COMP482
Cybersecurity
Week 5 - Monday

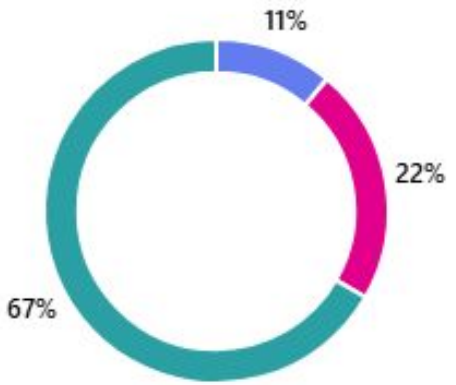
Dr. Nicholas Polanco
(he/him)

KALAMAZOO COLLEGE

1. How would you describe the timing of lectures?

More details

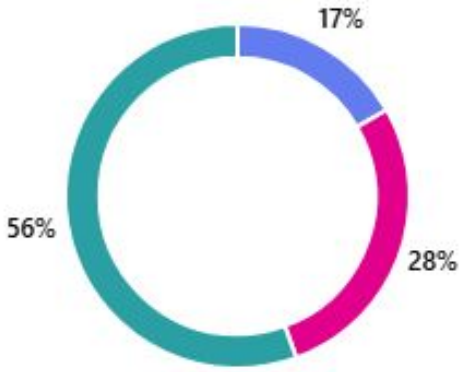
Too long	2
Too short	4
Just right	12



2. How would you describe the content in the lectures?

More details

Too much detail	3
Not enough detail	5
Just right	10



Survey Results

What other comments do you have about lectures?

- **I had a lot of people asking for the slides, because we move rather quick.**
  - *I have no problem making the slides available after class, I just want to make sure people are engaged and continue coming to class. I often see a sharp drop off once I make slides available.
- **I had notes about how much we cover (a lot), and maybe going a bit more in-depth on things**
  - *I can also make this adjustment, due to the nature of the class I am trying to cover as much of the entire field as possible. However, I will probably ask for input on lectures I could either skip, shorten, or extend

4. How would you describe the time allotted for activities?

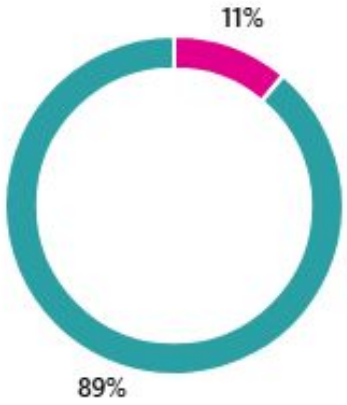
More details

Too much time	0
Not enough time	7
Just right	11

5. How would you describe the content in the activities?

More details

Confusing	0
Far too simple	2
Just right	16



Survey Results (continued)

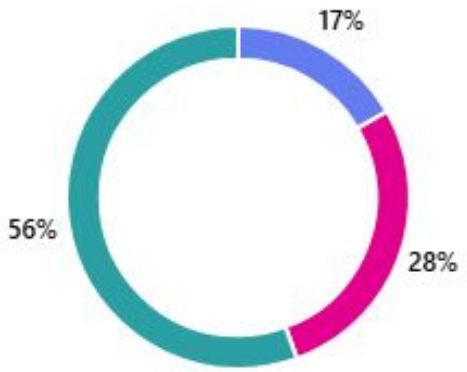
What other comments do you have about activities?

- **The main comment here was about having additional time (perhaps an entire class period).**
  - *This was the intention of those flex days, I am sorry I took one of them away last week due to my absence. Perhaps I can remove one of the lectures we have coming up (insider threats) and instead do a work day so people can catch-up on things. I can adjust the schedule for this.

7. How would you describe the discussion aspect of class?

More details

Too much discussion	3
Not enough discussion	5
Just right	10



8. How would you describe the value of discussion in the class?

More details

The discussion is essential	10
The discussion has no value	0
It depends on the lecture	8

Survey Results (continued)

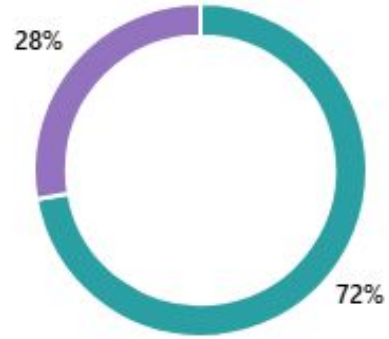
What other comments do you have about discussions?

- **I had a lot of comments about students either disliking discussions where we don't have a right or a wrong answer, but also students who think right or wrong prompts are too easy.**
- **I also had notes about students not liking the debate style, and some students really liking these.**
  - *This has me confused, I think I need to just keep it as is? I am open to suggestions for these.

10. How would you describe the difficulty of the class in relation to other classes?

More details

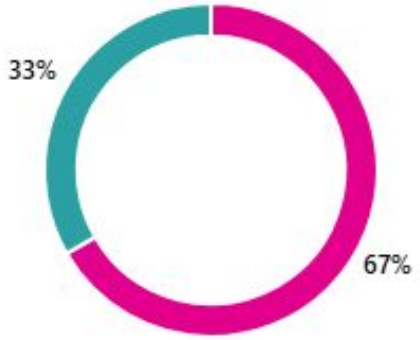
The class is too difficult	0
The class is too easy	0
The class is just right	13
The class is easy, but I don't want to do more work.	5



11. How would you describe the change in your cybersecurity knowledge since the course began?

More details

I have learned nothing	0
I have learned a lot	12
I have learned a fair amount	6



12. How would you describe the classroom environment?

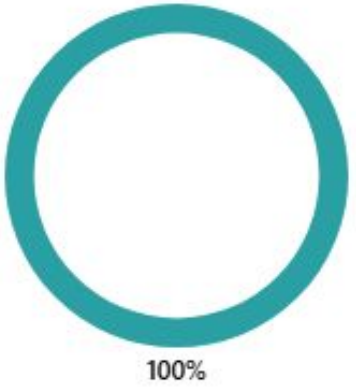
More details

I enjoy coming to class and I feel comfortable sharing my opinion	17
I hate coming to class and I feel uncomfortable sharing my opinion	0
I am neutral	1

13. How would you describe the collaboration aspect of the class?

More details

I think we are allowed to work in groups too often, we should do more independent work	0
I don't think we are encouraged to work in groups enough	0
The collaboration aspect is perfect	18



Important Notes

- Your presentations are due a **Week from today (Wednesday - Week 5)**
  - This is an academic presentation, you will need citations.
  - I'm not going to tell anyone to dress up, but be "presentable"
  - We will select the order **today**
- I am going to set aside some class time today and Wednesday to allow us to work and catch up on things
  - This includes your IoT activity, topic presentation, and activity for today

Important Dates (Week 5)

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
		IoT Activity Topic Deliverable: Topic Presentation		Reflection Week 4		

Cryptography

Outline

1. What is Cryptography?
2. Terminology
3. Brute Force
4. Rainbow Tables
5. Activity: Caesar Cipher

What is Cryptography?

What is Cryptography?

Cryptography is the science and practice of securing communication and information from unauthorized access or alteration. It involves techniques for encrypting (scrambling) data so that only authorized parties can decrypt (unscramble) and understand it.

What impact (positive or negative) does cryptography have on our CIA triad?

What is Cryptography? (continued)

How has Cryptography been used in the past?
Egypt: The Egyptians used simple substitution ciphers, such as replacing letters with symbols.

Sparta: The Spartans used a device called the *scytale*, a type of transposition cipher. A message was written on a strip of parchment wrapped around a rod, and it could only be read by someone with a rod of the same diameter.

Image Credit

Egyptian hieroglyphs

A	F	S
I/A	M	SH
Y	N	K/Q
Y	R	K
A	H	G
W/U	H	T
W/U	KH	CH
B	KH	D
P	S	J

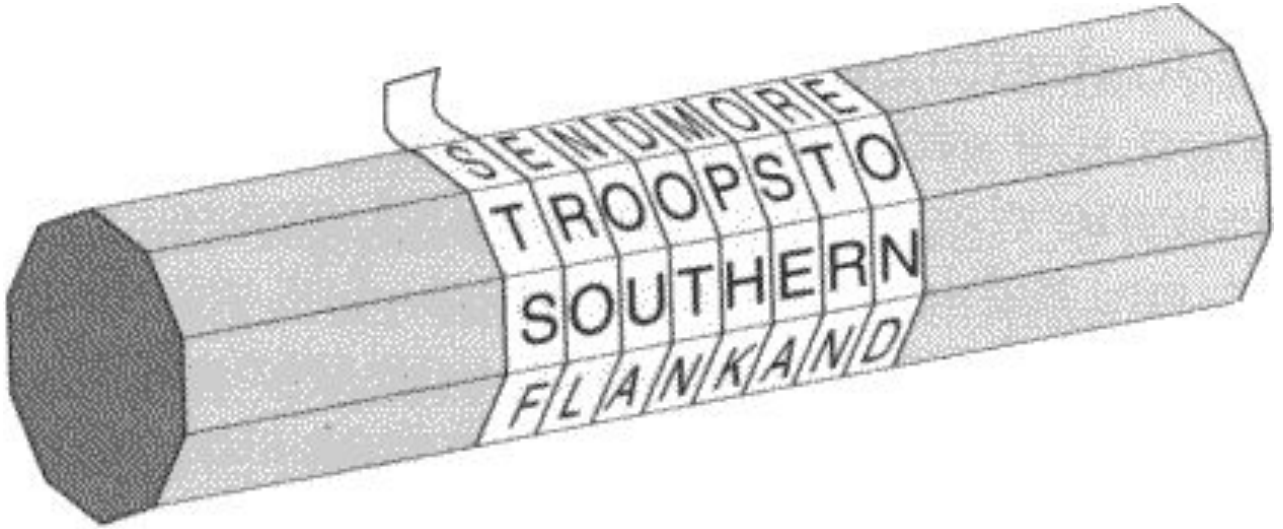


Image Credit
https://techinnercircle.co.uk/library/encryption-explained/
https://www.cachesleuth.com/scytale.html

KALAMAZOO COLLEGE

What is Cryptography? (continued)

How has Cryptography been used in the past? (continued)

Julius Caesar: The Roman general and statesman Julius Caesar is famous for his use of a cipher, now known as the Caesar Cipher.

- This is a substitution cipher in which each letter of the plaintext is shifted by a certain number of places in the alphabet. For example, a shift of 3 would transform "A" into "D," "B" into "E," and so on.
- It was a simple way to encrypt messages sent between military leaders.

Image Credit

K = 2 Shifts the alphabet 2 characters to the right

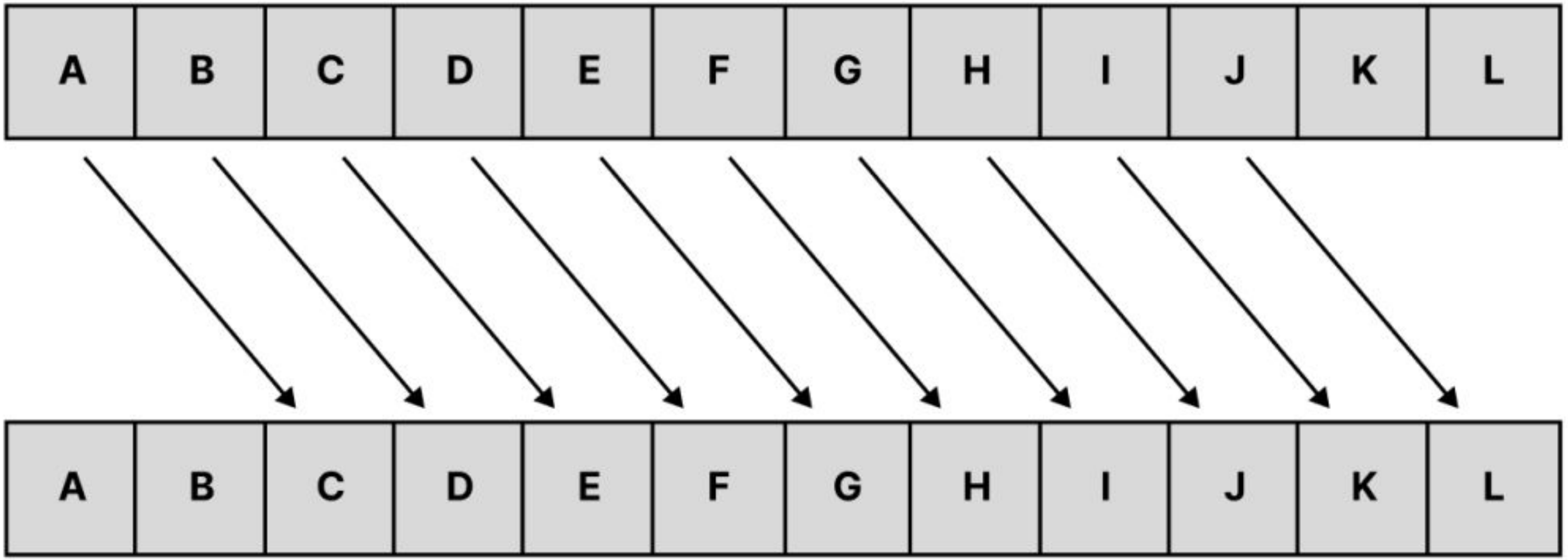


Image Credit
https://consoleflare.com/blog/the-caesar-cipher-an-encryption-technique/

KALAMAZOO COLLEGE

What is Cryptography? (continued)

How has Cryptography been used in the past? (continued)
Enigma Machine (1930s–1945): This was during WWII, the Germans used the Enigma machine for encrypting military communications.

- The machine employed a complex system of rotors that could be set to various configurations, making it difficult to break the encryption.
- However, the British, with the help of mathematicians like Alan Turing, were able to crack the Enigma code at Bletchley Park using an electromechanical device called the "Bombe”.

Image Credit

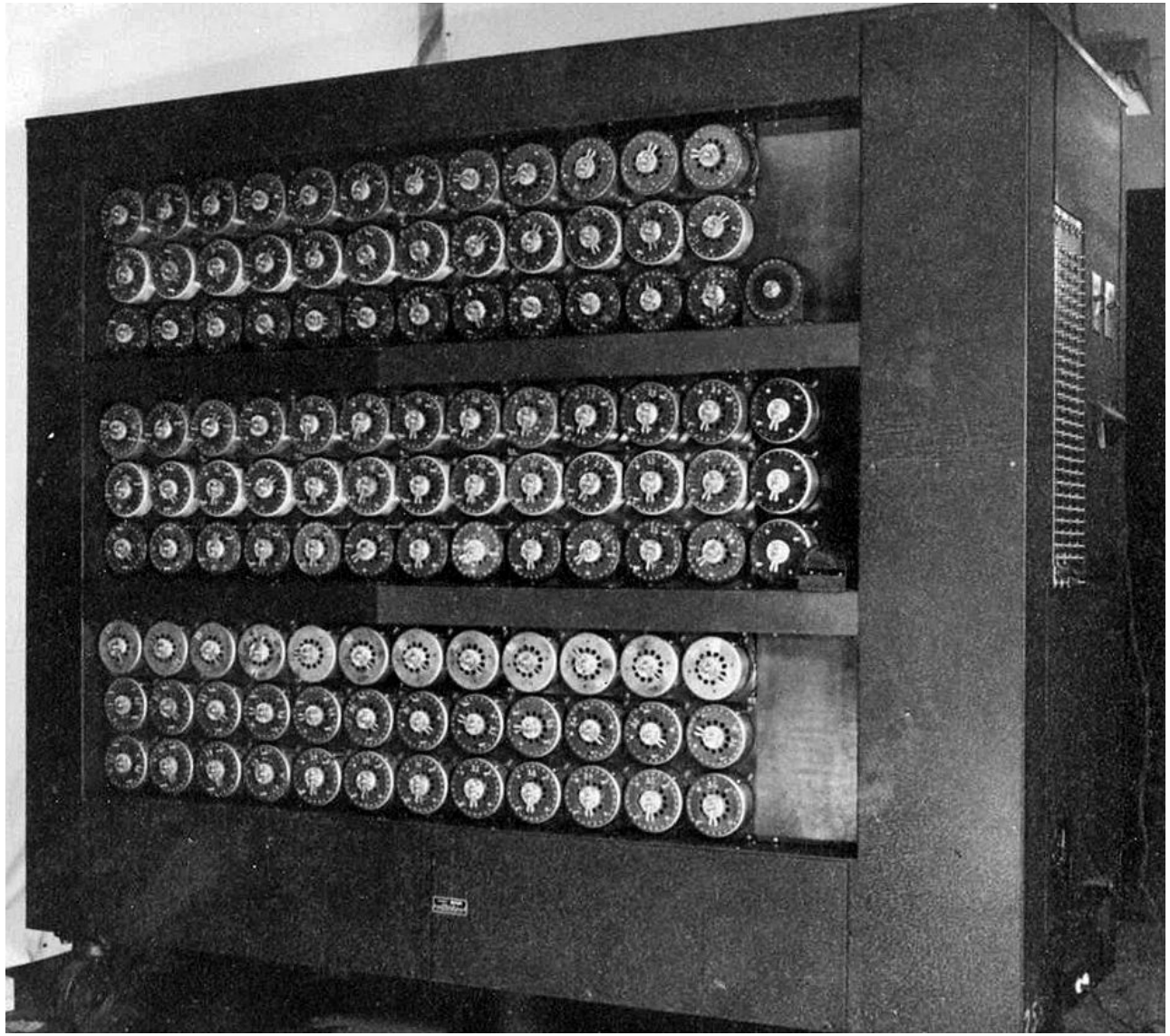


Image Credit
https://en.wikipedia.org/wiki/Bombe#/media/File:Wartime_picture_of_a_Bletchley_Park_Bombe.jpg

KALAMAZOO COLLEGE

Terminology

Terminology

Plaintext - The original, unencrypted data or message that is meant to be kept confidential. It’s the readable form of the information before any encryption has taken place.

- Example: If you're sending an email that says, "Hello, Nick! Let's meet at 11 AM," that email is plaintext before encryption.

*Role in Cryptography: Plaintext is the input for the encryption process.

Image Credit

Terminology (continued)

Cipher - A cipher is the algorithm or method used to perform the encryption and decryption of plaintext. It defines how the characters in plaintext are transformed into ciphertext and vice versa.

- Examples:
  - Substitution Cipher - This replaces each character in the plaintext with another.
  - Transposition Cipher - This rearranges the characters of the plaintext in a specific way.

*Role in Cryptography: The cipher is the core component of encryption and decryption. It provides the rules and steps to transform data.

Image Credit

Terminology (continued)

Ciphertext - The encrypted form of plaintext. It is the unreadable data that results from applying a cipher to the plaintext. This is meant to be secure and only readable by authorized parties with the correct decryption key.

- Example: After applying AES encryption to the message "Hello, Bob! Let's meet at 5 PM," the output would be a string of random-looking characters, like X8aJ2BvG6sYw... — this is ciphertext.

*Role in Cryptography: The Ciphertext is the form in which sensitive data is transmitted or stored. It is secure and cannot be easily read by attackers without decryption.

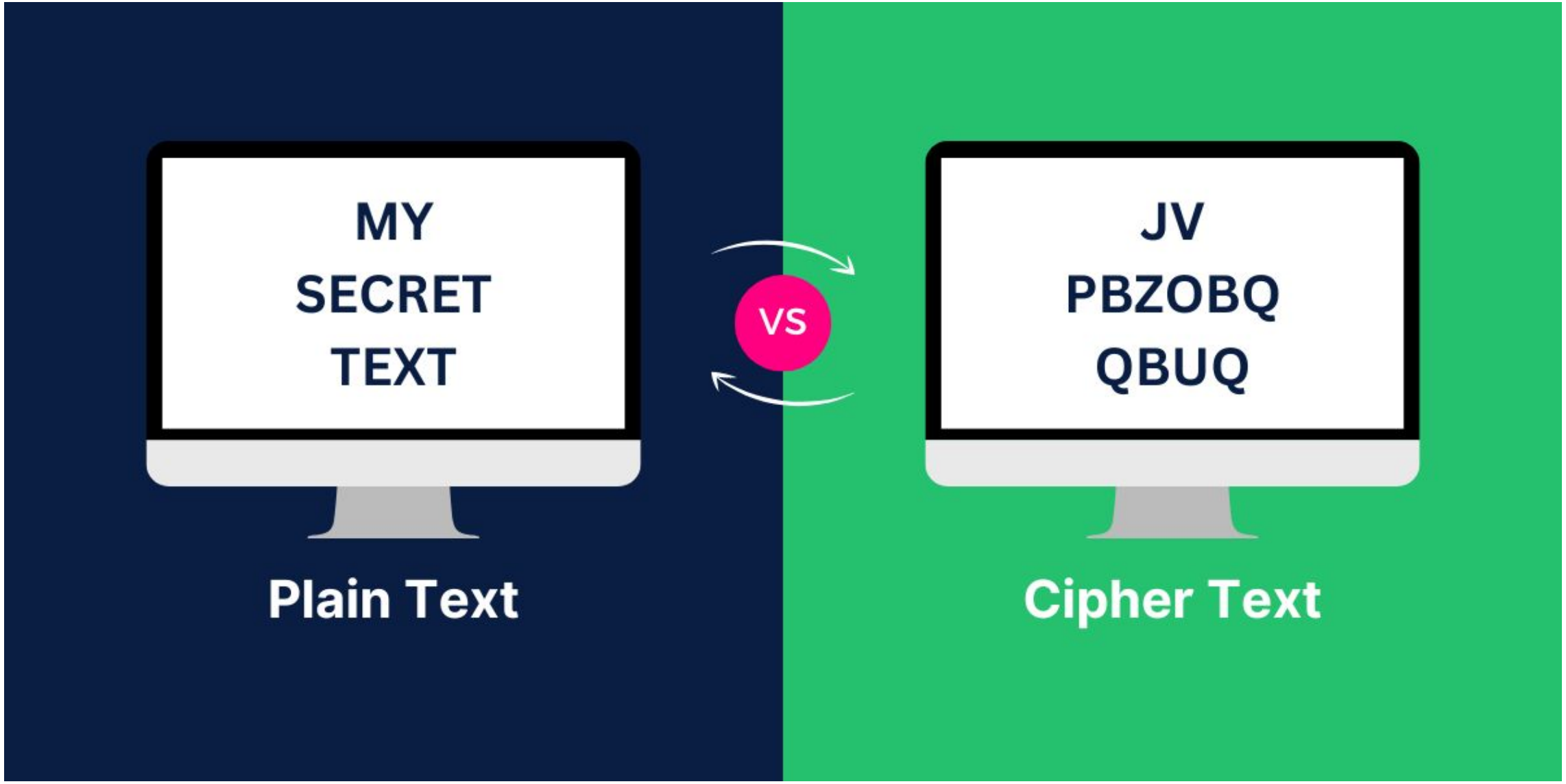


Image Credit
https://sslinsights.com/plaintext-vs-ciphertext/

KALAMAZOO COLLEGE

Terminology (continued)

Cryptographic Algorithm - It describes *the steps* used to turn plaintext into ciphertext (encryption) and ciphertext back into plaintext (decryption).

- Example: AES (Advanced Encryption Standard) and RSA are examples of encryption algorithms.

*Role in Cryptography: The algorithm defines how encryption and decryption occur. The strength and security of an encryption system largely depend on the strength of the algorithm used.

Terminology (continued)

Key - A secret piece of data used by an algorithm to encrypt and decrypt data. These can vary in length (e.g., 128-bit, 256-bit, 2048-bit, 4096-bit) and directly influence the security of the encryption system.

- Example: The amount to shift by in a Caesar Cipher.

*Role in Cryptography: The key is the "secret" that both parties need to access the plaintext. The security of the system relies on how well the key is protected and how difficult it is to guess.

Image Credit

Terminology (continued)

Public Key - It is made publicly available, meaning anyone can use it to encrypt messages for the owner of the corresponding private key.

- Example: If Bob wants to send Alice a secure message, he can encrypt it using Alice's public key. Only Alice can decrypt it with her private key.

*Role in Cryptography: The public key allows anyone to **encrypt data** to be securely sent to the owner of the corresponding private key.

Terminology (continued)

Private Key - This is kept secret by its owner. It is used to decrypt data that has been encrypted with the corresponding public key. It is essential that the private key remains confidential.

- Example: Continuing with the Alice and Bob example, after Bob encrypts a message using Alice's public key, Alice uses her private key to decrypt and read the message.

*Role in Cryptography: The private key is the counterpart to the public key. Only the holder of the private key can decrypt messages intended for them.

Image Credit

Image Credit
https://www.rapidsslonline.com/ssl/difference-between-public-and-private-key/

KALAMAZOO COLLEGE

Terminology (continued)

Hash Function - A hash function takes input data (of any size) and produces a fixed-size string, often a digest or hash, that uniquely represents that input. Hash functions are one-way (you cannot reverse them to get the original input).

- Example: SHA-256 is a popular cryptographic hash function that produces a 256-bit hash from any input data (like a file or message).

*Role in Cryptography: Hash functions are used for data integrity verification and storing passwords securely. They're also used in digital signatures and blockchain technology.

What is a hash function?

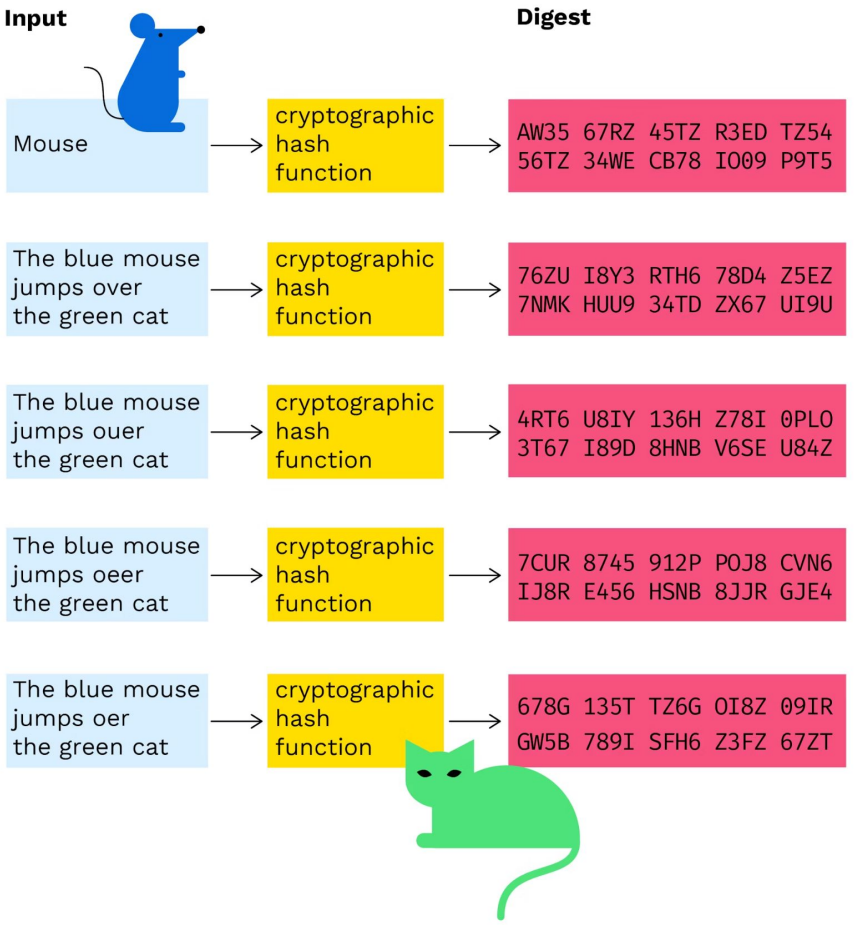


Image Credit
https://www.bitpanda.com/academy/en/lessons/what-is-a-hash-function-in-a-blockchain-transaction/

KALAMAZOO COLLEGE

Brute Force

Brute Force

In cryptography, a brute force attack is the process of systematically trying all possible keys to break an encrypted message or a system. A brute force attack on an encrypted message attempts to guess the correct key by trying all potential keys until it matches the correct one and decrypts the ciphertext into readable plaintext.

Image Credit

Brute Force (continued)

Key Space - The total number of possible keys is referred to as the "key space." A brute force attack works by testing every key in this space.

- For example, if an encryption system uses a 128-bit key, the key space has 2^{128}.

As the key length increases, the time required for a brute force attack grows exponentially. For modern encryption systems with long keys, brute forcing is considered infeasible with current technology.

<u>Does the growth of technology make brute force attacks more concerning?</u>

Image Credit

Brute Force in Password Cracking

In cybersecurity, a brute force attack is commonly used to crack passwords. The attacker tries every possible combination of characters until the correct password is found.

- The size of the password space depends on the character set (letters, numbers, special characters) and password length.
  - For instance, if you use only lowercase letters (26 characters), a 6-character password has 26^6 possible combinations (about 308 million).

Image Credit

Brute Force in Password Cracking (continued)

When the attacker knows your username and attempts to guess your password through a brute force attack, they will try every possible combination until they find the correct one.

- This is especially feasible when the password is weak or short (like "123456" or "password").

<u>What can systems or users implement to defend against these types of attacks?</u>

Image Credit

Brute Force in Password Cracking (continued)

When the attacker knows your username and attempts to guess your password through a brute force attack, they will try every possible combination until they find the correct one.

- This is especially feasible when the password is weak or short (like "123456" or "password").

<u>What can systems or users implement to defend against these types of attacks?</u>

- Account Lockout, Captcha, Two-Factor Authentication, Password Length and Complexity

Image Credit

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Image Credit

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

USING CHATGPT HARDWARE TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 secs
9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months
13	Instantly	1 hours	12 months	10 years	47 years
14	Instantly	1 days	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

Image Credit

KALAMAZOO COLLEGE

Rainbow Tables

Rainbow Tables

Rainbow tables are precomputed tables of hash values corresponding to all possible plaintext inputs. The idea behind rainbow tables is to reduce the time and computational effort needed to crack a hash by providing a lookup table of precomputed hashes.

*Instead of hashing every potential password guess on the fly (which can be time-consuming), attackers can simply look up the hash in a rainbow table to see if it corresponds to a plaintext password.

Image Credit

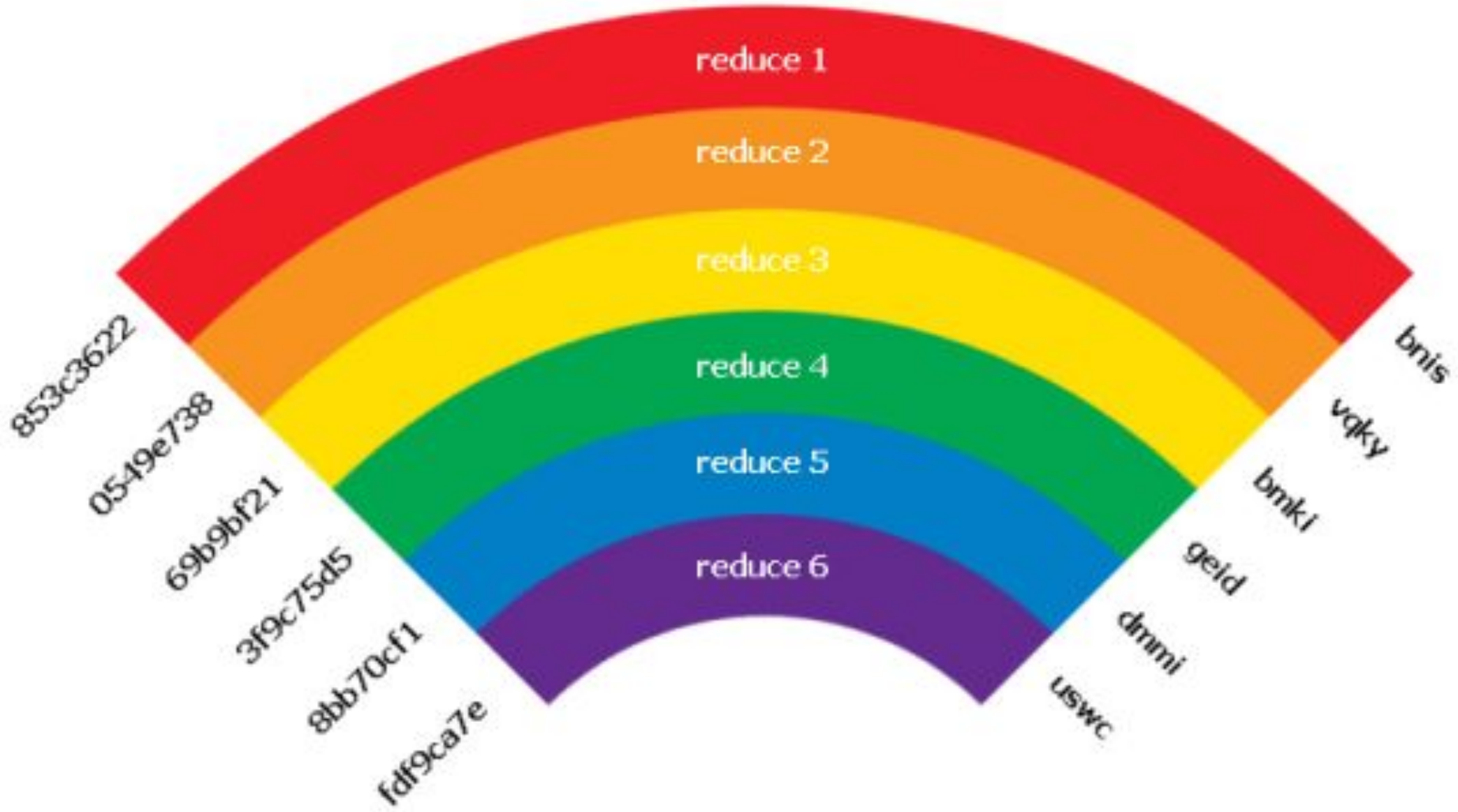


Image Credit
https://medium.tuanh.net/reasons-why-rainbow-table-attacks-are-dangerous-and-how-salting-passwords-protects-against-them-548db34d7ac4

KALAMAZOO COLLEGE

Rainbow Tables (continued)

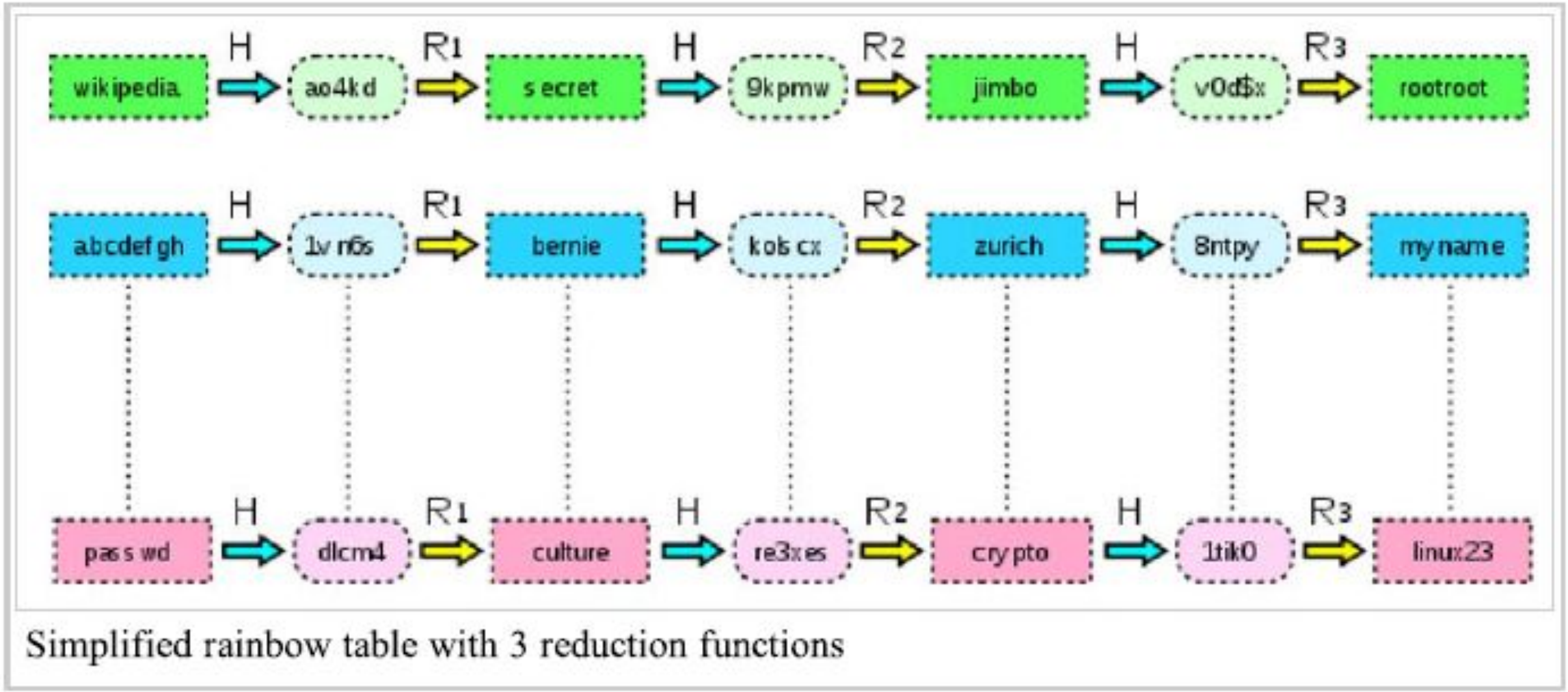
How Do Rainbow Tables Work?

1. Precomputing: The attacker first chooses a set of possible passwords. They then hash each password using a cryptographic hash function (e.g., MD5, SHA-1, or SHA-256).

2. Hash Lookup: When the attacker wants to crack a password, they hash the target password (that they have obtained, usually from a data breach) and look it up in the precomputed rainbow table.

3. Reduction Function: To make rainbow tables more efficient, attackers can use a technique called reduction. This is a function that takes a hash and converts it into another potential password, which is then hashed again.
    a. In essence, the reduction function is like a series of transformations that transform a complex hash into a simpler representation, making it easier to find the corresponding plaintext during a rainbow table attack

Image Credit



Simplified rainbow table with 3 reduction functions

Image Credit
https://infosoftworld.wordpress.com/2015/06/12/rainbow-tables/

KALAMAZOO COLLEGE

Pause: Salt

Salt - This is random data added to input (e.g., a password) before applying a hash function. It prevents attackers from using precomputed hash databases (rainbow tables) to reverse-engineer hashed passwords.

- Example: A user’s password might be "password123," but adding salt like "abc123" makes the hashed output different.

*Salting ensures that even if two users have the same password, their hashed values will be different, improving security.

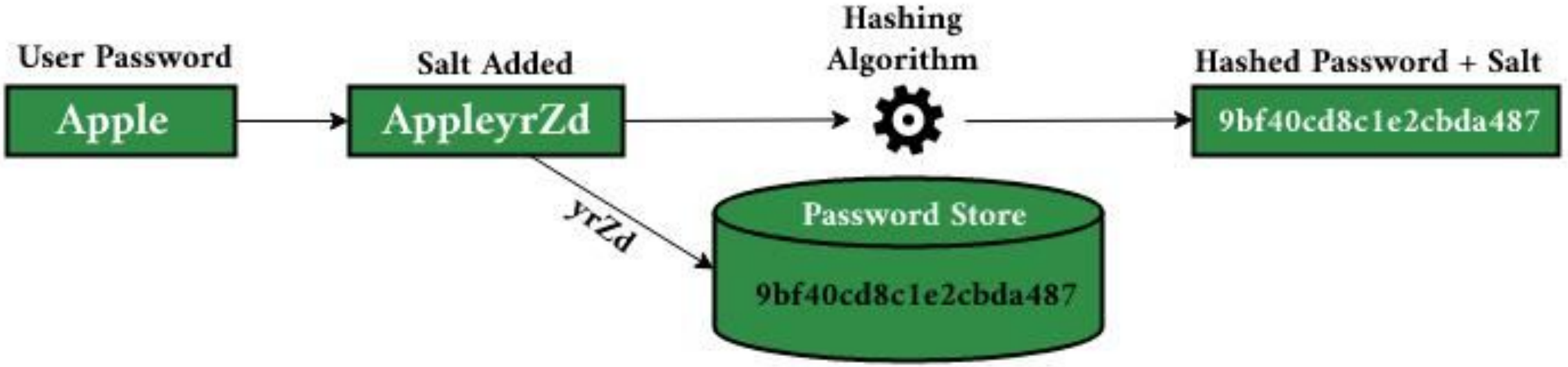


Image Credit
https://www.geeksforgeeks.org/what-is-salted-password-hashing/

KALAMAZOO COLLEGE

Activity: Caesar Cipher

Activity: Caesar Cipher

Activity: Caesar Cipher

OR

Activity: IoT Activity

OR

Topic Presentation

OR

Course Project

Questions?