphabetic rings that can be rotated independently.
- Concepts apply to Roman secrets and modern digital encryption.
- https://cipherfidget.com/
- Lessons are available on the website

CipherFidget Lesson 1 The Basic Substitution Cipher

(monoalphabetic symmetric encryption)

- Alphabetic Offset (ROTation) to encrypt HELLO
- Click the alphabet “X” positions to the right and read the letters above H E L L & O
- https://cipherfidget.com/lessons/rot-x

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	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
				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												

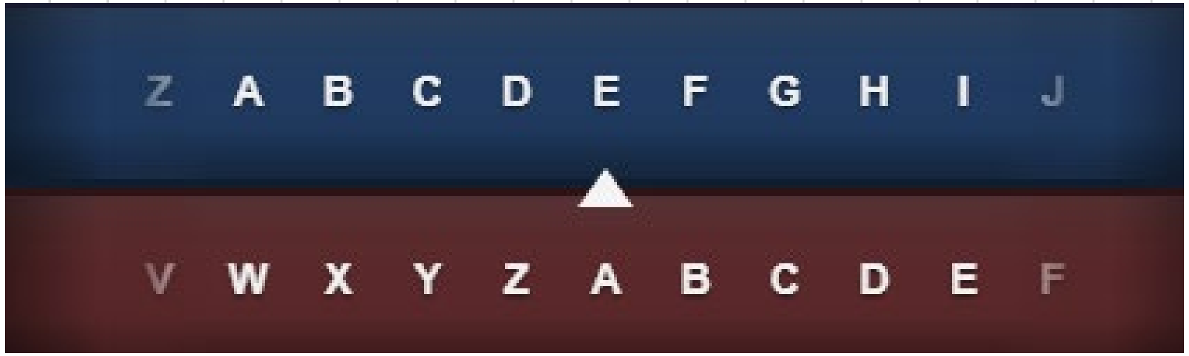


See the Movie
https://www.youtube.com/watch?v=G8svL3REX9o

CipherFidget Lesson 1 Discussion

- Alphabetic Offset (ROTation) to encrypt HELLO
- Notice anything about the encrypted message?
- Besides the double letter, what is the weakness?
- How many combinations are there for the key? (26)

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	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
				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												



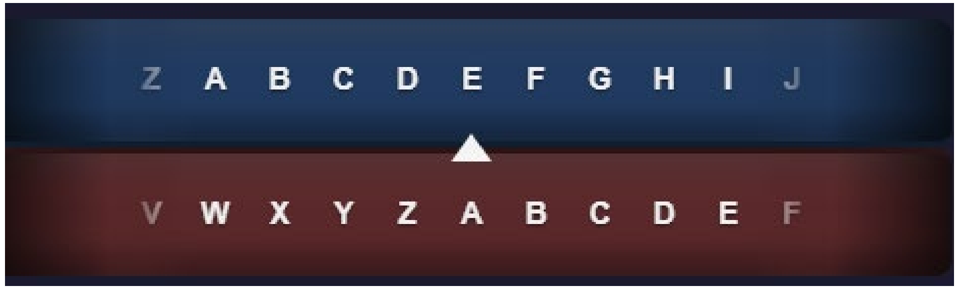
Can you crack this in 2 guesses?

M EQ E QER

CipherFidget Lesson 2

- ROT-X+: Rotating + Shift
- https://cipherfidget.com/lessons/rot-x-plus
- We will use an initial ROTx and add a click (or more) between letters to avoid the same result for the "LL"

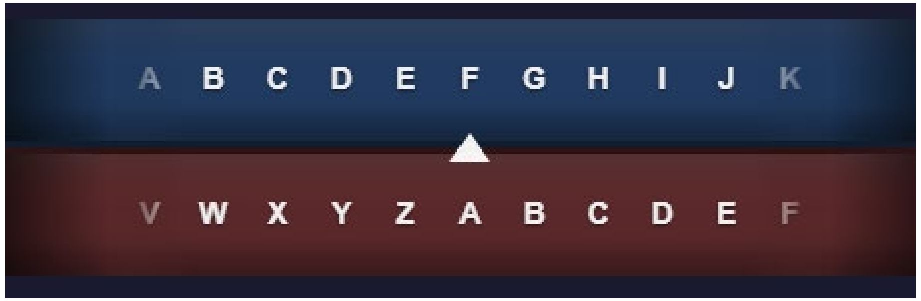
1



Z A B C D E F G H I J

V W X Y Z A B C D E F

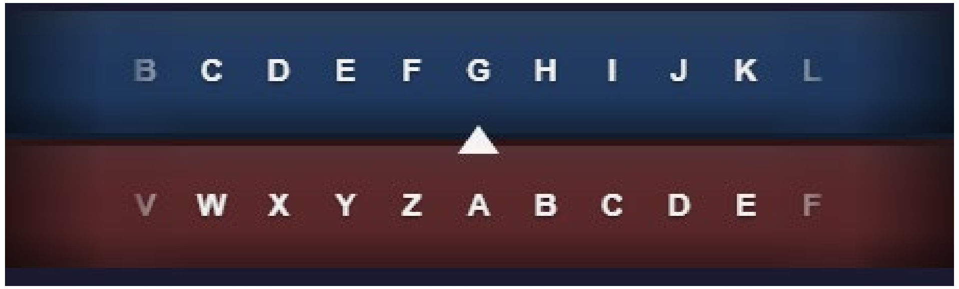
2



A B C D E F G H I J K

V W X Y Z A B C D E F

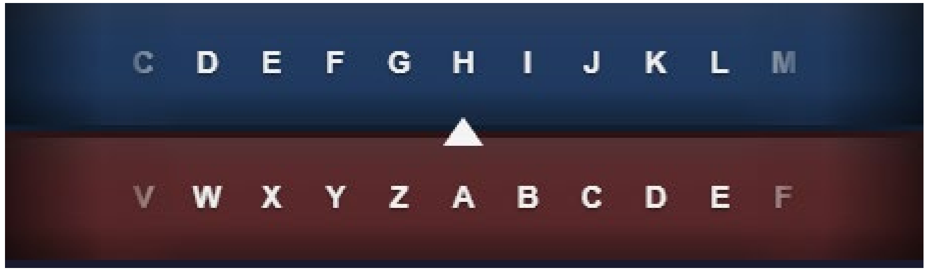
3



B C D E F G H I J K L

V W X Y Z A B C D E F

4



C D E F G H I J K L M

V W X Y Z A B C D E F

CipherFidget Lesson 2 Discussion

I AM A MAN

ROTx+

M FS H UJX

ROTx

M EQ E QER

- ROT-X+: Rotating + Shift
- HELLO was LIPPS: becomes LJRSW with ROT4+1
- What if we did +1, +2, +3, +1, etc? LJSVZ
- Is this stronger because of the second key, or because of the more complex algorithm?

  Practice: Decrypt this using Rot6 +2 **NIZBWDWMO**

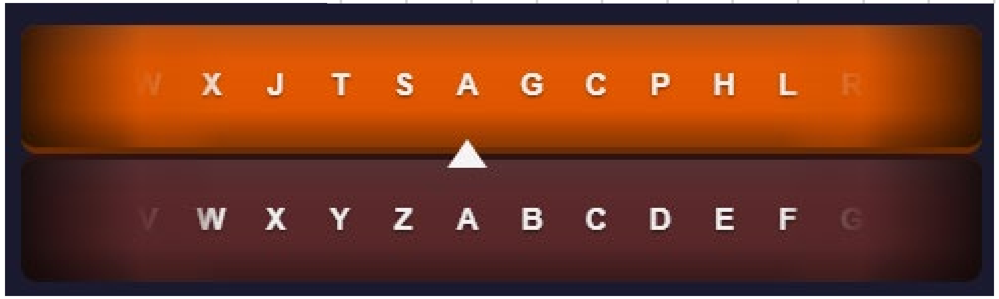
  - If an adversary knew the algorithm (ROTX+) but not the keys, could they crack it faster than if they knew the keys but not the algorithm?
- The takeaway: Adding more keys (like the increment) is valuable because it increases the "key space" — the number of possibilities an attacker must try.
- The algorithm complexity helps too (it defeats pattern analysis), but never rely on keeping the algorithm secret!

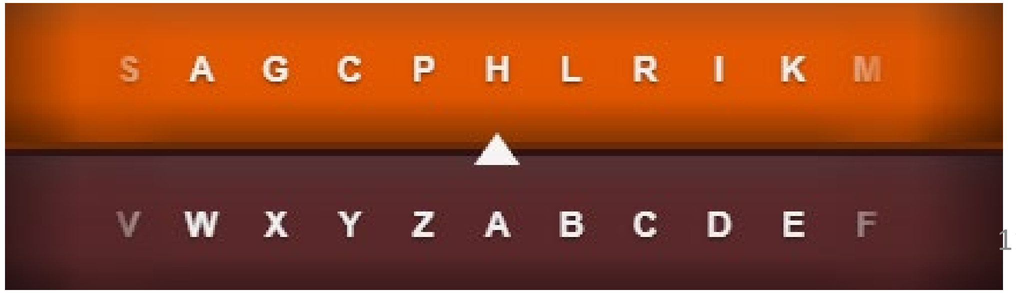
CipherFidget Lesson 3

- Randomized Alphabet Top Ring
- https://cipherfidget.com/lessons/randomized-alphabet
- We will replace the upper ring with an Orange randomized alphabet (and use an offset of 4).

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





CipherFidget Lesson 3 Discussion

- Randomized Alphabet Top Ring (Set to ROT4)

I AM A MAN
O HY H YHB

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

- HELLO became FKVVU. Oh! L=V, so does that mean K is U? (no)
  - Can we combine ROTx+ with the randomized ring
- How much more powerful is the random ring?
  - With a randomized alphabet, there are 26! (26 factorial) = 403,291,461,126,605,635,584,000,000 possible alphabet arrangements!

Practice: Decrypt this using Rot3 **WILJEI**

Want to Get More Complicated?

- Are three rings better than two?
- Return the alphabetic ring as ring 2 (A’s aligned)
- Add the randomized alphabet as the top ring (A’s aligned)
- Perform a ROT4 on the bottom ring

CipherFidget Lesson 3A Using 3 Rings

(polyalphabetic)

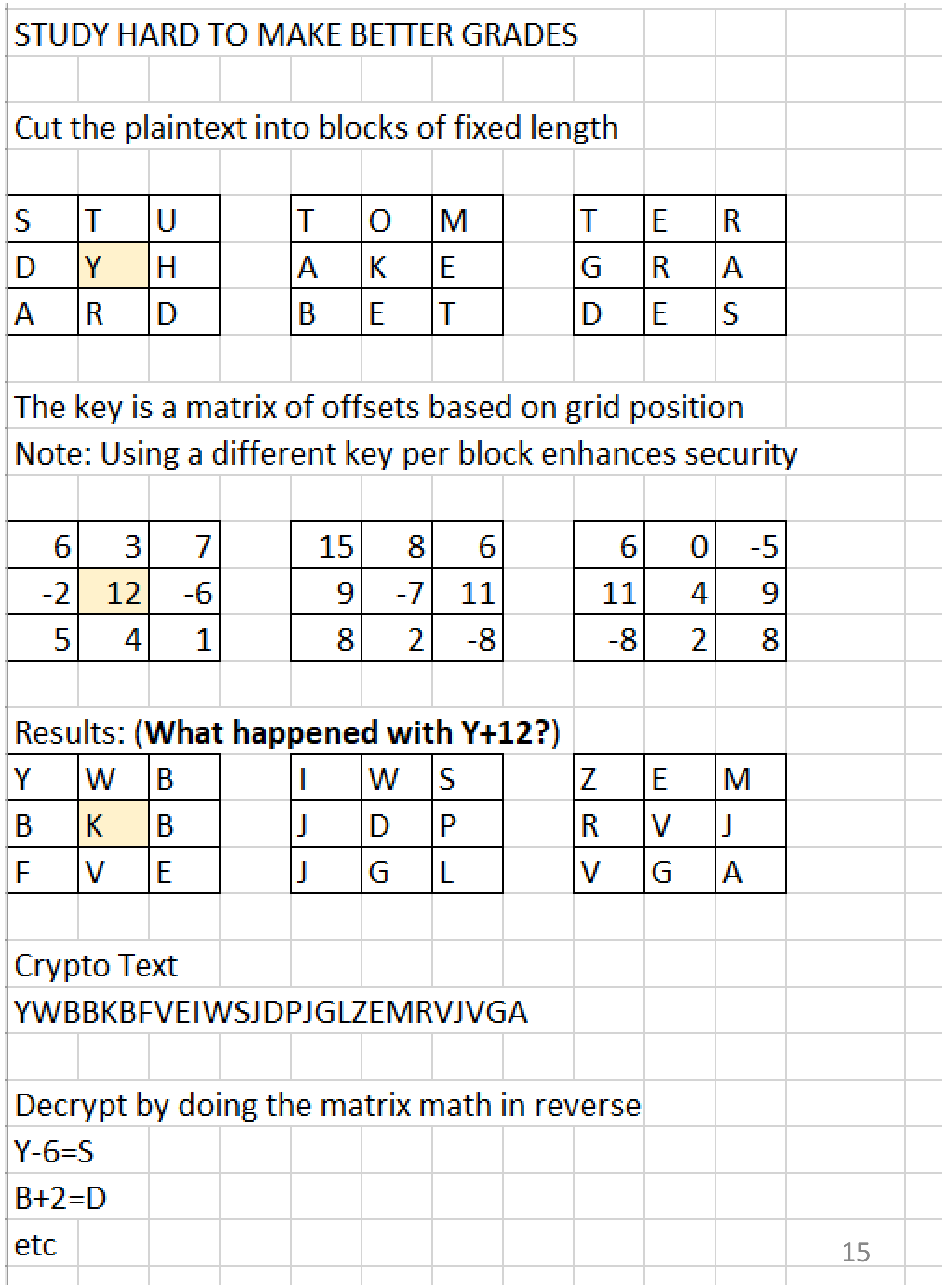
Alternating between two offset alphabets

An offset random alphabet	A	G	C	P	H	L	R	I	K	M	N	F	O	D	Q	V	Y	B	U	Z	E	W	X	J	T	S	A	G	C	P
An offset 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	A	B	C	D
					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	T	T	A	C	K		A	T		N	O	O	N		F	R	O	M		T	H	E		E	A	S	T		
An offset random alphabet	H	J	J	H	R	Q		H	J		B	U	U	B		M	W	U	Y		J	F	K		K	H	X	J		
An offset alphabet	E	X	X	E	G	O		E	X		R	S	S	R		J	V	S	Q		X	L	I		I	E	W	X		
Two Offset Alphabets	E	J	X	H	G	Q		E	J		R	U	S	B		J	W	S	Y		X	F	I		K	E	X	X		

- Using each ring by itself suffers from double letter syndrome (monoalphabetic)
  - That is solved here without using ROTx+
- Now the adversary has to identify a new algorithm *And* a new alphabet. (polyalphabetic)
- Could we make it harder by doing a ROTx+?

A Different Key Structure: Block Encryption and Transposition

- The prior exercises encrypted a stream of characters using Substitution
- We will take a different approach here: Transposition



STUDY HARD TO MAKE BETTER GRADES

Cut the plaintext into blocks of fixed length

S	T	U		T	O	M		T	E	R
D	Y	H		A	K	E		G	R	A
A	R	D		B	E	T		D	E	S

The key is a matrix of offsets based on grid position

Note: Using a different key per block enhances security

6	3	7		15	8	6		6	0	-5
-2	12	-6		9	-7	11		11	4	9
5	4	1		8	2	-8		-8	2	8

Results: (**What happened with Y+12?**)

Y	W	B		I	W	S		Z	E	M
B	K	B		J	D	P		R	V	J
F	V	E		J	G	L		V	G	A

Crypto Text

YWBBKBFVEIWSJDPJGLZEMRVJVGA

Decrypt by doing the matrix math in reverse

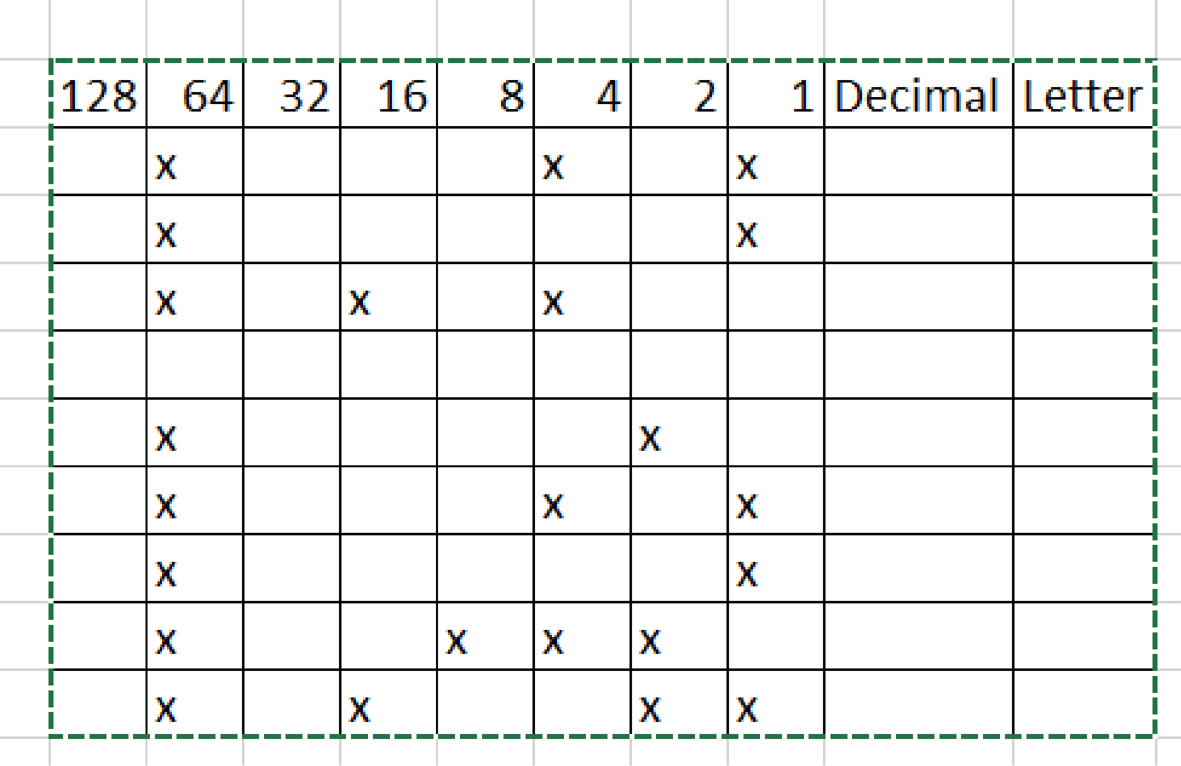
Y-6=S

B+2=D

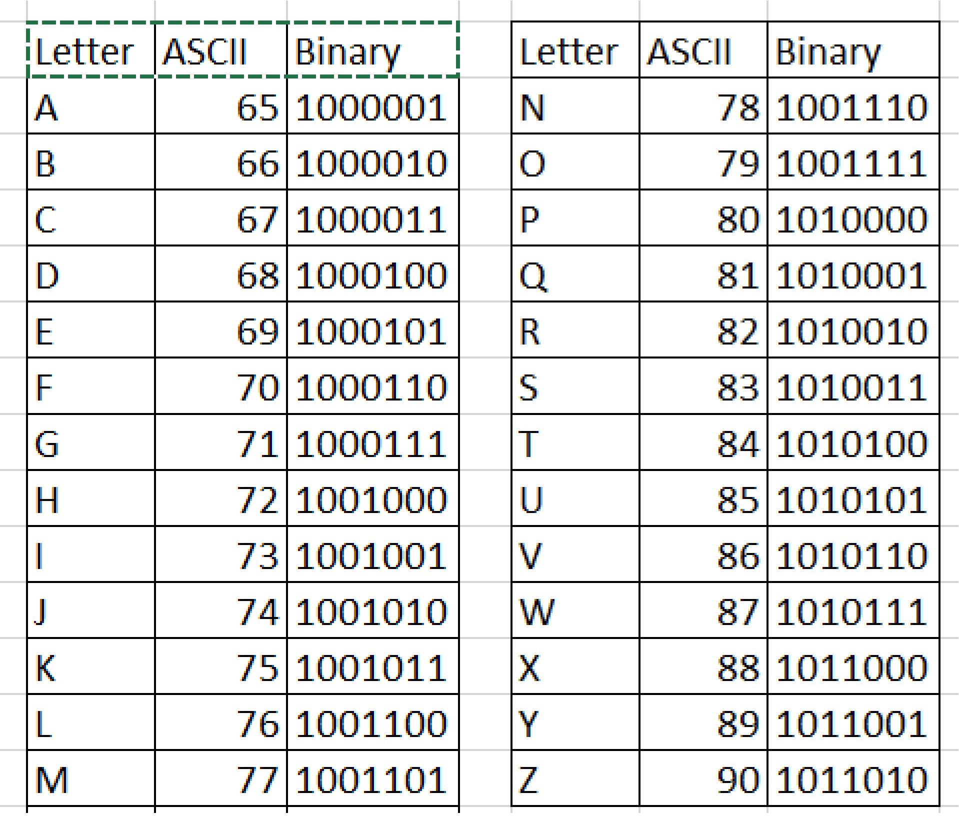
etc

A Look Under the Hood: Binary Representation

- We have been using the alphabet to demonstrate the concepts, but computers user Binary representation for letters and numbers
- Let’s do a quick review of how binary and decimal are related
  - (1’s, 10’s, 100’s, 1000’s vs 1’s, 2’, 4’s, 8’s)
- What message is represented here?



128	64	32	16	8	4	2	1	Decimal	Letter
	x				x		x		
	x						x		
	x		x		x				
	x					x			
	x				x		x		
	x						x		
	x			x	x	x			
	x		x			x	x		



Letter	ASCII	Binary
A	65	1000001
B	66	1000010
C	67	1000011
D	68	1000100
E	69	1000101
F	70	1000110
G	71	1000111
H	72	1001000
I	73	1001001
J	74	1001010
K	75	1001011
L	76	1001100
M	77	1001101

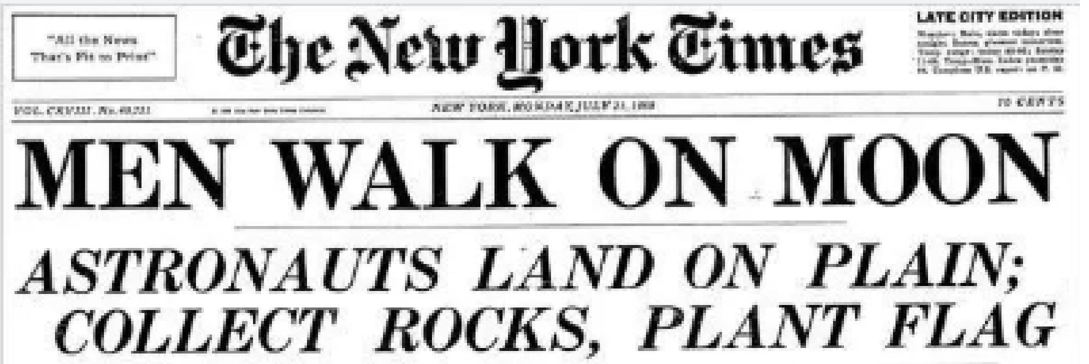
Letter	ASCII	Binary
N	78	1001110
O	79	1001111
P	80	1010000
Q	81	1010001
R	82	1010010
S	83	1010011
T	84	1010100
U	85	1010101
V	86	1010110
W	87	1010111
X	88	1011000
Y	89	1011001
Z	90	1011010

Some Ideas for Key Exchange

- Via telephone (but not email or text)
- A codebook with a new key for every day of the year
- A formula to compute a new key based on the high temperature the day before*
- The first letter of words in today's headlines (MWOMALOPCRPF)
- Hidden in plain sight (ROBIN)

*Key = 48 (temperature) / 7 (date) truncated to 6 decimal places
6.857142

Aside. If you have 9 friends and want to exchange secrets with all of them independently, how many keys do you need? How do you manage them?



"All the News That's Fit to Print"

The New York Times

LATE CITY EDITION

[illegible]

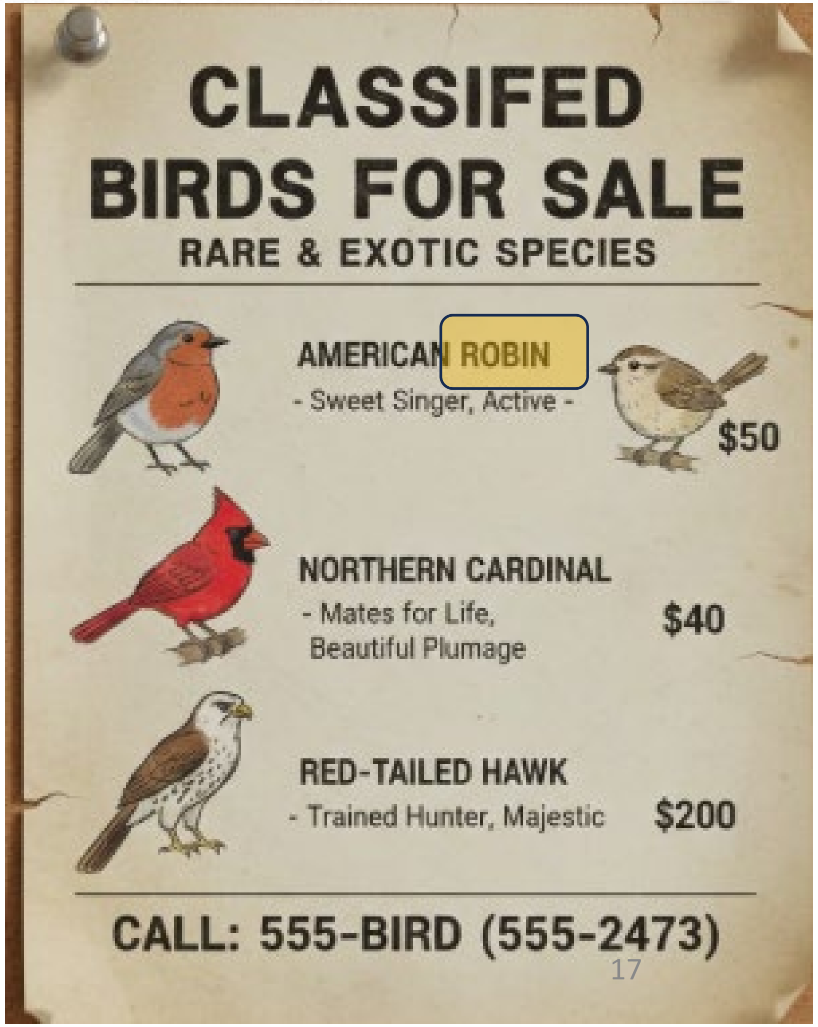
VOL. CXVIII . No. 40,721

NEW YORK, MONDAY, JULY 21, 1969

10 CENTS

MEN WALK ON MOON

ASTRONAUTS LAND ON PLAIN; COLLECT ROCKS, PLANT FLAG



CLASSIFED

BIRDS FOR SALE

RARE & EXOTIC SPECIES

AMERICAN ROBIN
- Sweet Singer, Active -
$50

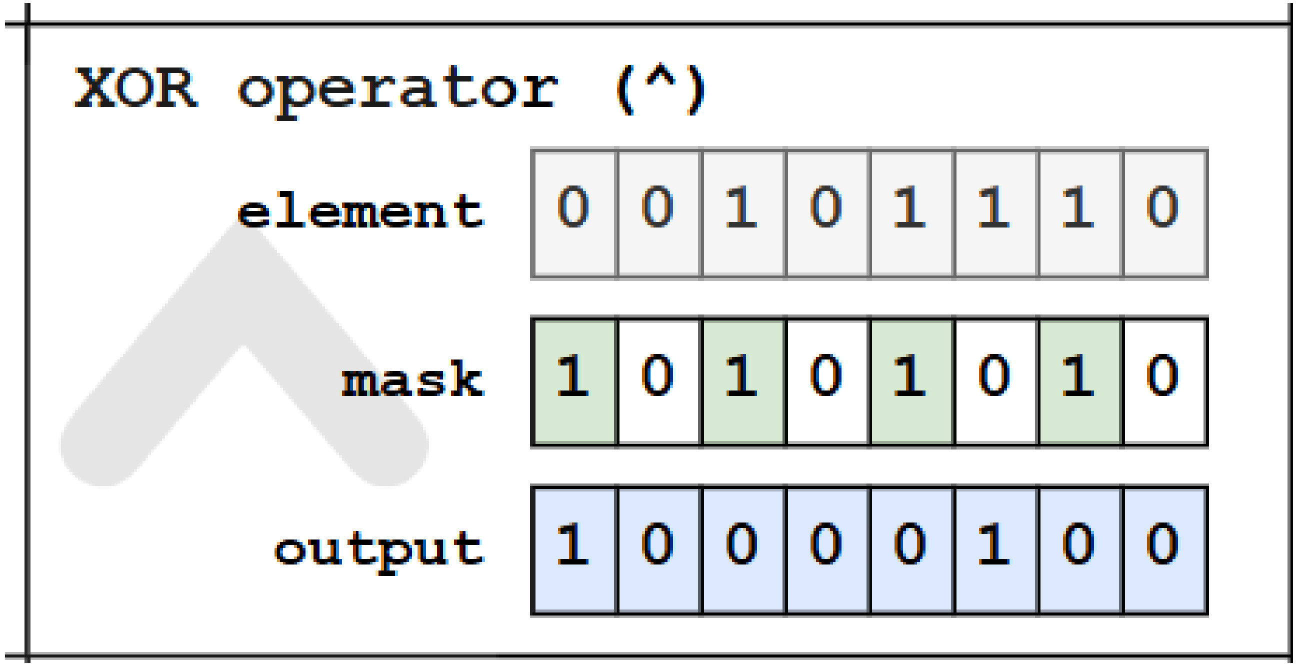
NORTHERN CARDINAL
- Mates for Life, Beautiful Plumage
$40

RED-TAILED HAWK
- Trained Hunter, Majestic
$200

CALL: 555-BIRD (555-2473)

Binary Logic Operations

- You’ve seen AND and OR. Here is a new one
- XOR (Exclusive OR) is a logical, binary, and bitwise operation that returns “True”or “False”
  - 0 and 1 (in any order) is 1 (output is “True”)
  - 1 and 1 is zero, and 0 and 0 is 0. (Both inputs are the same the output is “False”)

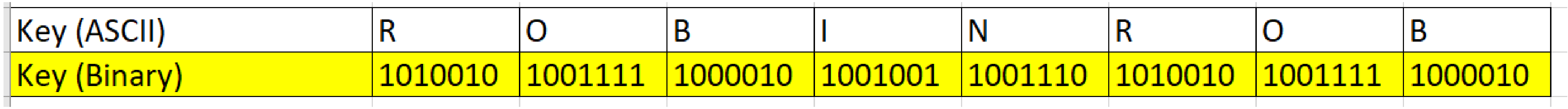


XOR operator (^)

element	0	0	1	0	1	1	1	0
mask	1	0	1	0	1	0	1	0
output	1	0	0	0	0	1	0	0

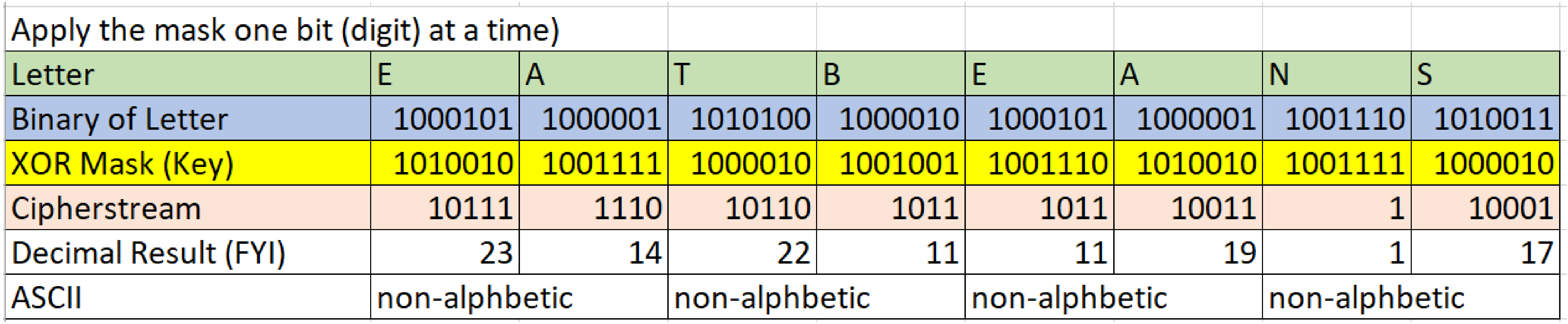
Applying XOR to Binary Encryption

- We create a key (and exchange via secure channel) that has a binary representation



Key (ASCII)	R	O	B	I	N	R	O	B
Key (Binary)	1010010	1001111	1000010	1001001	1001110	1010010	1001111	1000010

- To encrypt, we XOR the key to the binary (bits) of the plaintext

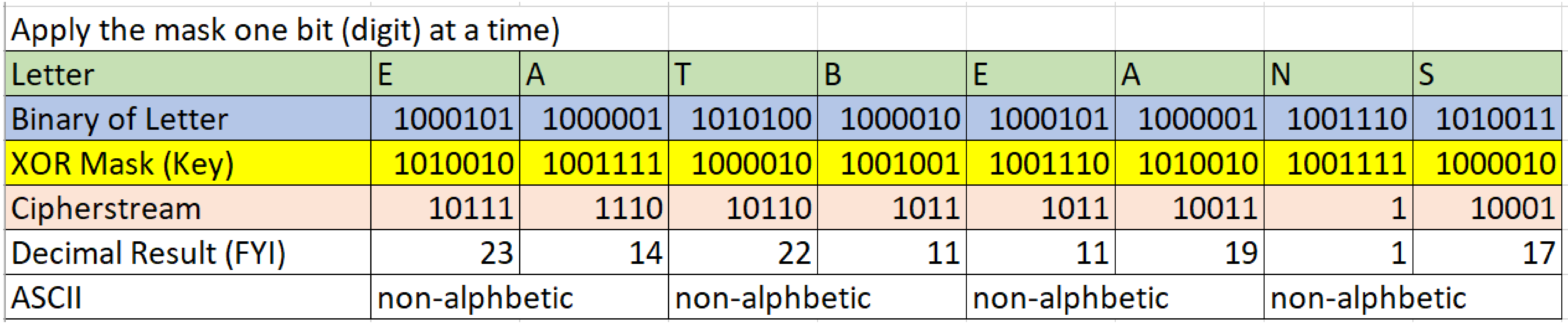


Apply the mask one bit (digit) at a time)								
Letter	E	A	T	B	E	A	N	S
Binary of Letter	1000101	1000001	1010100	1000010	1000101	1000001	1001110	1010011
XOR Mask (Key)	1010010	1001111	1000010	1001001	1001110	1010010	1001111	1000010
Cipherstream	10111	1110	10110	1011	1011	10011	1	10001
Decimal Result (FYI)	23	14	22	11	11	19	1	17
ASCII	non-alphbetic		non-alphbetic		non-alphbetic		non-alphbetic	

Note: The binary will not always represent readable letters.

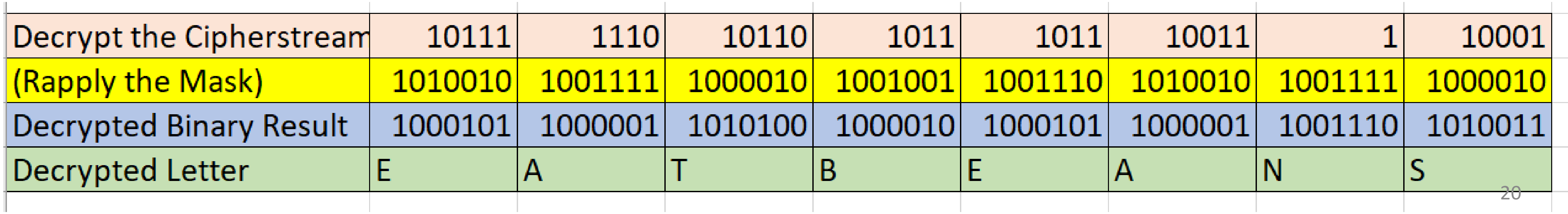
Applying XOR to Binary Decryption

- Recall: To Encrypt, we XOR the key to the binary (bits) of the plaintext



Apply the mask one bit (digit) at a time)								
Letter	E	A	T	B	E	A	N	S
Binary of Letter	1000101	1000001	1010100	1000010	1000101	1000001	1001110	1010011
XOR Mask (Key)	1010010	1001111	1000010	1001001	1001110	1010010	1001111	1000010
Cipherstream	10111	1110	10110	1011	1011	10011	1	10001
Decimal Result (FYI)	23	14	22	11	11	19	1	17
ASCII	non-alphbetic		non-alphbetic		non-alphbetic		non-alphbetic	

- To Decrypt, we XOR the key to the binary (bits) of the cyphertext



Decrypt the Cipherstream	10111	1110	10110	1011	1011	10011	1	10001
(Rapply the Mask)	1010010	1001111	1000010	1001001	1001110	1010010	1001111	1000010
Decrypted Binary Result	1000101	1000001	1010100	1000010	1000101	1000001	1001110	1010011
Decrypted Letter	E	A	T	B	E	A	N	S

SKIP?

Other CipherFidget Lessons (Codebreaking)

- Known Plaintext Attack
  - Guessing likely words or phrases, or easy words like “I”, “IN”, “ON”, or “A” to solve part of the ciphertext, resulting in a quick crack.
  - Maybe you know the sender always starts letters with "DEAR" or ends with "SINCERELY." This partial knowledge is called a crib, and it can break even complex ciphers!
- `T LX RZTYR ZY L ECTA TY L MZLE`

SKIP?

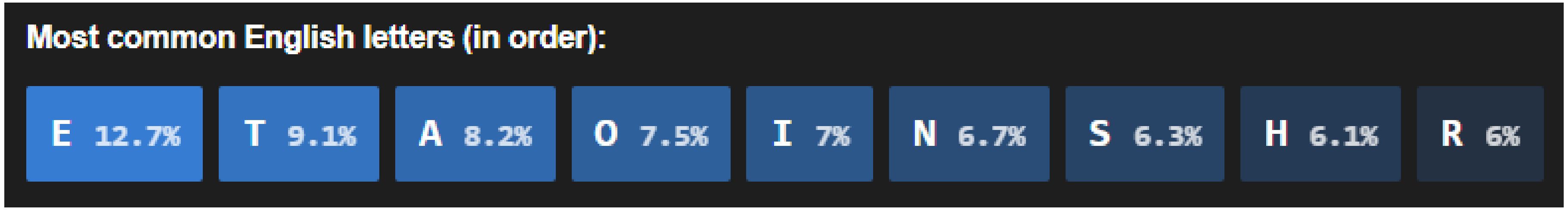
Other CipherFidget Lessons (Codebreaking)

- Known Plaintext Attack
  - Guessing likely words or phrases, or easy words like “I”, “IN”, “ON”, or “A” to solve part of the ciphertext, resulting in a quick crack.
  - Maybe you know the sender always starts letters with "DEAR" or ends with "SINCERELY." This partial knowledge is called a crib, and it can break even complex ciphers!
- `T LX RZTYR ZY L ECTA TY L MZLE`
- `I AM GOING ON A TRIP IN A BOAT`

SKIP?

Other CipherFidget Lessons (Codebreaking)

- Frequency Analysis Attack
  - In English text, some letters appear much more frequently than others. The letter **E** appears about 12.7% of the time, while **Z** appears less than 0.1%.
  - In earlier lessons, we mentioned that simple substitution ciphers have a weakness: repeated letters in the plaintext produce repeated letters in the ciphertext. But how exactly do attackers exploit this?
  - The answer is **frequency analysis** — a technique that has been used for over a thousand years to break substitution ciphers. It was first described by the Arab mathematician Al-Kindi in the 9th century!
  - **For Caesar ciphers specifically:** once you guess one letter, you know the shift!



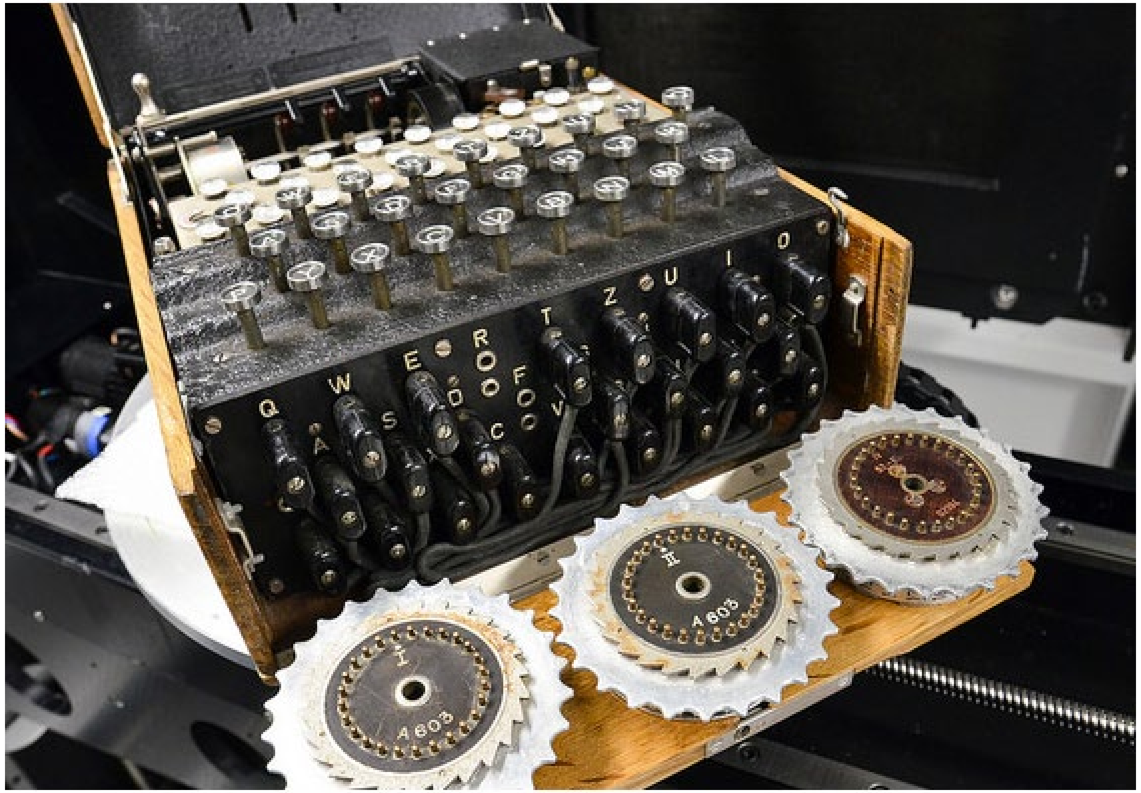
Most common English letters (in order):

E	T	A	O	I	N	S	H	R
12.7%	9.1%	8.2%	7.5%	7%	6.7%	6.3%	6.1%	6%

SKIP?

Enigma

- https://www.101computing.net/enigma-machine-emulator/



The Enigma's rotors and plug board

The (unique) Key is the sole secret, and must be kept secret. Keys must be exchanged via secure channels

Key management is the downfall of symmetric key encryption.

- If I work with 10 people and want to assure confidentiality with all 10, how many keys do we all have to manage?
- What if I have 1000 employees plus 150 business partners, 15 banks?
  - 10 ->45   100->4950 1000-> 50 million (It is she sum of numbers from 1 to X-1)
- And what if my company policy requires that keys be changed every year? Will I be able to open last year's emails with this year's keys?
- Is there a better way? YES! It is called public key infrastructure (PKI) or asymmetric keys.

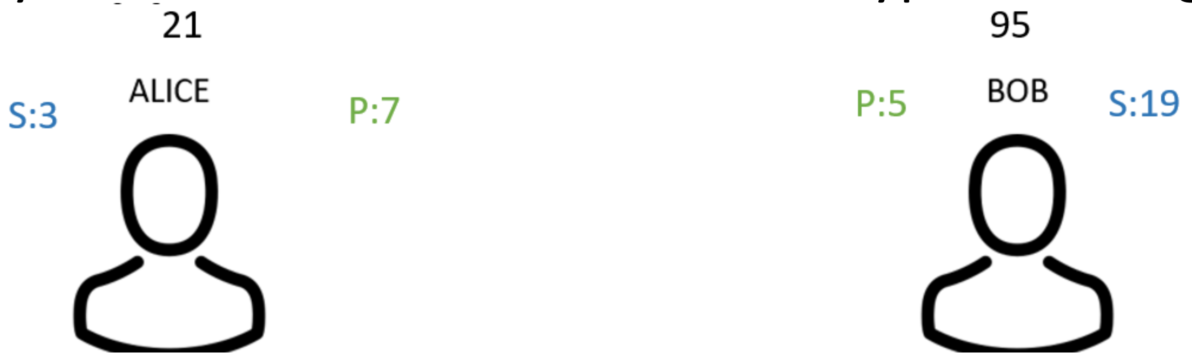
Public-Key Encryption (PKI*) Concepts

- Public Key Infrastructure involves the creation, management, integrity, and distribution of encryption keys.
- This concept and technology is often the most confusing, but holds the most promise for simplification of key management in large enterprises.
- Remember the mantra for symmetric encryption:
  - The (unique) Key is the sole secret, and must be kept secret
  - But the problem is, in a workgroup of 100 people, about 5000 symmetric keys have to be exchanged.
- Well now we are going to assign a pair of keys to everyone and post one them publicly for everyone to see.
  - One key is used for encryption and the other is used for decryption.

* PKI means Public Key Infrastructure

Creating Public-Key Encryption (PKI) Keys
(Asymmetric encryption.. approximate example)

- Well now we are going to generate a pair of keys (that are mathematically linked). For example, 3x7=21   5x19=95 (in reality, VERY large prime numbers)
- Everyone gets their own pair.
  - One key is used for encryption and the other is used for decryption
  - They are created using prime factors of very large numbers
  - The public key (P) (and its product) are stored in a central server.
  - Anyone can see the public key, but only the key owner can see the private key (S)
  - Nobody can see the product
- So which key do you think Alice would use to encrypt a message to Bob?

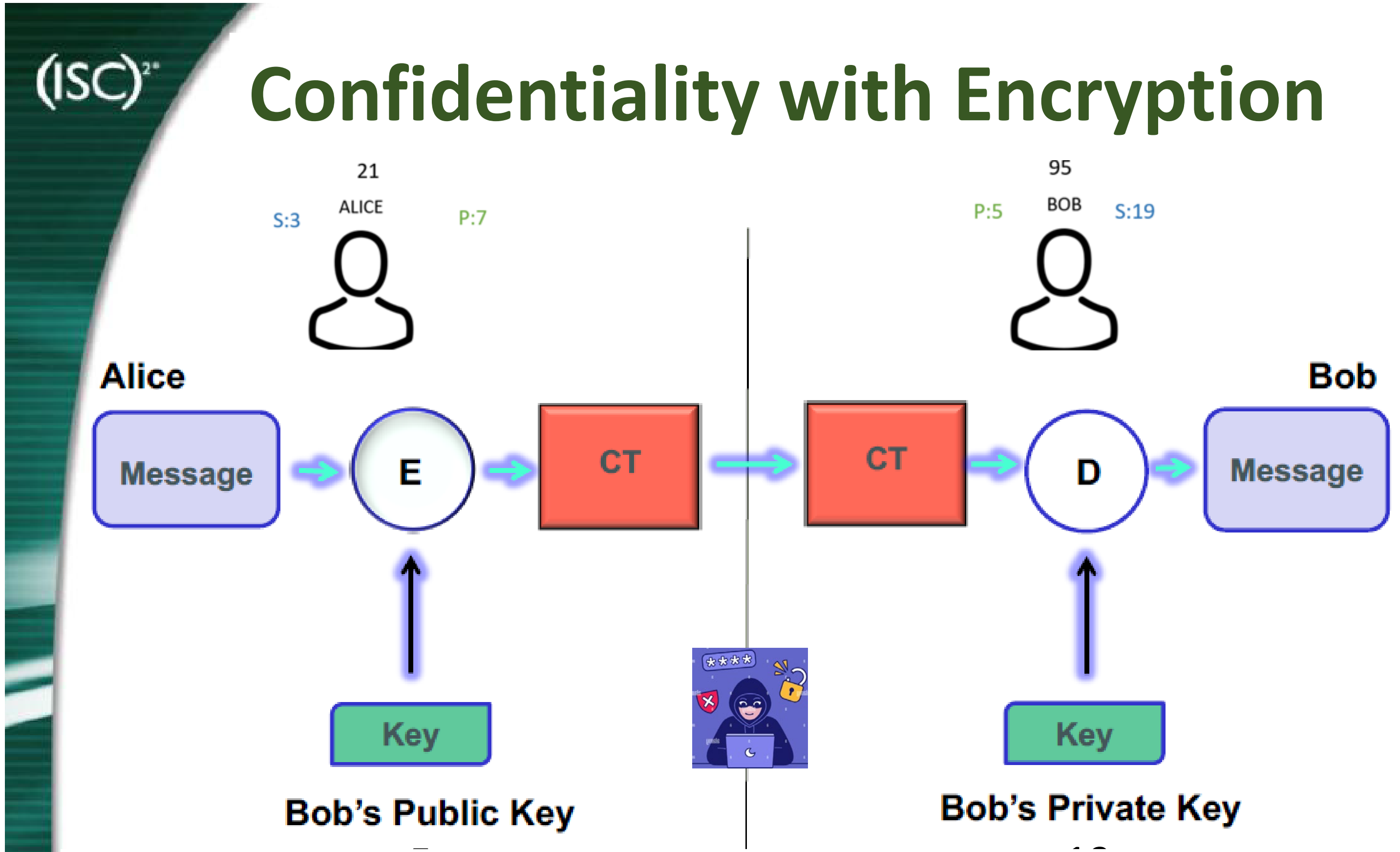


Using PKI to Send an Encrypted Message

*	Confidentiality
	Integrity
*	Availability
	Authenticity
	Non-repudiation
*	Privacy

Confidentiality

- Alice Uses Bob’s public key (5) to encrypt a message to him
- Bob uses his private (secret) key (19) to decrypt the message
- Bob does the reverse to send a secure reply



Confidentiality with Encryption

Note: The man-in-the middle can possibly intercept the ciphertext, but would need to guess the Bob’s private key to decrypt. Knowing Bob’s public key only enables someone to encrypt, not decrypt. But maybe he can replace the cyphertext.

More About PKI Keys

- Real PKI Keys use very large prime numbers (2048 bits = 600+ decimal digits)
- 5 x 19 =21 was a simple case. If you know Bob’s public key of 5, you can guess some of its multiples against primes and get to 95 quickly. (5x3, 5x7, 5x11, 5x13, 5x17, 5x19=95)
- Here is a pair of large five-digit prime numbers and their resulting product:
  - Prime 1: 88,897
  - Prime 2: 77,773
  - Product: 6,913,786,381
- If 88,897 is my public key, what are the chances you could derive my private key?
- While a computer can multiply these two numbers instantly, it is incredibly difficult for a computer to do the reverse—taking the product 6,913,786,381 and "factoring" it back into 88,897 and 77,773

Welcome to Hashes

- What is a Hash?
  - A hash function is a function that takes as input an arbitrarily long string of bits (or bytes) and produces a fixed-size result
  - The result is a Hash. It is basically a number.
- A hash comparison is used to assure a file has not been altered.
- Let's invent a simple hash for this slide by choosing the first letter of each line. Would it be a good tool to see if there are any changes? WAbTALWRsMbMe
- Real hashes look like this: The results are completely different for even a slight change in the text or document
  - `My dog has fleas that it got from the cat.`
    `b4f5dc1dc963f40b24c4eeabf3da715f`
  - `My dog has Fleas that it got from the cat.`
    `e18e88b66a82a7f5bf95d7681706ee3b`

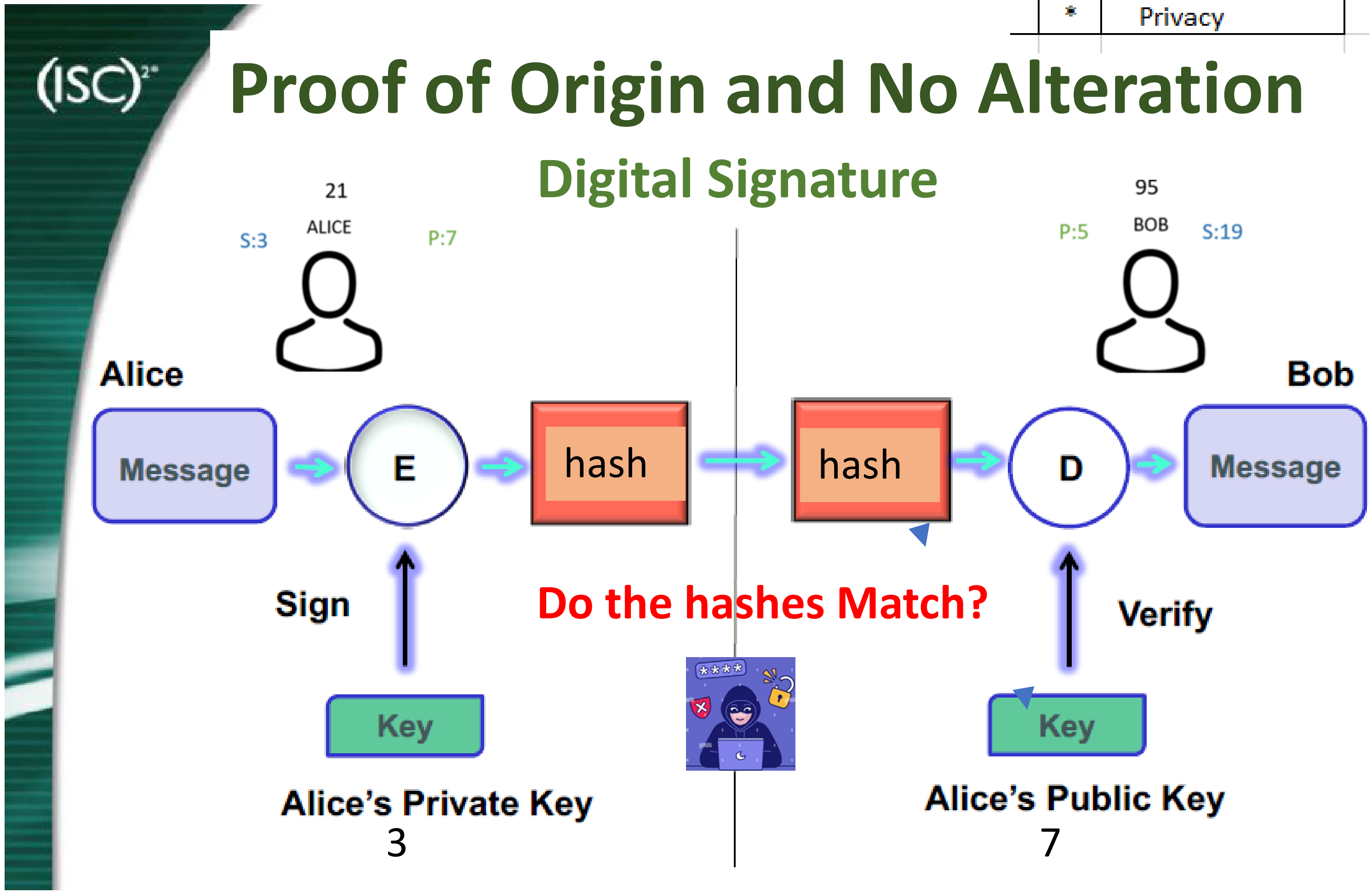
Aside: How are hashes used with password storage?

Using PKI to Verify Message Integrity and Sender Verification

*	Confidentiality
#	Integrity
*	Availability
#	Authenticity
#	Non-repudiation
*	Privacy

Integrity

- Alice creates a Hash of the message in the previous slide.
- Alice uses her Private key (3) to encrypt the hash and then sends it to Bob. (This is the signature)
- Bob uses his Alices public key (7) to decrypt the Hash.
- If the decrypt is successful, that verifies Alice was the sender. (Non-repudiation)
- Bob creates a Hash from the message he received in the prior slide, compared to this one Alice sent.
- If the Hashes match, then there was no alteration. (Integrity)

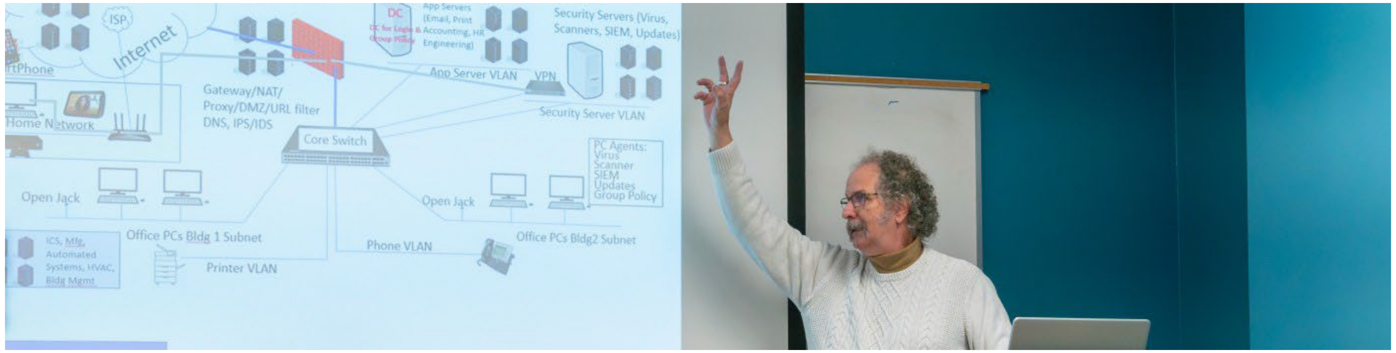


Proof of Origin and No Alteration

Digital Signature

Note: The hash need not be encrypted, but doing so adds the value of verifying that Alice sent it. It also assures the has was not maliciously altered to match a possible man-in-the-middle attack.

Download slides at
Bhudsoncissp.com



Cyber Encryption. A Hands-on Experience

Presented by Barry Hudson

bhudsoncissp@gmail.com

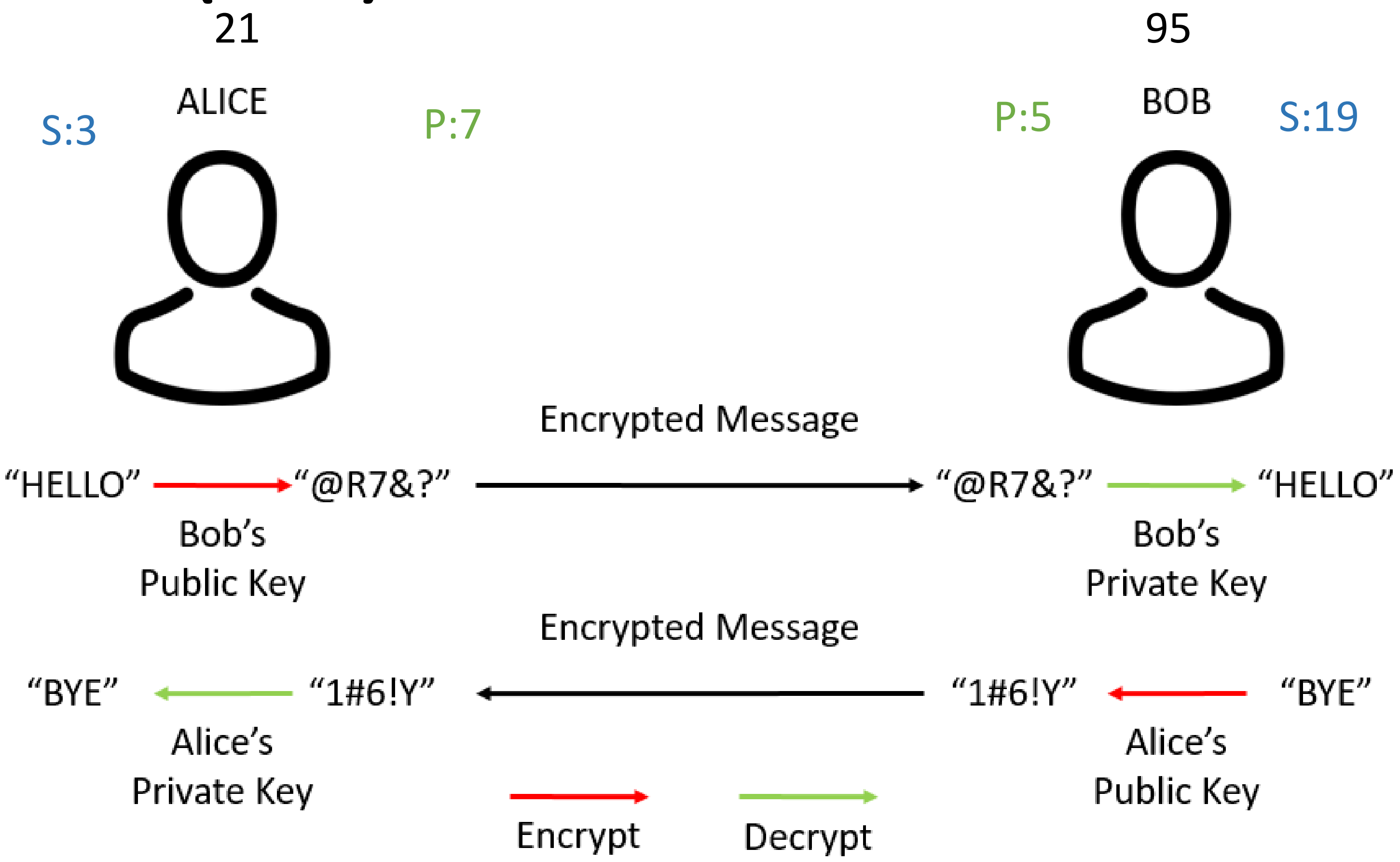
GCFIV IRGVCTXMSR E LERHW-SR IBTIVMIRGI

TVIWIRXIH FC FEVVC LYHWSR

SKIP?

Public-Key Encryption (PKI) Process

- So which key do you think is used for encryption? Public. Listen carefully..
  - When Alice wants to send a message to Bob, she first obtains Bob's public key.
  - Alice encrypts the message m with the public key P(Bob) to get the ciphertext c, and sends c to Bob.
  - Bob uses his secret key S(Bob) and the decryption algorithm to decrypt the message and get the message m.
  - The process is reversed when Bob replies to Alice.



Barry sez: Email is used for illustration only. The same thing can be done under program control for server-to- server, between applications, and web sessions and more.