Managing Enterprise Cybersecurity
MIS 4596

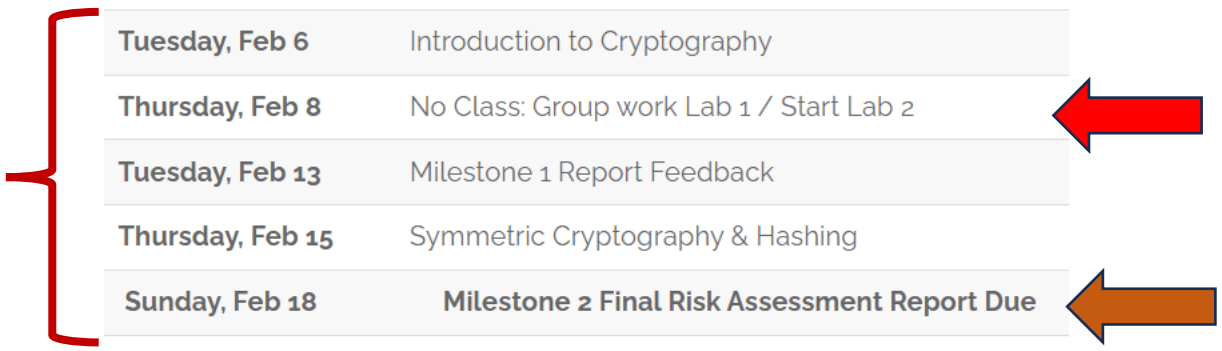
Class 6

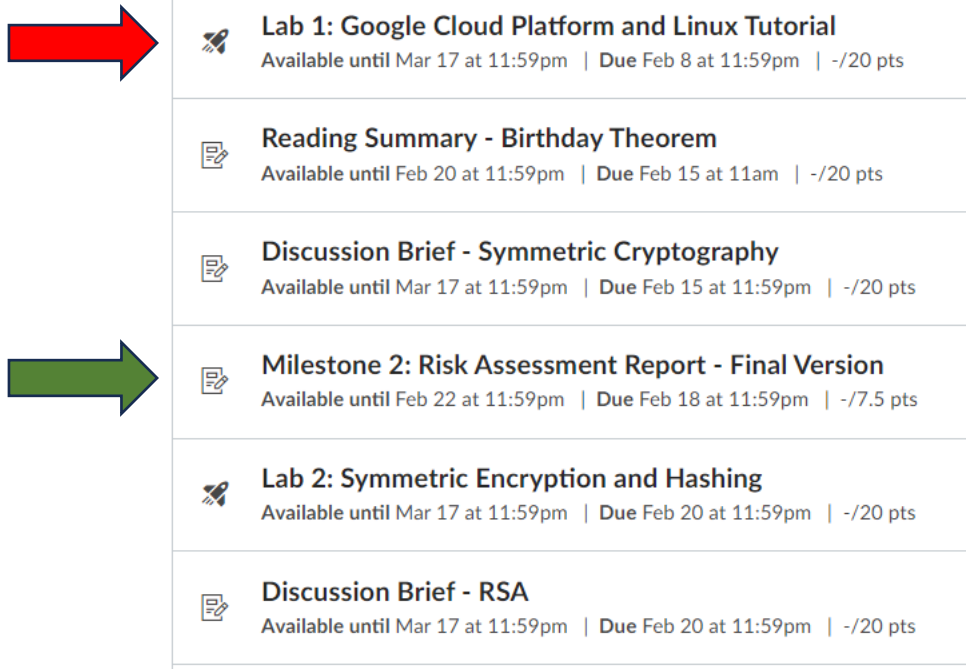
Agenda

- Updated Schedule
- Cryptography terminology
- Substitution
- Transposition
- Symmetric key cryptography
- Symmetric stream cryptography
- Next: Symmetric Encryption Lab

Updated Schedule

DATES	TOPICS
Tuesday, Jan 16	Introduction to the Course
Thursday, Jan 18	Introduction to the Course continued…
Tuesday, Jan 23	Threat modeling
Thursday, Jan 25	Risk Assessment & Milestone 1 Risk Assessment Report – Q&A
Sunday, Jan 28	**Milestone 1 Risk Assessment Report Due**
Tuesday, Jan 30	Introduction to Google Cloud Platform (GCP) & Linux
Thursday, Feb 1	Data Privacy
Tuesday, Feb 6	Introduction to Cryptography
Thursday, Feb 8	No Class: Group work Lab 1 / Start Lab 2
Tuesday, Feb 13	Milestone 1 Report Feedback
Thursday, Feb 15	Symmetric Cryptography & Hashing
Sunday, Feb 18	**Milestone 2 Final Risk Assessment Report Due**
Tuesday, Feb 20	Asymmetric Cryptography & Digital Signatures
Thursday, Feb 22	Digital Certificates and Public Key Infrastructures





Cryptography

- Method of transmitting and storing data in a form that only those it is intended for can read and process
- An effective way of protecting sensitive information as it is transmitted through untrusted network communication paths or stored on media
- Complements physical and logical access controls

The etymology is Greek and means: “*secret writing*”

Cryptanalysis

- The study of methods to break cryptosystems
- Often targeted at obtaining a key
- Attacks may be passive or active

- Kerckhoff's Principle
  - The only secrecy involved with a cryptosystem should be the key
- Cryptosystem Strength
  - How hard is it to determine the secret associated with the system?

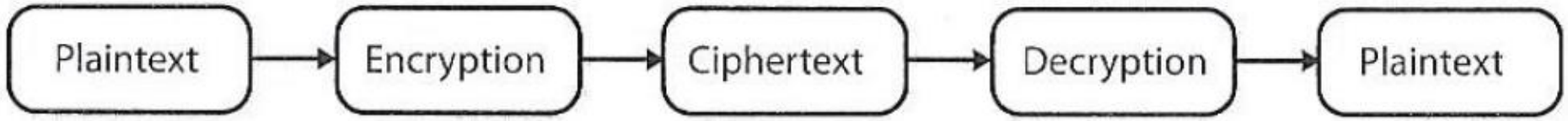
Cryptology

"The study of codes, or the art of writing and solving them"

- Is a term that encompasses both cryptography and cryptanalysis

Terminology

- **Plaintext** – is the readable version of a message
- **Ciphertext** – is the unreadable results after an encryption process is applied to the plaintext
- **Cryptosystem** – includes all the necessary components for encryption and decryption
  - Algorithms
  - Keys
  - Software
  - Protocols



Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

Cipher = encryption algorithm

2 main attributes combined in a cypher

1. **Confusion:** usually carried out through substitution
2. **Diffusion:** Usually carried out through transposition

Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

Example: Substitution cipher or algorithm

- A mono-alphabetic substitution cipher

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA
```

"SECURITY" <=> "HVXFIRGB"

- **Standard Alphabet:**
  ABCDEFGHIJKLMNOPQRSTUVWXYZ
- **Cryptographic Alphabet:**
  DEFGHIJKLMNOPQRSTUVWXYZABC

- **Plaintext:**
  LOGICAL SECURITY
- **Ciphertext:**
  ORJLFDO VHFXULWB

Services of cryptosystems

- **Confidentiality** – Renders information unintelligible except by authorized entities
- **Integrity** – Data has not been altered in an unauthorized manner since it was created, transmitted, or stored
- **Authentication** – Verifies the identity of the user or system that created, requested or provided the information
  - ***Authorization*** *– On proving identity, the individual is provided with the key or password that will permit access to some resource*
- **Nonrepudiation** – Ensure the sender cannot deny sending the information

Repudiation – the sender denying he sent the message

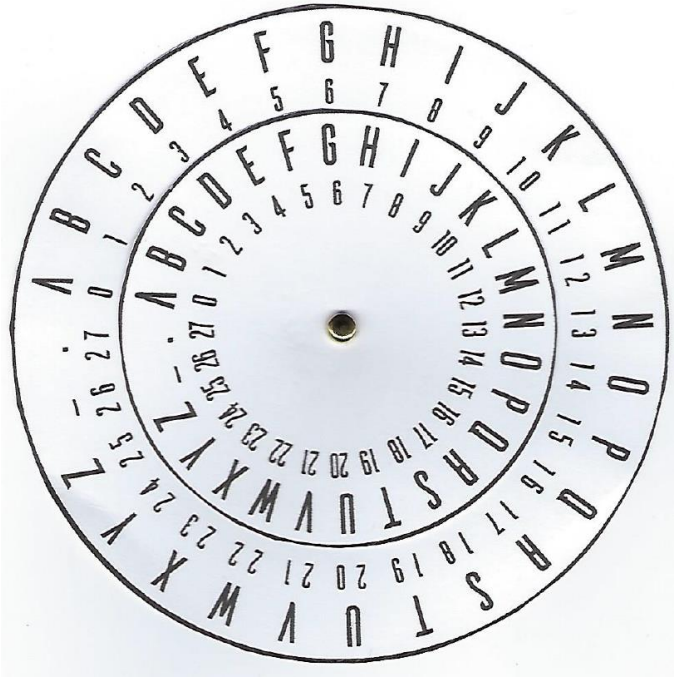
Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

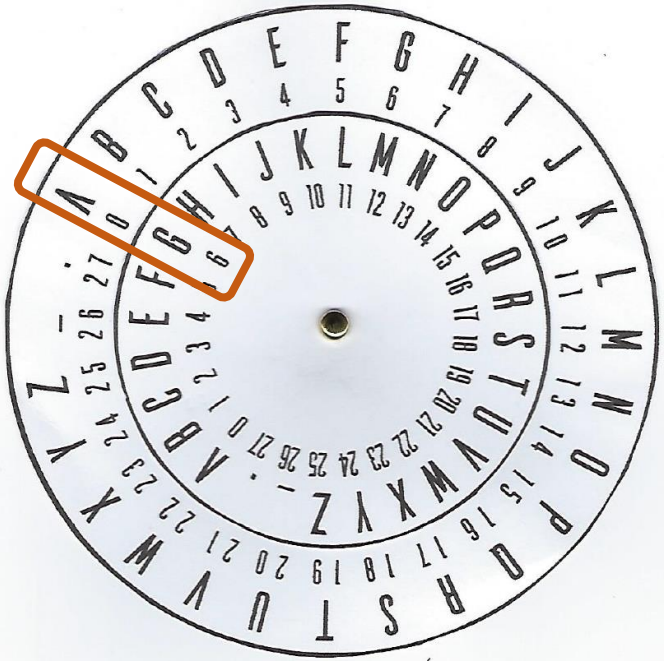
Cipher Disk

Outer wheel is for the *plaintext* alphabet

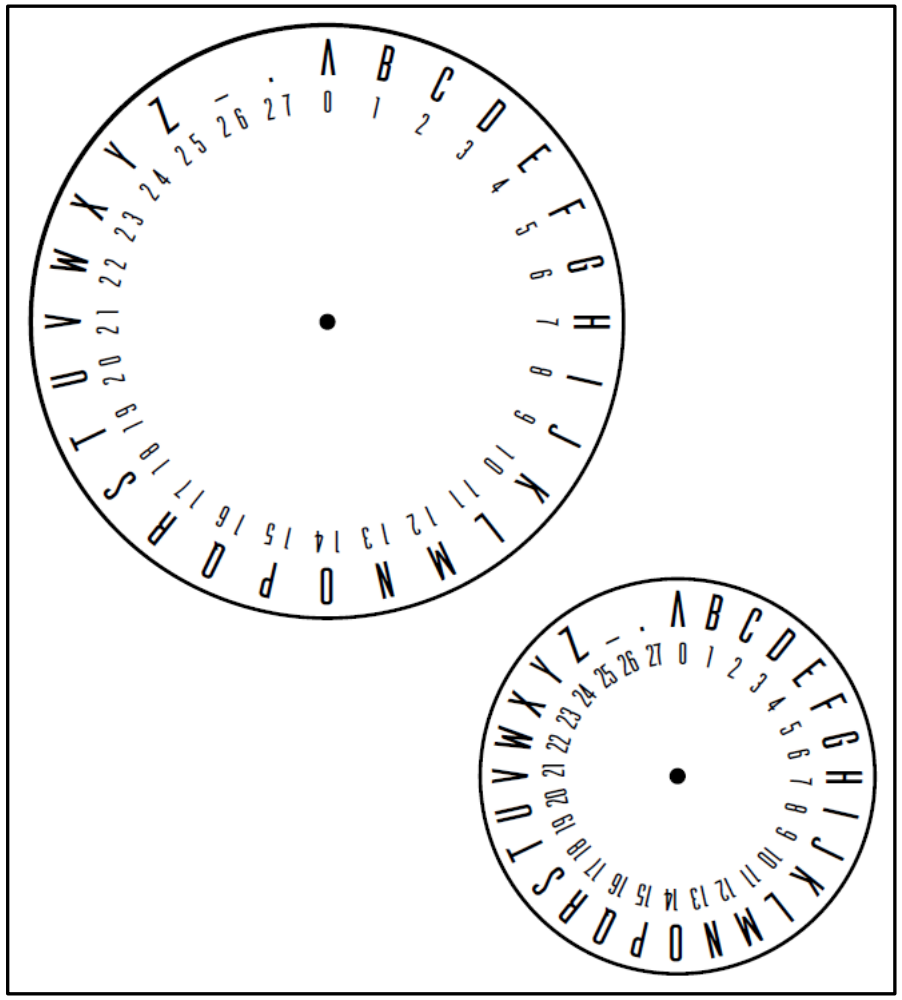
Inner wheel is for *ciphertext*

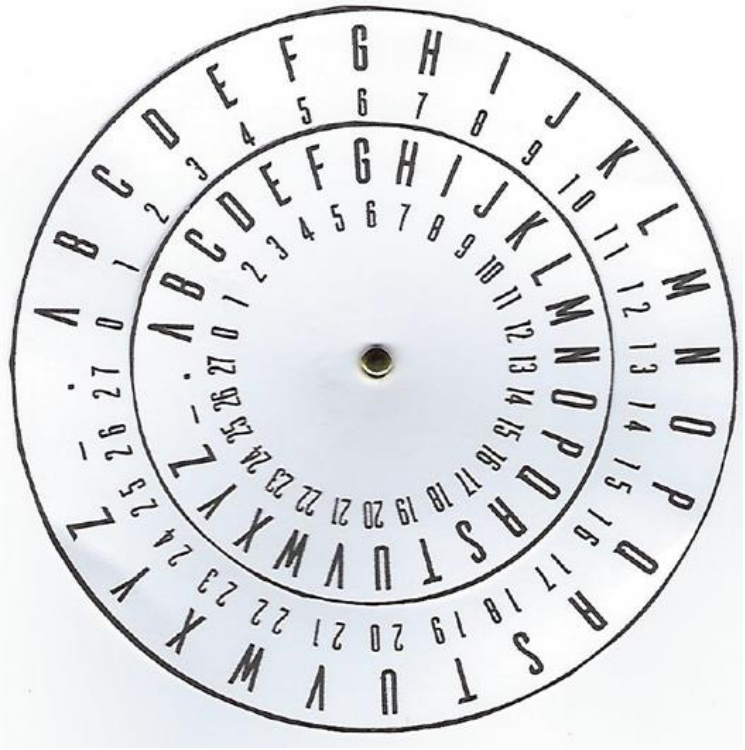
When the outer wheel and inner wheel and are both aligned at the letter “A” (i.e. position zero), there is no encryption mapping the letters on the outer wheel to letters on the inner wheel





You can make your own cipher disk

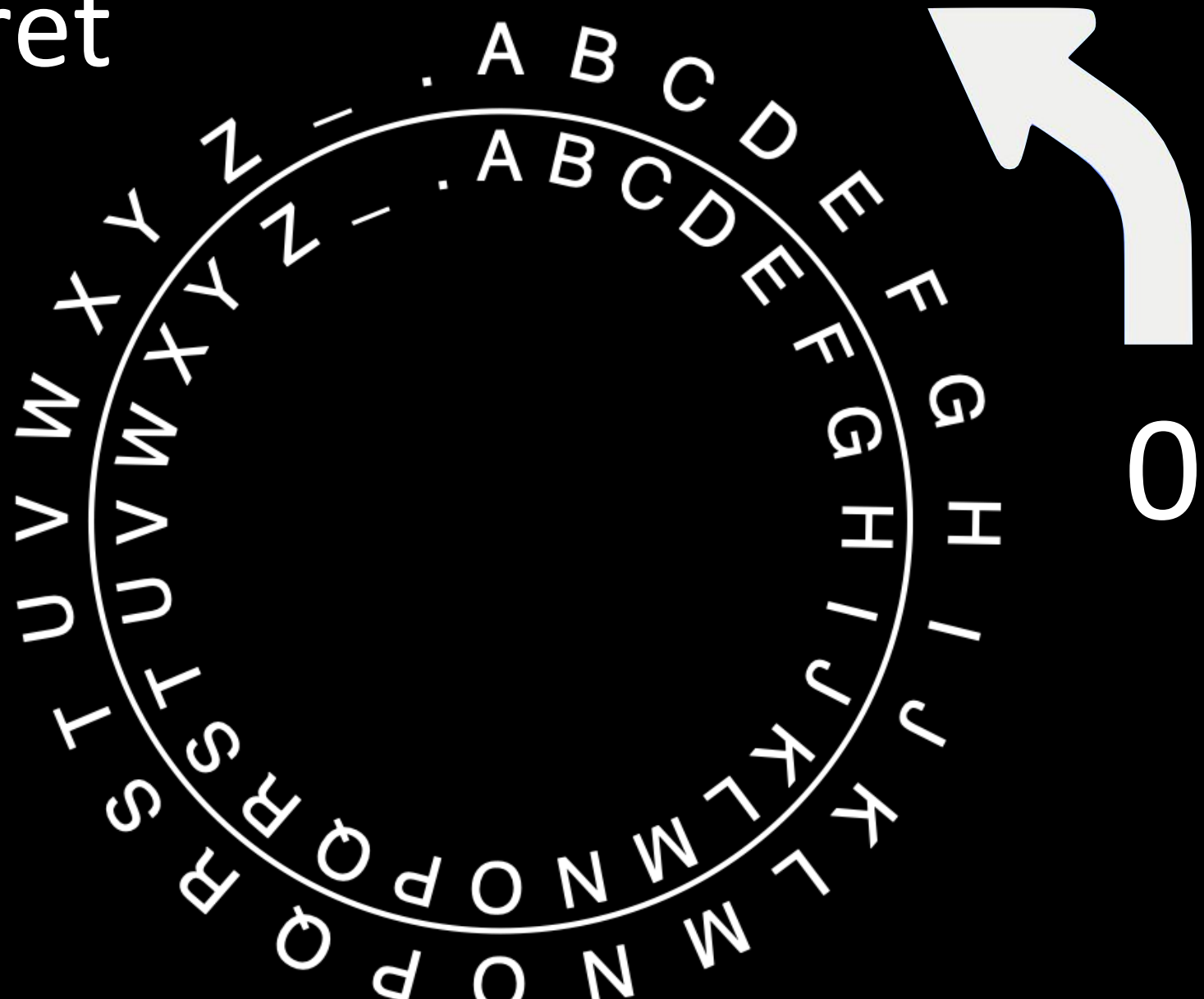


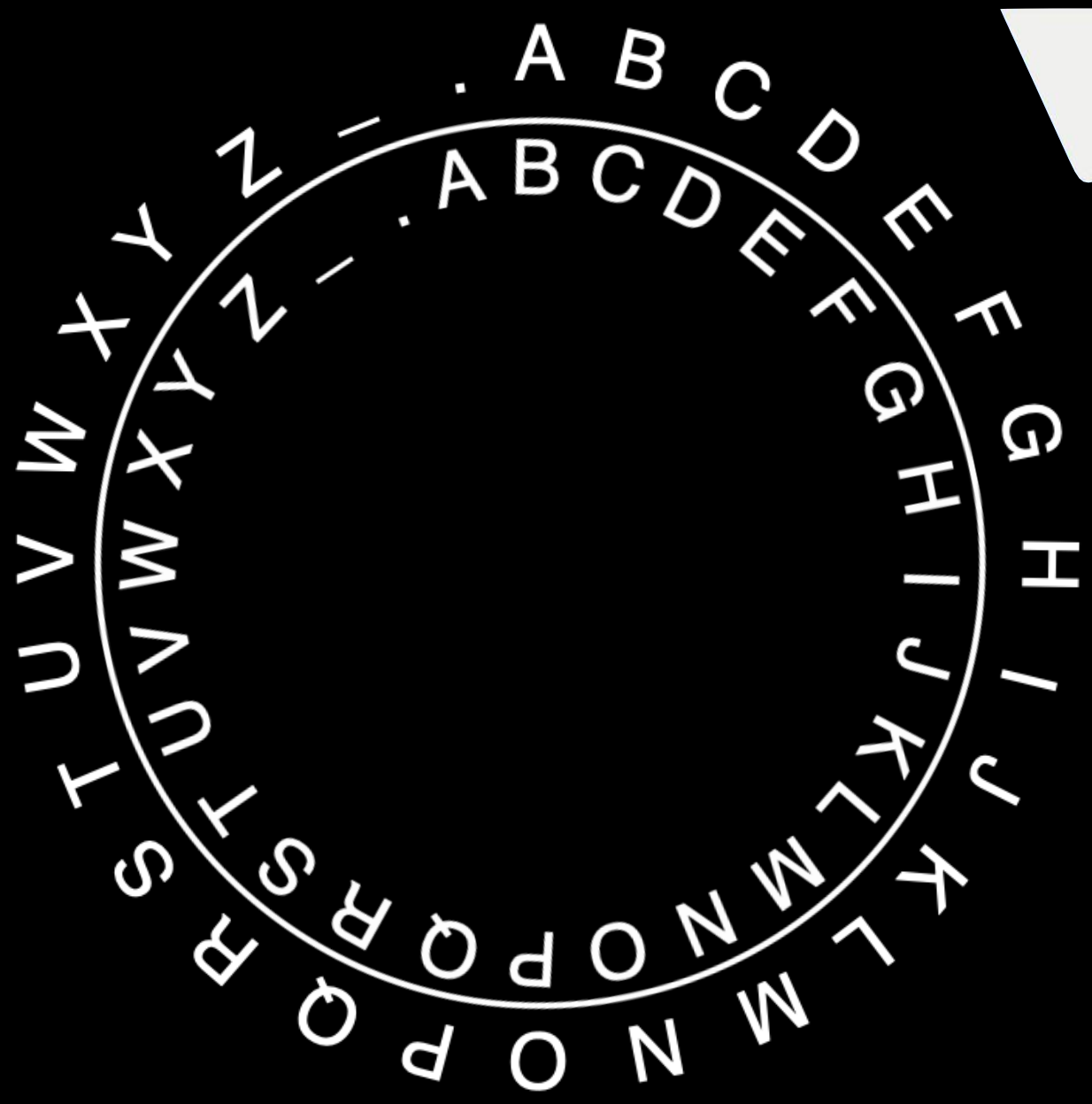


Printout available on [MIS Community Site]

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 Q R S T U V W X Y Z _ .
O

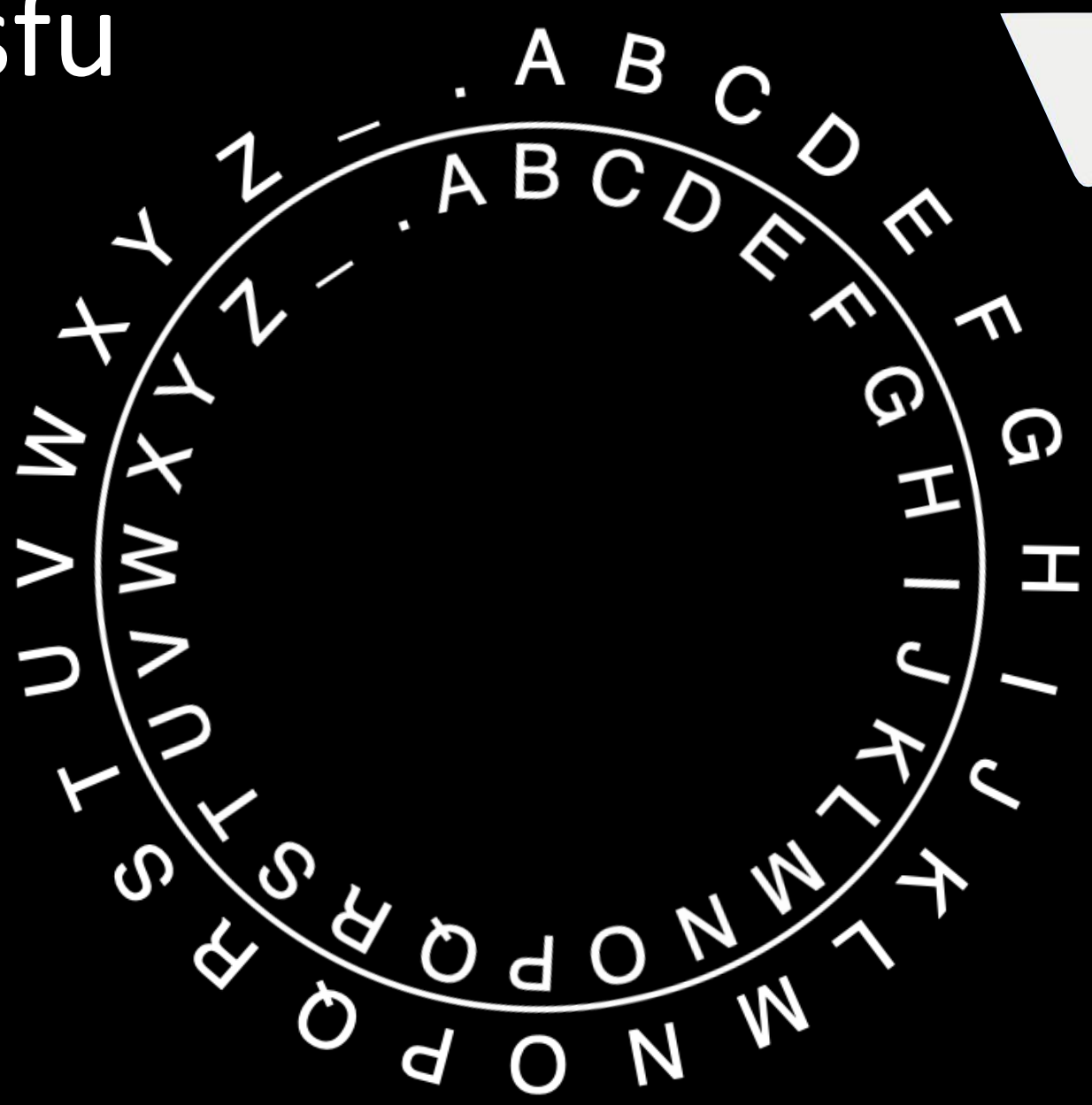
Secret


. 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 Q R S T U V W X Y Z _
O

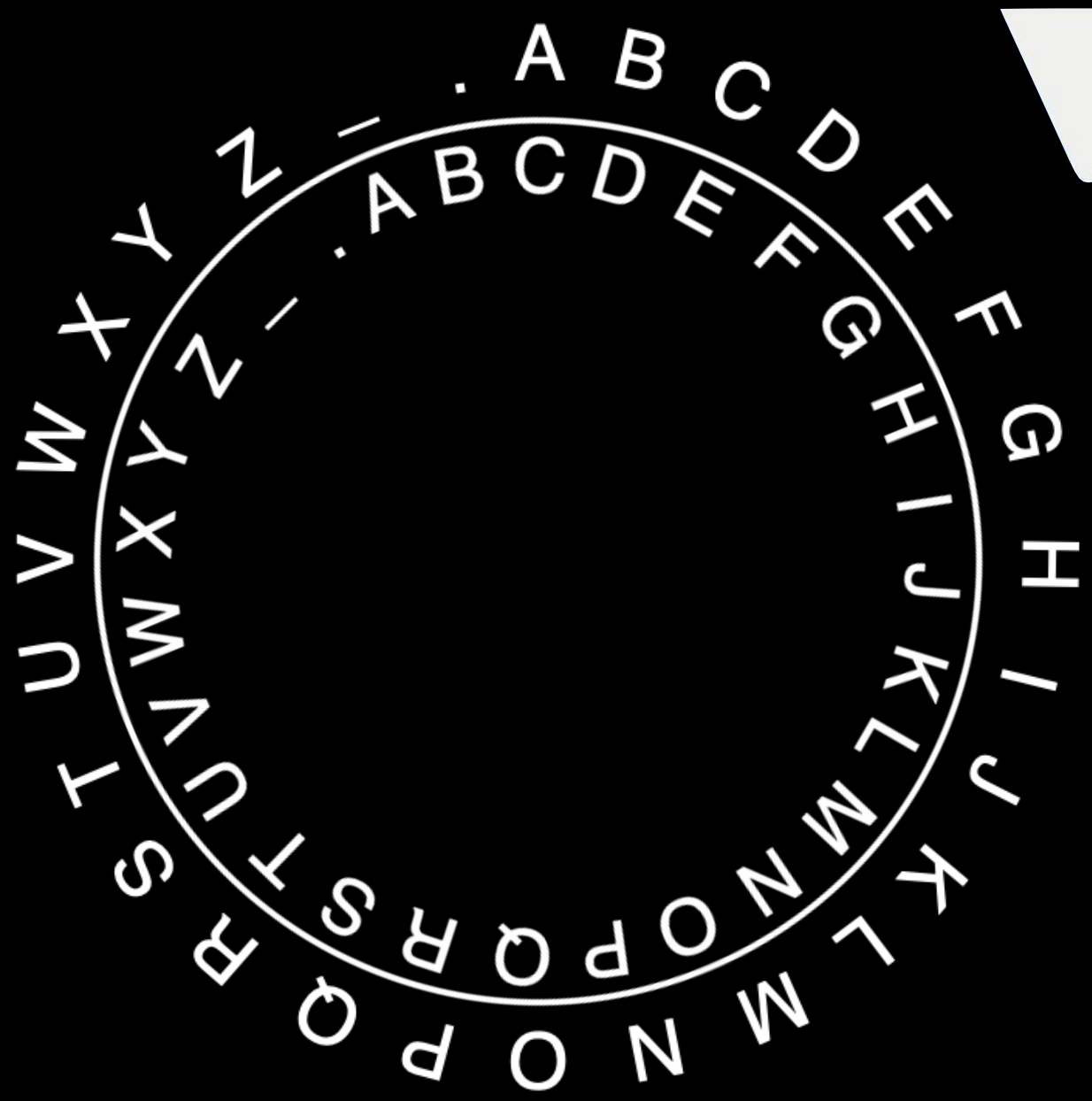

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _ .
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z _ .

1

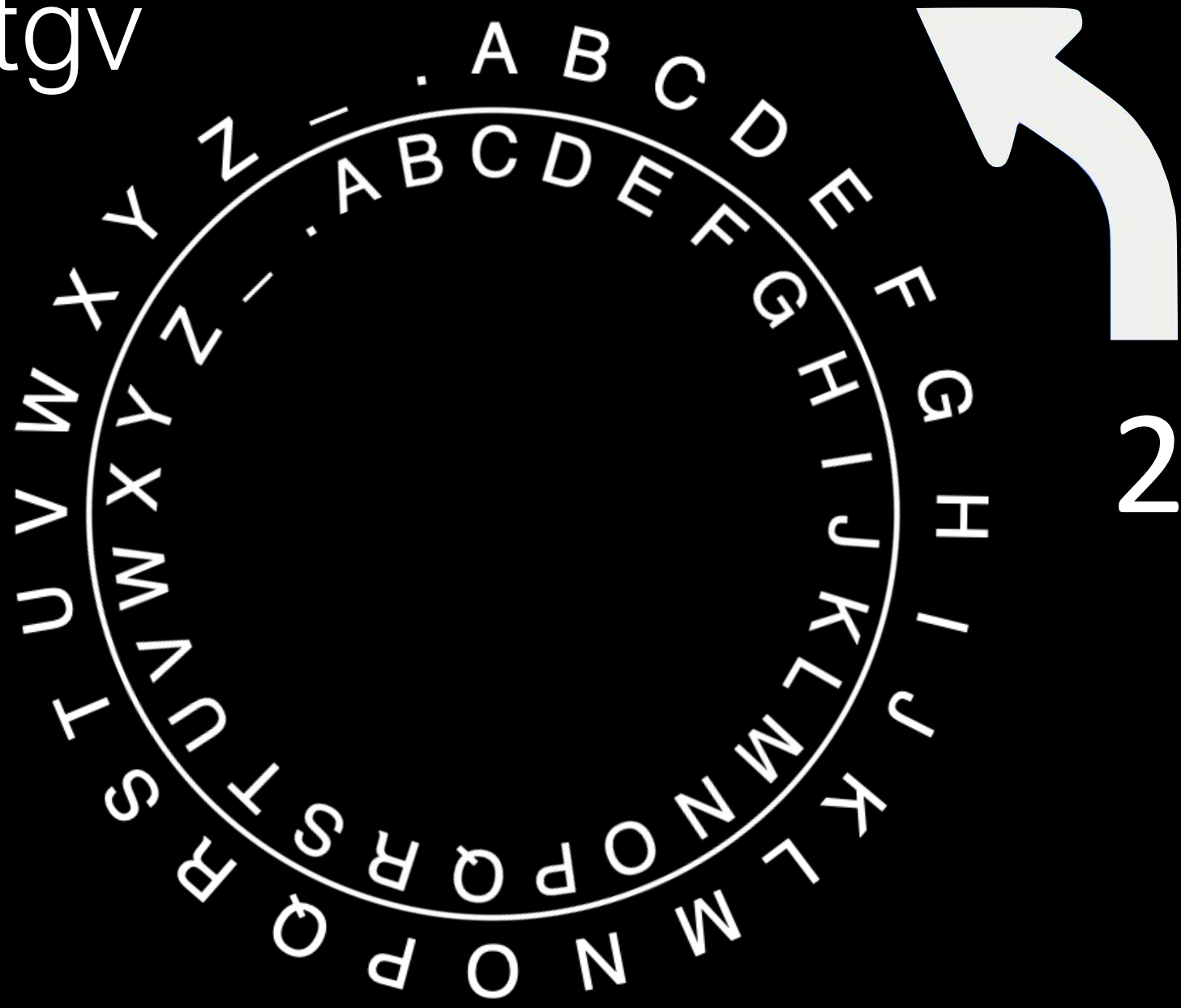
Tfdsfu


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 Q R S T U V W X Y Z _ .

1


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 Q R S T U V W X Y Z _ .
2

Ugetgv


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 Q R S T U V W X Y Z _ .
2

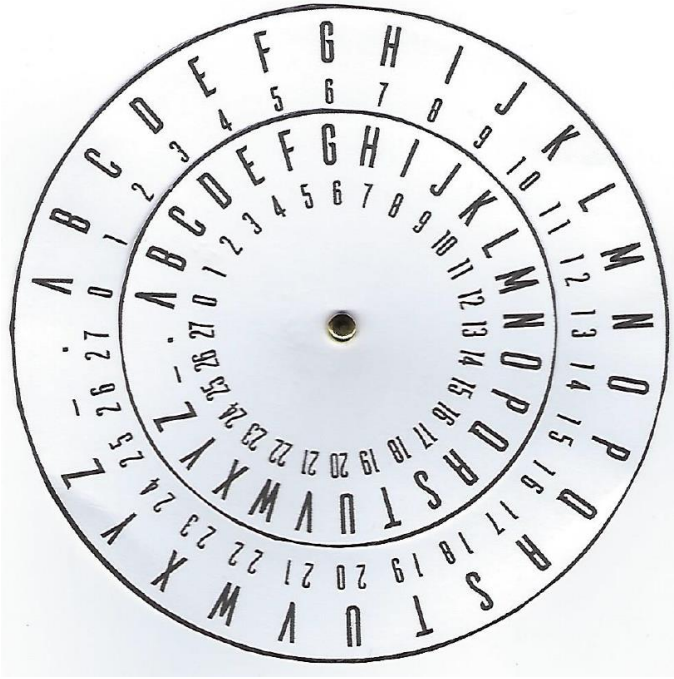
Using the Cipher Disk

Outer wheel is for the *plaintext* alphabet

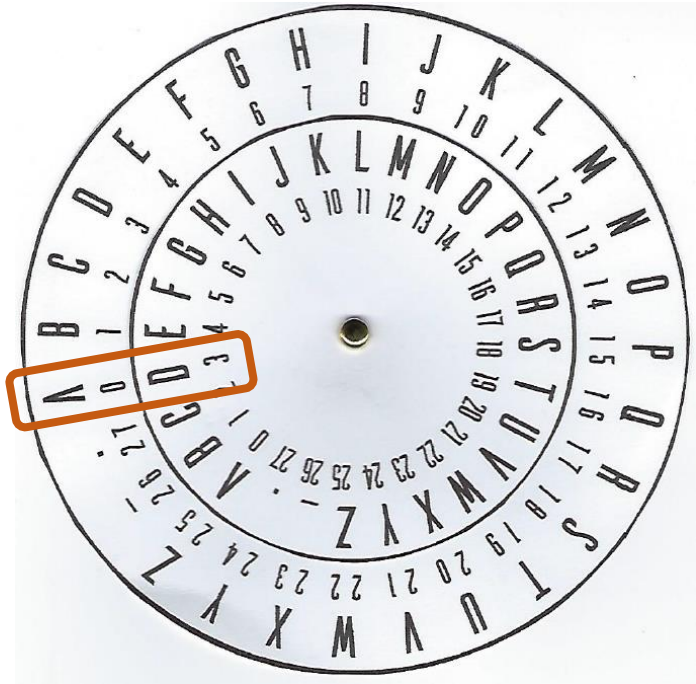
Inner wheel is for *ciphertext*

Setup the Cipher Disk: Make sure the letter “A” on the inner disk is aligned with the letter “A” on the outer disk

When the outer wheel and inner wheel and are both aligned at the letter “A” (i.e. position zero), there is no encryption mapping the letters on the outer wheel to letters on the inner wheel



1. Rotate the inner wheel <u>3 positions counter-clockwise</u>
   - ➢The position set on the inner wheel is the encryption “key”
   - ➢Key = 3 (A for plaintext aligns with D for ciphertext)

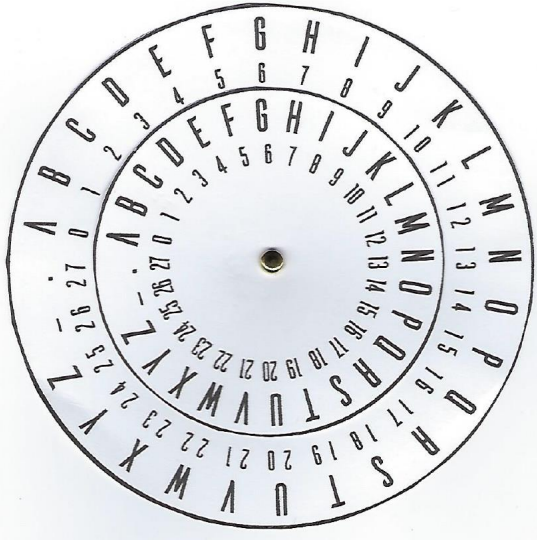


Encrypt the plaintext “SECRET”

Question: What is the resulting ciphertext?

VHFUHW

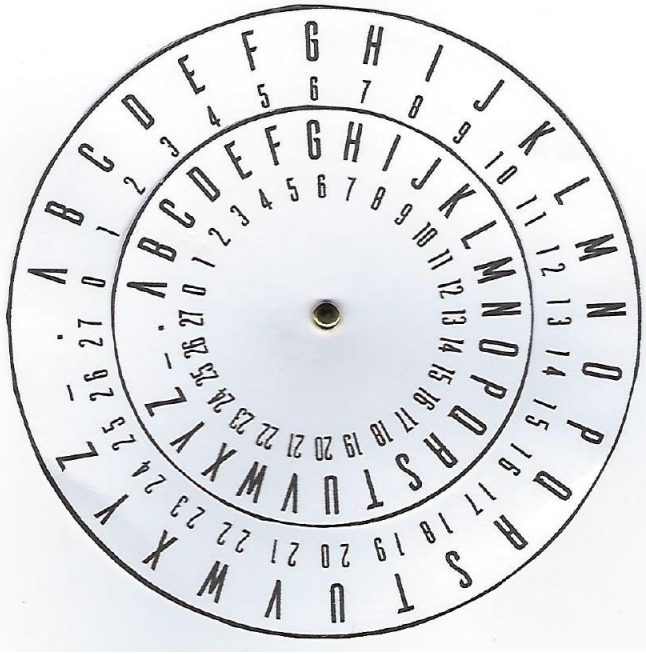
Using the Cipher Disk



2. Choose a different key (a number between 1 – 27)
   - We cannot use “0”, which will return the plaintext without encryption
   - Write the ciphertext on a piece of paper and think about how your friend could decrypt it…

Question: What is the maximum number of guesses needed to find the plaintext?

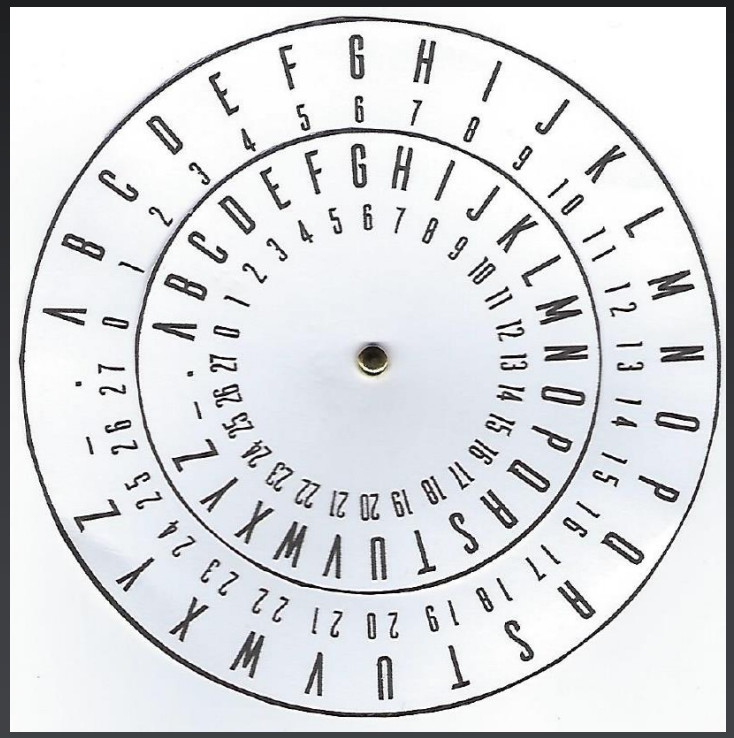
In-class activity: Cipher Disk



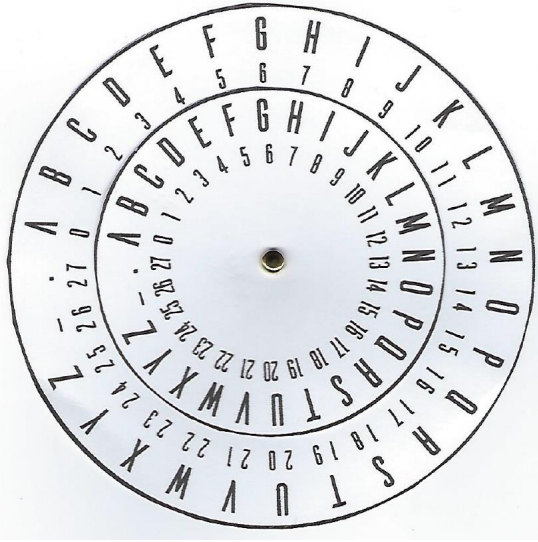
Question: What is the maximum number of guesses needed to find the plaintext?

- Answer: 28, the size of the alphabet 26 + “.” and “-”
- Guessing all possible keys is called “brute force search” or “brute forcing”

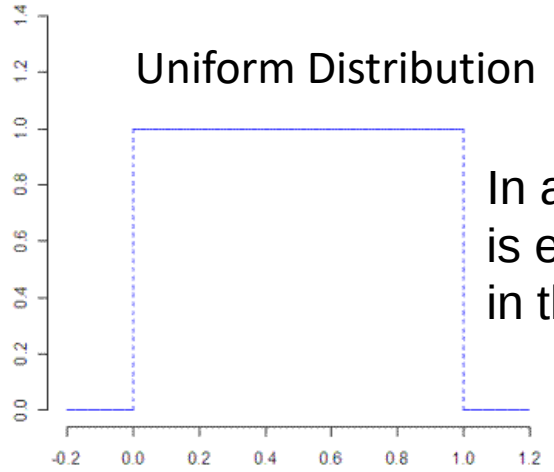
“Keyspace" is the number of possible keys



Question B: Assuming each key is equally likely (randomly distributed) how many random guesses would your friend likely have to make to find the key to decrypt the plaintext?



- Answer: ~14, (28 -1) = 27 and 27/2 = 13.5 which is approximately 14
  - Because the average of a uniform distribution is half
  - Recall 26 letters in the alphabet + "." and "-" = 28, but we cannot use "0" as the key which gives us the original plaintext back the size of the alphabet



In a uniform distribution any number is equally likely, the average is right in the middle, or half the distribution

- This is important in cryptography because the average number of attempts needed to successfully guess the key through brute forcing is half of the key space
- This is true of the simple cipher wheel as well as modern encryption schemes with very large key spaces.

Could your friend make fewer guesses than 14 guesses?

- **Question A:** What is the maximum number of guesses needed to find the plaintext?
  - **Answer:** The size of the keyspace
- **Question B:** Assuming each key is equally likely (randomly distributed) how many random guesses would your neighbor likely have to make ("on average") to find the key to decrypt the plaintext?
  - **Answer:** Half the size of the keyspace

Question C: If your friend did it faster than 14 or 27 attempts, how was your neighbor able to do it faster?

If it was not just a lucky guess, then they were likely using "cryptanalysis", the science of breaking codes

What strategies did might they use?

Linguistic cryptanalysis…

Examples:

- Recognizing the beginning of the word
- Looking for letter pairs
- Looking at vowels

This form of cryptanalysis uses your knowledge of the English language

Linguistic cryptanalysis examples…

One form of linguistic cryptanalysis is *frequency analysis of letters used in English*

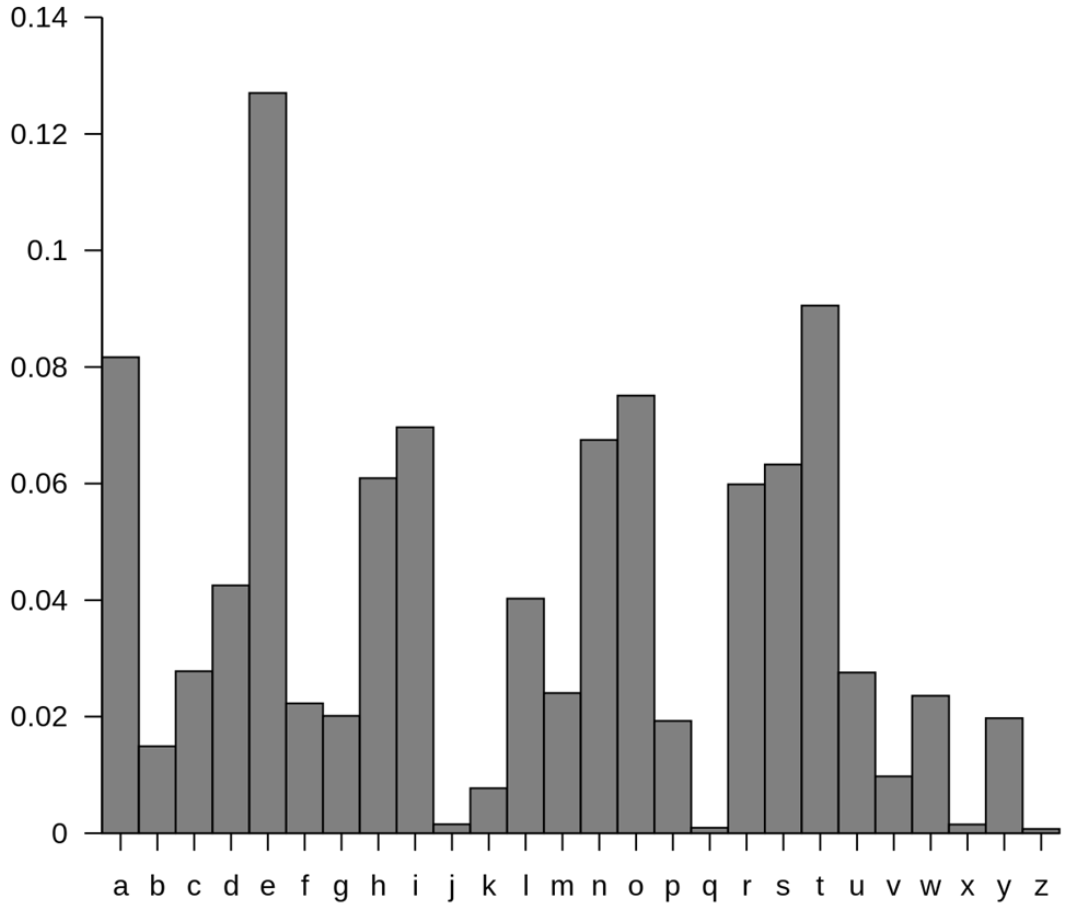
Frequency analysis recognizes that different letters have different probabilities of frequencies of use in words:

Given a sentences written in the English language

- E, T, A and O are the most common
- Z, Q and X are rare

- TH, ER, ON, and AN are the most common pairs of letters (termed bigrams or digraphs)

- SS, EE, TT, and FF are the most common repeats

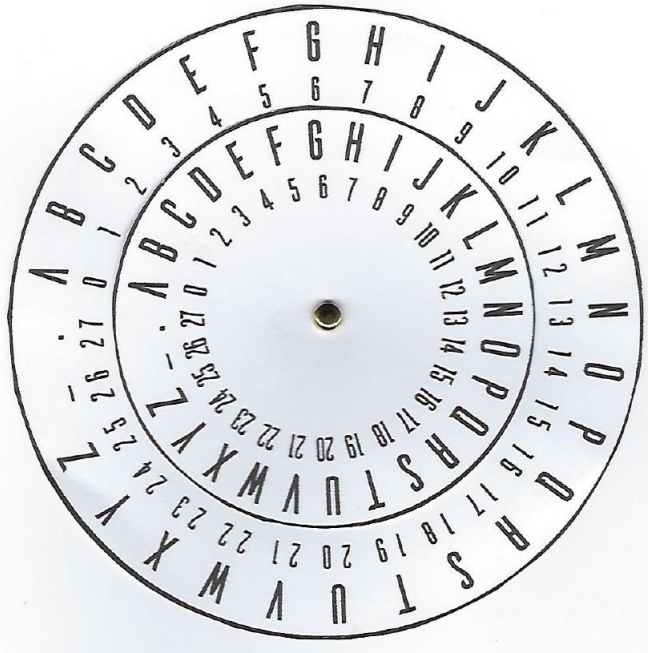


Example: Substitution cipher or algorithm

- A mono-alphabetic substitution cipher

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA
```

“SECURITY” <=> “HVXFIRGB”



Polyalphabetic Cipher

Ciphers can be made stronger, and frequency analysis made more difficult when more than one cipher alphabet is used

- For example, encrypt the plaintext message “SEND MONEY”
  - Use the word “SECURITY” as the key, but repeat its use in the key to make it have as many letters as the plaintext:

Plaintext: SEND MONEY (10 characters including the space “_”)

Key: SECURITYSE (10 characters)

1. Encrypt by rotating the inner wheel so that “s” in the word “security” aligns with “a” on the outer wheel. Now “s” in the word “send” on the outer wheel maps to the letter “i” on the inner wheel, so “i” is the ciphertext.

Polyalphabetic Cipher

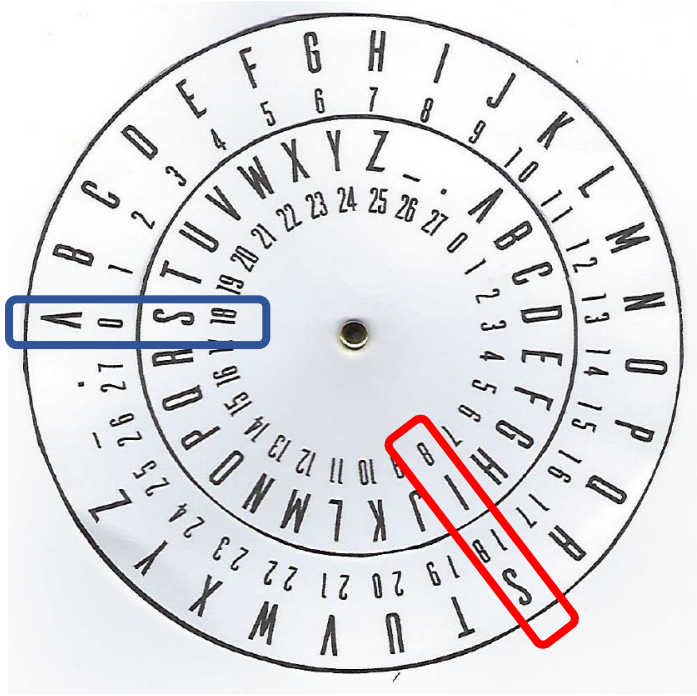
Plaintext: SEND MONEY (10 characters including the space "_")

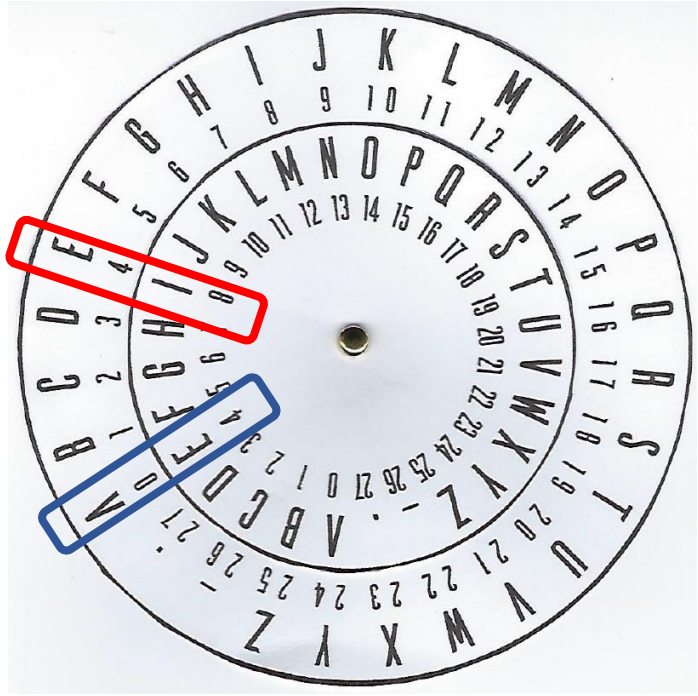
Key: SECURITYSE (10 characters)

1. Encrypt by rotating the inner wheel so that "S" in the word "SECURITY" aligns with "A" on the outer wheel
   Now "S" in the word "SEND" on the outer wheel maps to the letter "I" on the inner wheel, so "I" is the ciphertext

2. Next, rotate the inner wheel so that "E" in the word "SECURITY" aligns with "A" on the outer wheel. Now "E" in the word "SEND" on the outer wheel maps to "I" on the inner wheel, so "I" is the ciphertext again, even though the plaintext is different than before

Question D: What is the rest of the ciphertext for "SEND MONEY" using the polyalphabetic key "SECURITY"?
Compare your answer to your neighbor's





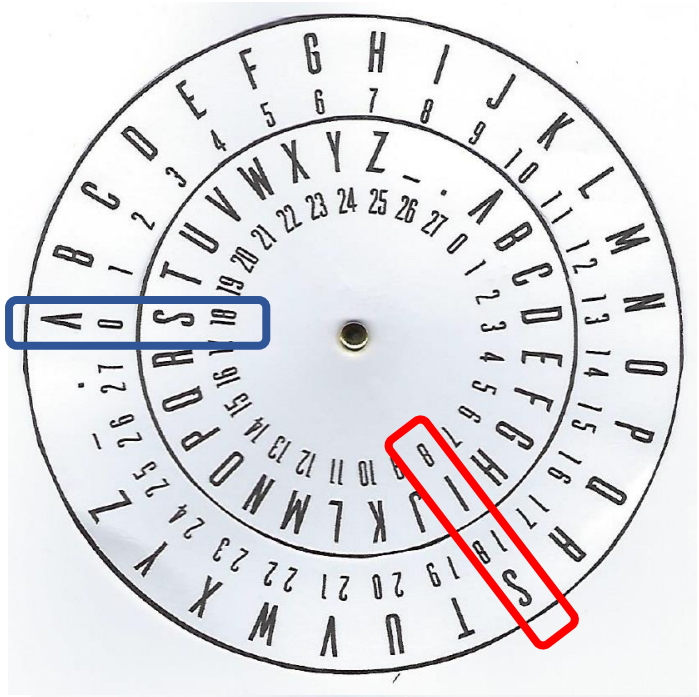
Polyalphabetic Cipher

Plaintext: SEND MONEY (10 characters including the space "_")

Key: SECURITYSE (10 characters)

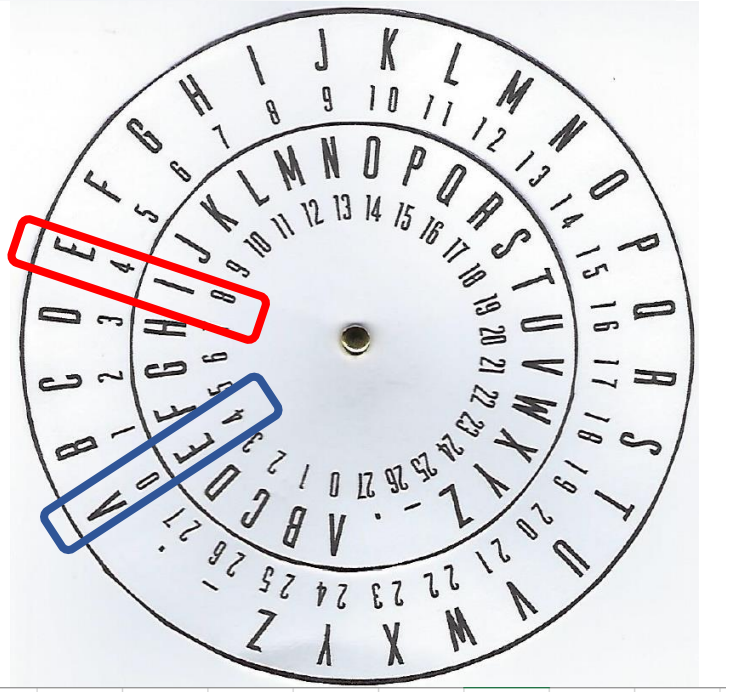
Question D: What is the rest of the ciphertext for "SEND MONEY" using the polyalphabetic key "SECURITY"?

IIPXPUFJWA



Polyalphabetic ciphers make frequency analysis more difficult

Polyalphabetic substitution is another building block of cryptography



To help you, use the following formula:

- Encryption: ciphertext = (plaintext + key) mod 28
- Decryption: plaintext = (ciphertext - key) mod 28

Number your alphabet so that it starts with zero, e.g., A = 0, Z=25, _ = 26, . = 27
This means that your alphabet will be abcdefghijklmnopqrstuvwxyz_.
As a general rule for shift ciphers, *the modulus is always the size of the alphabet, but you must start your alphabet at 0*

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	_	.
0	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	27

Random Polyalphabetic Cipher

What if we use a random polyalphabetic key that is as long as the message?

For example, let's say our plaintext is:

We intend to begin on the first of February unrestricted submarine warfare.

And the polyalphabetic key is a string of random characters as long as the message:

ackwulsjwkblogbzcukn.kqubpnnefjvcebuymaclzvzmzwfbxpmmzqwmm.tejzfutjcqrsf_hq

Question E: How can an attacker attempt to crack this message?
Is an attack possible?

Services of cryptosystems

- **Confidentiality** – Renders information unintelligible except by authorized entities
- **Integrity** – Data has not been altered in an unauthorized manner since it was created, transmitted, or stored
- **Authentication** – Verifies the identity of the user or system that created, requested or provided the information
- **Nonrepudiation** – Ensure the sender cannot deny sending the information

Repudiation – the sender denying she/he sent the message

Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

Cipher = encryption algorithm

2 main attributes combined in a cypher

1. **Confusion:** usually carried out through substitution
2. **Diffusion:** Usually carried out through transposition

Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

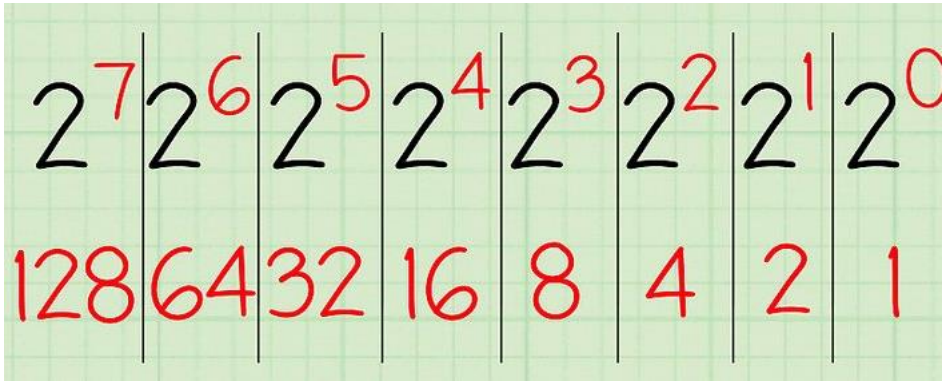
Translating what we type, into ASCII, and then into binary… which is what is sent as data packets across the network to other computers…

Binary – Decimal

0 0 0 0 0 0 0 0 = 0

1 1 1 1 1 1 1 1 = 255

8 bits supports 256 numbers



ASCII - Decimal

Dec	Hex	Name	Char	Ctrl-char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	0	Null	NUL	CTRL-@	32	20	Space	64	40	@	96	60	`
1	1	Start of heading	SOH	CTRL-A	33	21	!	65	41	A	97	61	a
2	2	Start of text	STX	CTRL-B	34	22	"	66	42	B	98	62	b
3	3	End of text	ETX	CTRL-C	35	23	#	67	43	C	99	63	c
4	4	End of xmit	EOT	CTRL-D	36	24	$	68	44	D	100	64	d
5	5	Enquiry	ENQ	CTRL-E	37	25	%	69	45	E	101	65	e

ASCII Character Table

Name	Hex	Dec
. (period)	2E	046
0	30	048
1	31	049
2	32	050
3	33	051
4	34	052
5	35	053
6	36	054
7	37	055
8	38	056
9	39	057

Name	Hex	Dec
A	41	065
B	42	066
C	43	067
D	44	068
E	45	069
F	46	070
G	47	071
H	48	072
I	49	073
J	4A	074
K	4B	075

Name	Hex	Dec
L	4C	076
M	4D	077
N	4E	078
O	4F	079
P	50	080
Q	51	081
R	52	802
S	53	083
T	54	084
U	55	085
V	56	086

Name	Hex	Dec
W	57	087
X	58	088
Y	59	089
Z	5A	090

XOR – Exclusive OR

Creating “confusion” (i.e. substitution) through a binary mathematical function called “exclusive OR”, abbreviated as XOR

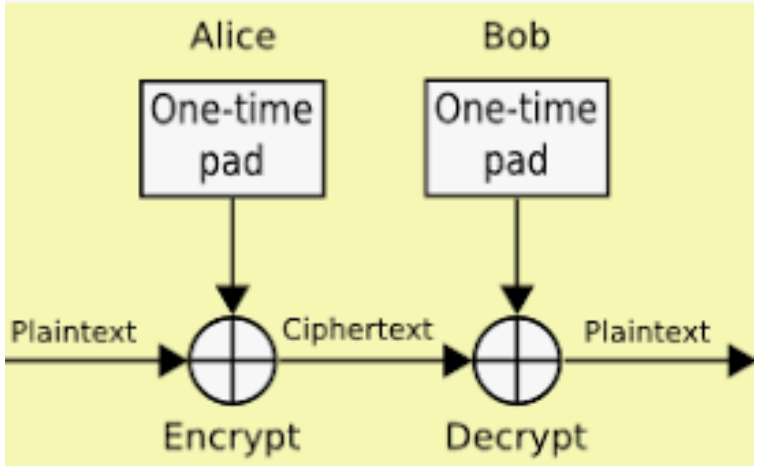
Message stream:	1001010111
Keystream:	0011101010
Ciphertext stream:	1010111101

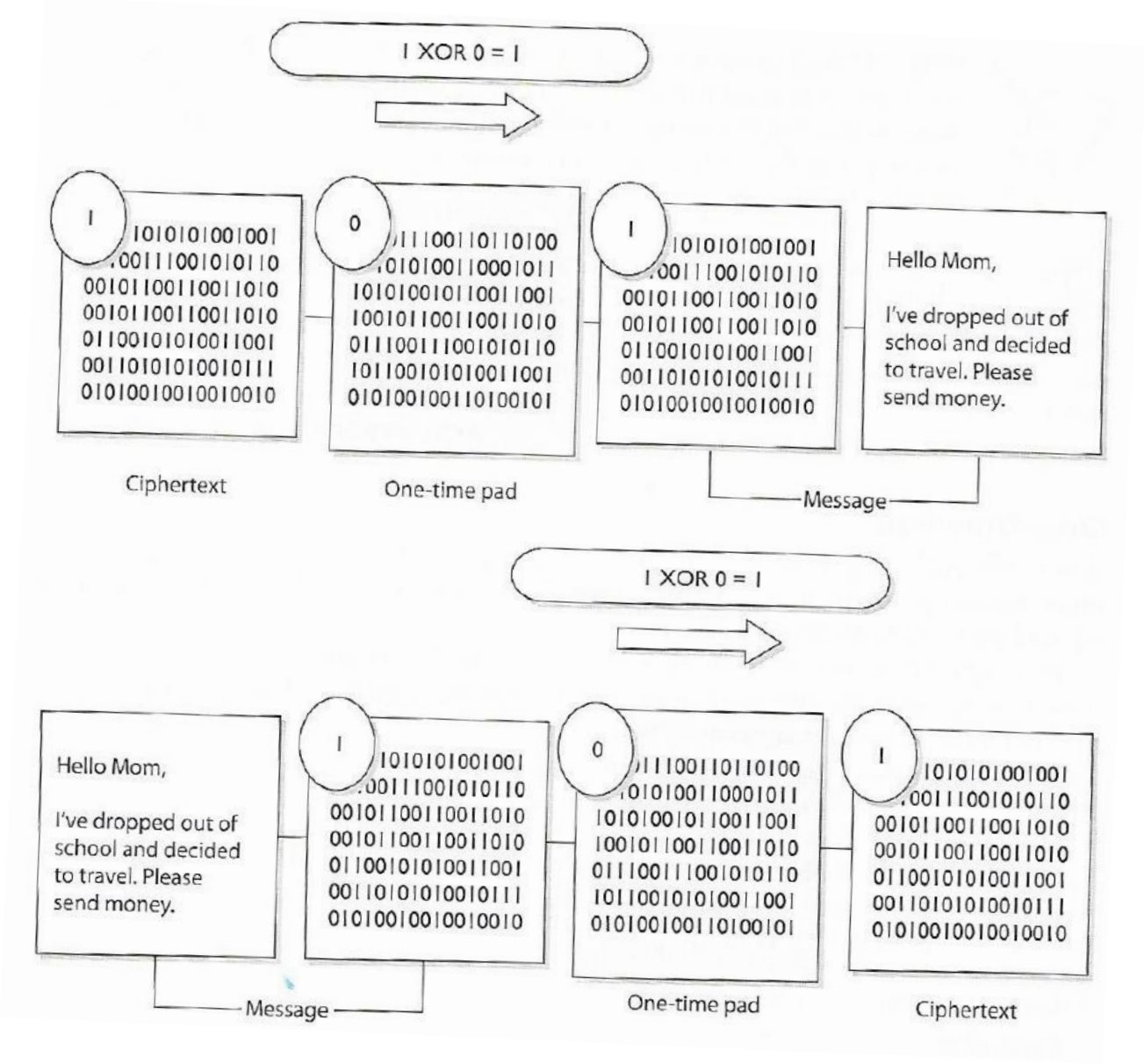
Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

One-Time Pad *a perfect encryption scheme*

One-Time Pad Requirements

- Made up of truly random values
- Used only one time
- Securely distributed to its destination
- Secured at sender's and receiver's sites
- At least as long as the message

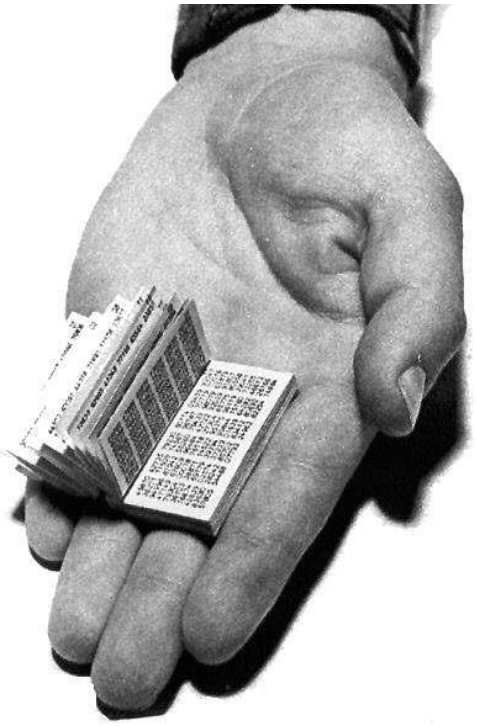




Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

One-time pad -- Problems

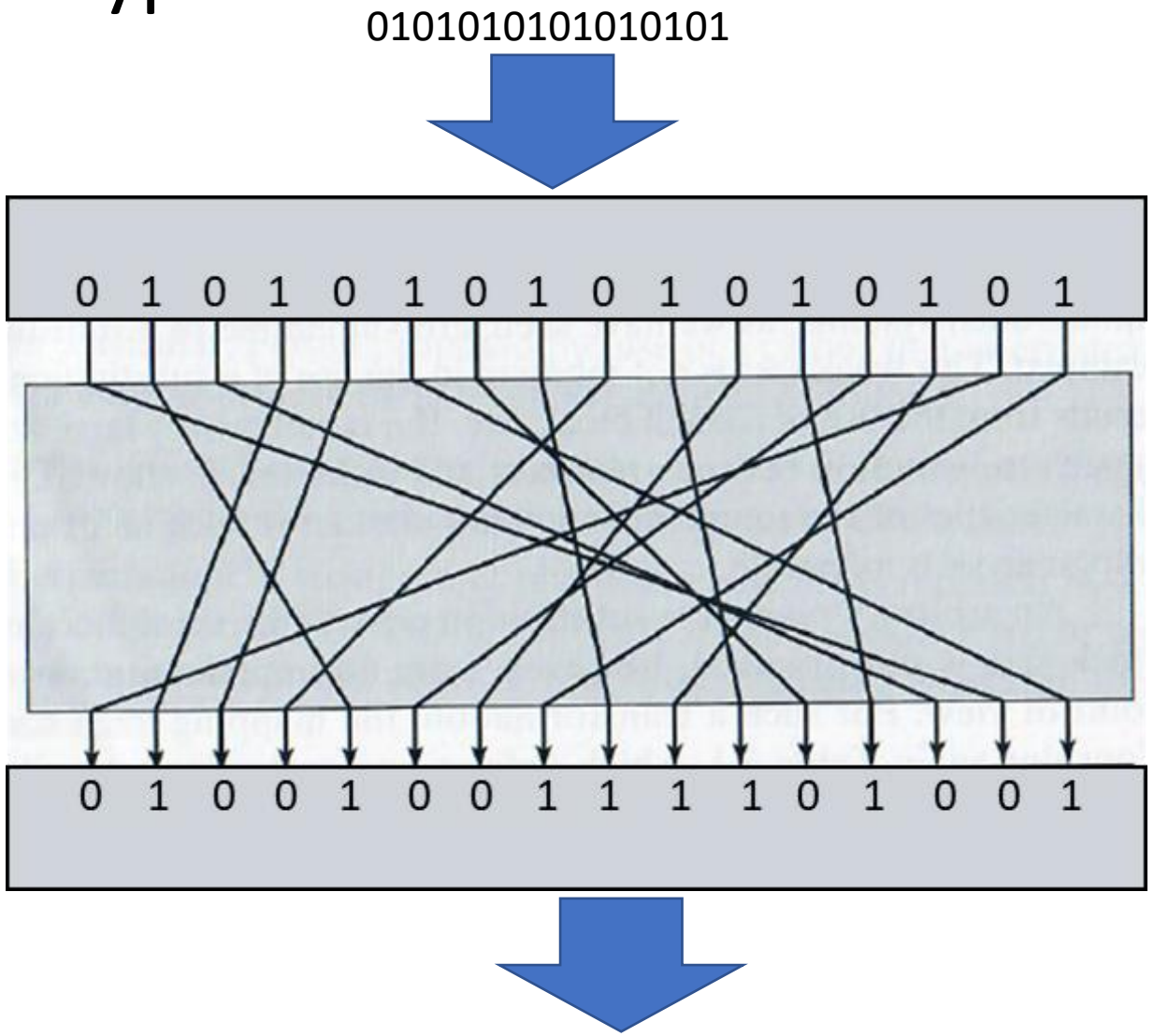
- Must be *perfectly random*
- Pad must be as long as the message
- Must be used **only once**
  - Skimp on any of these conditions, it becomes trivial to break your system
- Any software product claiming to use one-time pad is **snake-oil**.
  - Computers are bad at generating *truly* random numbers



2 main attributes combined in a cypher

1. Confusion: usually carried out through substitution

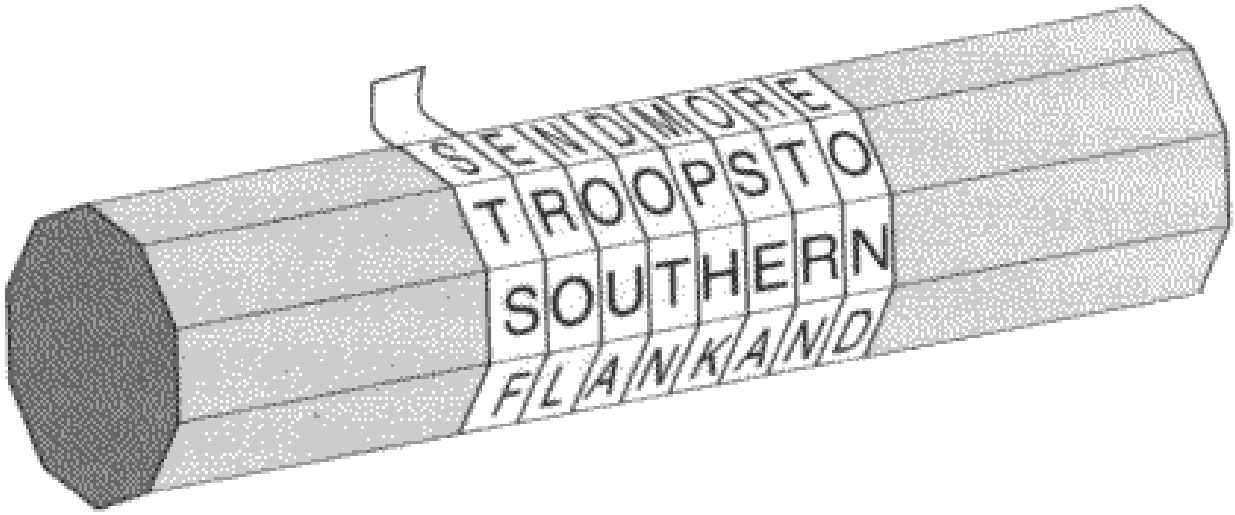
2. **Diffusion:** Usually carried out through transposition



Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

Transposition

- Ancient example: scytale



A profit was achieved by our ACT unit

a p r o f i t w a s
a c h i e v e d b y
o u r a c t u n i t

0 1 2 3 4 5 6 7 8 9

a p r o f i t w a s
a c h i e v e d b y
o u r a c t u n i t

6 0 2 5 4 8 7 1 3 9

t a r i f a w p o s
e a h v e b d c i y
u o r t c i n u a t

0 1 2 3 4 5 6 7 8 9

a p r o f i t w a s
a c h i e v e d b y
o u r a c t u n i t

How would you apply the transposition method using the key: SECURITY ?

1. Transform the key into a numeric representation based on alphabetic order:

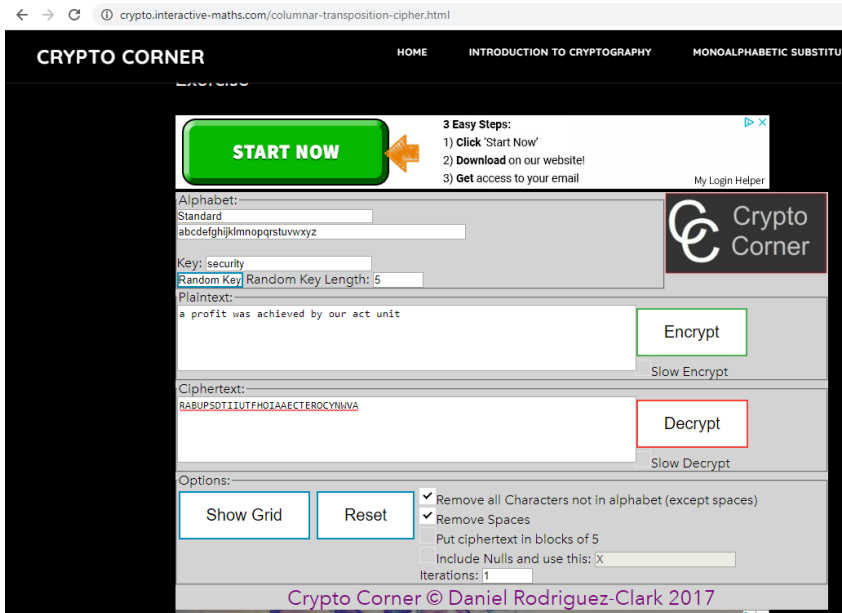
S	E	C	U	R	I	T	Y
5	2	1	7	4	3	6	8

2. Lay out the plaintext in columns aligned with the key:

S	E	C	U	R	I	T	Y
5	2	1	7	4	3	6	8
a	p	r	o	f	i	t	w
a	s	a	c	h	i	e	v
e	d	b	y	o	u	r	a
c	t	u	n	i	t	_	_

3. Reorganize the columns based on alphabetical order, collect data in row order:
*rabupsdtiiutfhoiaaecter_ocynwva_*

https://crypto.interactive-maths.com/columnar-transposition-cipher.html



Dichotomies is cryptography

- Symmetric versus Asymmetric
- Stream versus block
- 2-way functions versus 1-way functions

Symmetric versus asymmetric algorithms

- Symmetric cryptography
  - Use a copied pair of symmetric (identical) secret keys
  - The sender and the receive use the same key for encryption and decryption functions
- Asymmetric cryptography
  - Also know as “public key cryptography”
  - Use different (“asymmetric”) keys for encryption and decryption
  - One is called the “private key” and the other is the “public key”

Symmetric cryptography

Strengths:

- Much faster (less computationally intensive) than asymmetric systems.
- Hard to break if using a large key size.

Symmetric cryptography is 1,000 times faster than Asymmetric cryptography

Weaknesses:

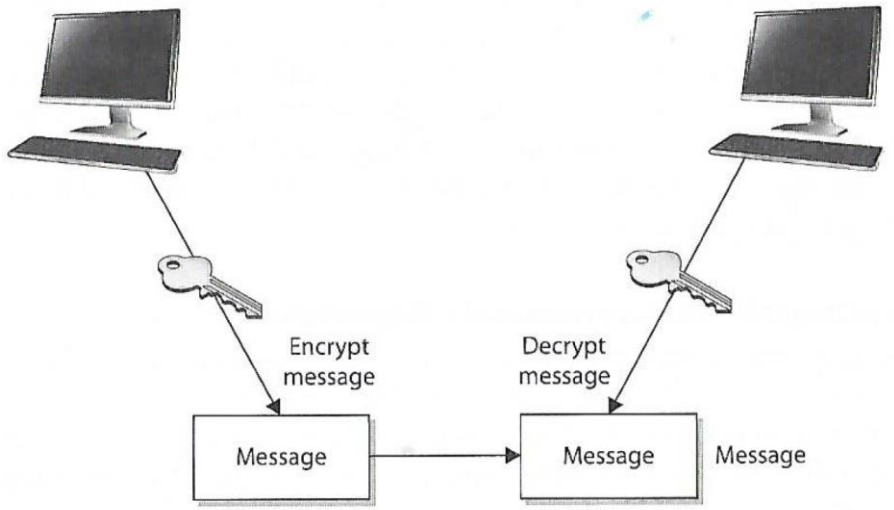
- Requires a secure mechanism to deliver keys properly.
- Each pair of users needs a unique key, so as the number of individuals increases, so does the number of keys, possibly making key management overwhelming.
- Provides confidentiality but not authenticity or nonrepudiation.

Two types: Stream and Block Ciphers

- **Stream Ciphers** treat the message a stream of bits and performs mathematical functions on each bit individually

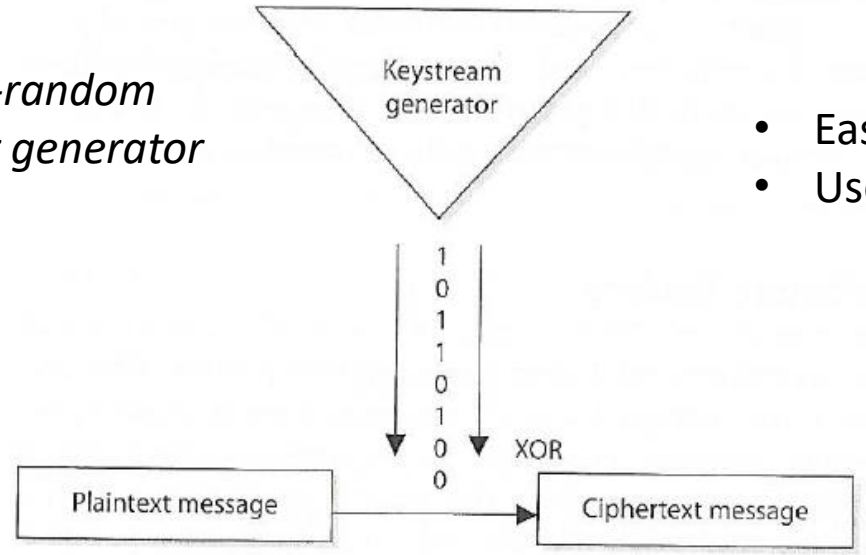
- **Block Ciphers** divide a message into blocks of bits and transforms the blocks one at a time

Symmetric encryption uses the same keys.



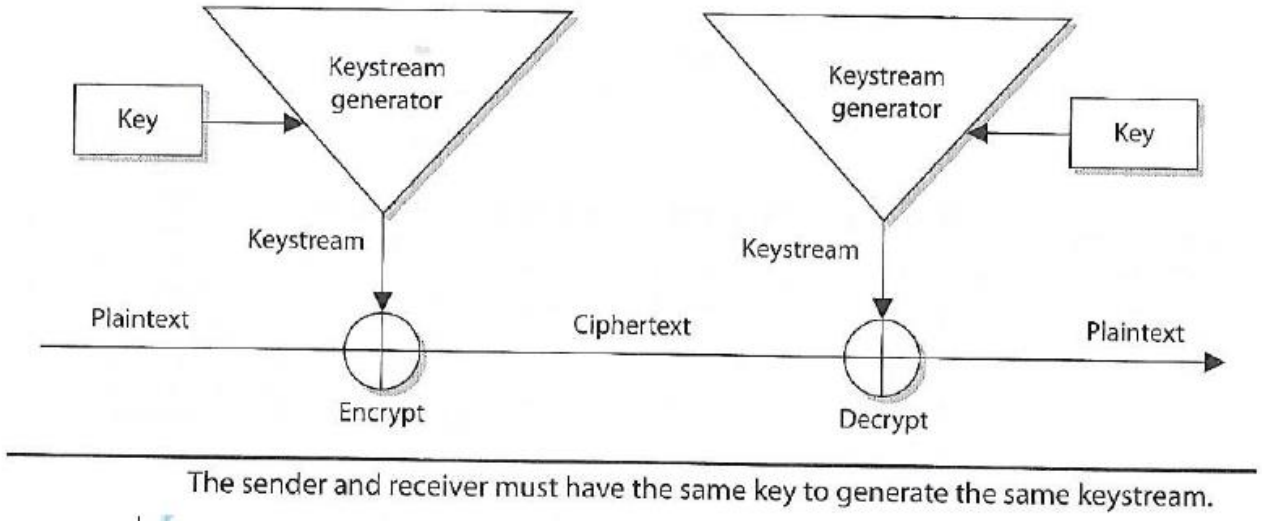
Symmetric Stream Ciphers

Pseudo-random number generator (PRNG)



- Easy to implement in hardware
- Used in cell phones and Voice Over Internet Protocol

Wi-Fi access points (like the one on the classroom ceiling) and cell phone use stream ciphers to encrypt/decrypt data they send and receive



Harris, S. and Maymi, F. (2016) All-In-One CISSP Exam Guide, McGraw Hill Education

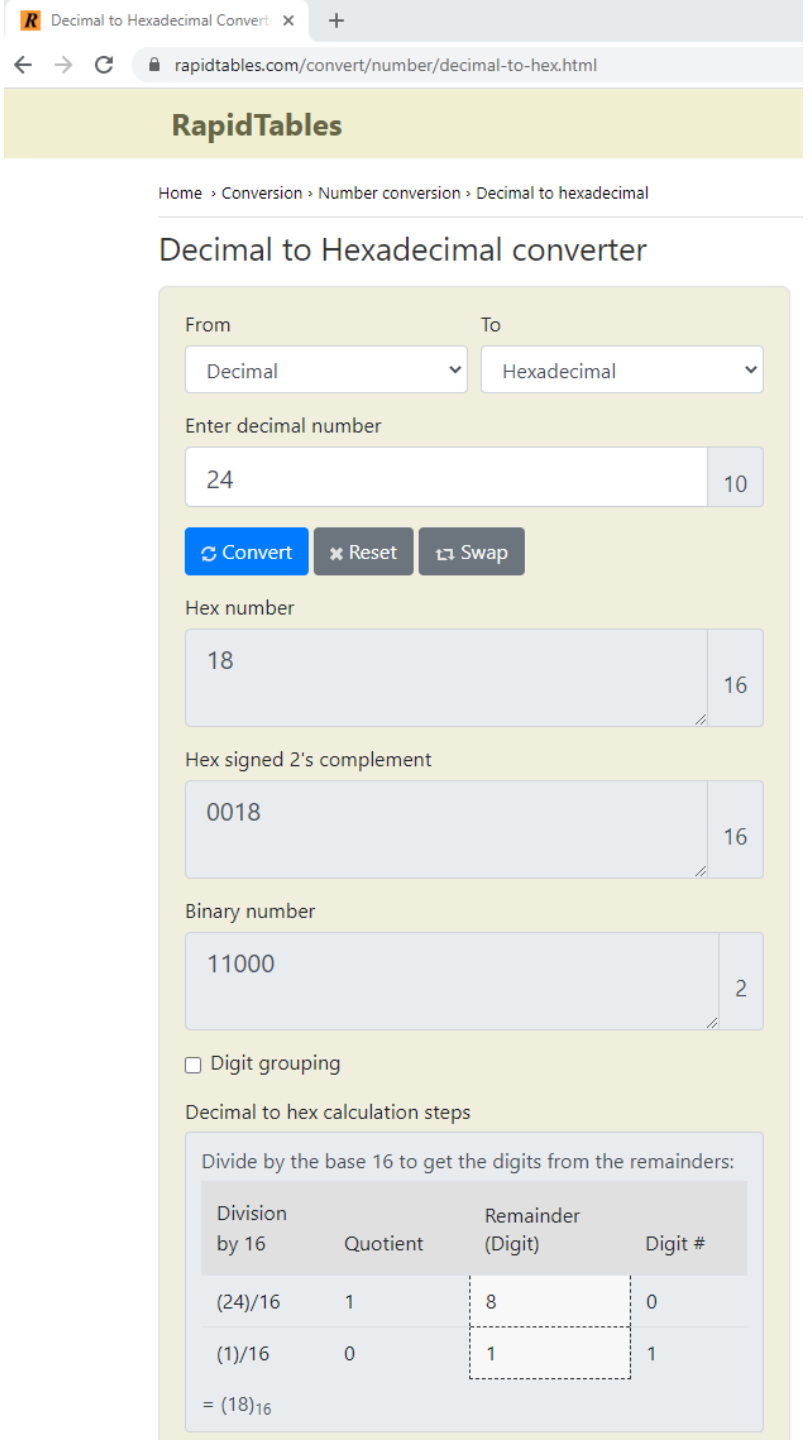
One more thing…

Hex	Binary	Octal	Decimal
0	0	0	0
1	1	1	1
2	10	2	2
3	11	3	3
4	100	4	4
5	101	5	5
6	110	6	6
7	111	7	7
8	1000	10	8
9	1001	11	9
A	1010	12	10
B	1011	13	11
C	1100	14	12
D	1101	15	13
E	1110	16	14
F	1111	17	15

- **Hexadecimal ("hex“)** is a number system made up of 16 symbols (base 16)
  - Our standard numeral system, decimal (base 10) uses 10 symbols: 0,1,2,3,4,5,6,7,8,9
  - Hexadecimal uses 16 symbols: 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F
  - There are no numerical symbols that represent values greater than 9, so English alphabet letters are used
  - For example: Hexadecimal A = decimal 10, and Hexadecimal F = decimal 15
- Humans mostly use the decimal system, probably because humans have ten fingers on our hands
- Computers only have on and off, called a binary digit (or bit)
- A binary number is just a string of zeros and ones, e.g. 11011011
- For convenience, engineers working with computers tend to group bits together
- In earlier days, such as the 1960s, they would group 3 bits at a time, 3 bits, each being on or off, can represent the eight numbers from 0 to 7:
  - 000 = 0; 001 = 1; 010 = 2; 011 = 3; 100 = 4; 101 = 5; 110 = 6 and 111 = 7. This is called **octal**
- As computers got bigger, it was more convenient to group bits by four instead of three to double the numbers that the symbol would represent; giving it 16 hexadecimal values instead of eight
- In computer jargon four bits make a *nibble* (sometimes spelled *nybble*). A nibble is one hexadecimal digit, written using a symbol 0-9 or A-F
- Two nibbles make a byte (8 bits). Most computer operations use the byte, or a multiple of the byte (16 bits, 24, 32, 64, etc.). Hexadecimal makes it easier to write these large binary numbers.
- To avoid confusion with decimal, octal or other numbering systems, hexadecimal numbers are sometimes written with a "h" after or before the number. For example, 63h and 0x63 mean 63 hexadecimal

https://simple.wikipedia.org/wiki/Hexadecimal

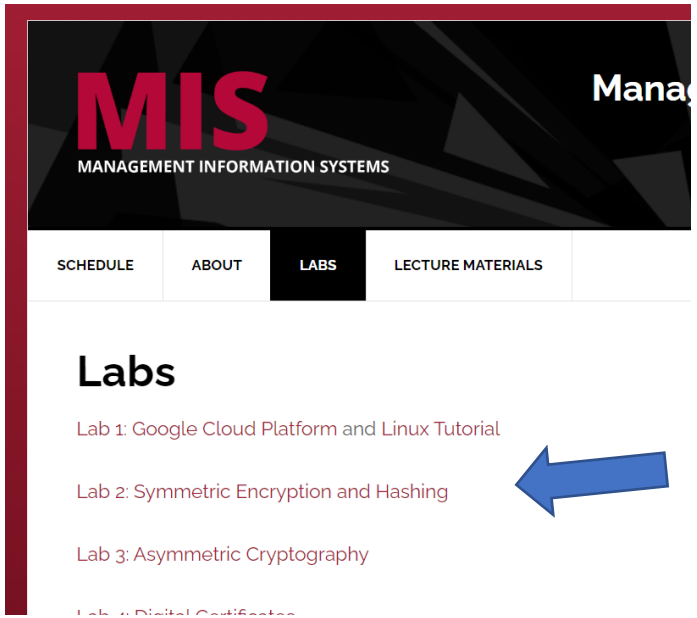
One more thing…

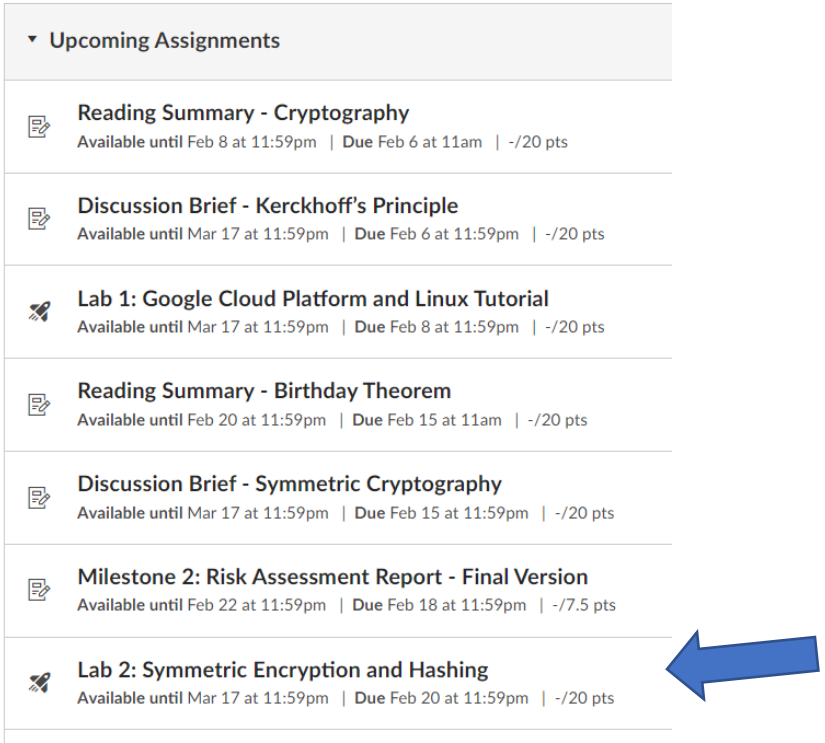


Hex	Binary	Octal	Decimal
0	0	0	0
1	1	1	1
2	10	2	2
3	11	3	3
4	100	4	4
5	101	5	5
6	110	6	6
7	111	7	7
8	1000	10	8
9	1001	11	9
A	1010	12	10
B	1011	13	11
C	1100	14	12
D	1101	15	13
E	1110	16	14
F	1111	17	15

Symmetric Encryption Lab

- https://security-assignments.com/labs/lab_hashing_and_symmetric_encryption.html
- Today's lecture should help you do "Part 1" of the lab
- Next class we will cover hashing and equip you to finish "Part 2"





Agenda

- ✓Cryptography terminology
- ✓Substitution
- ✓Transposition
- ✓Symmetric key cryptography
- ✓Symmetric stream cryptography
- ✓Next: Symmetric Encryption Lab