Applied Cryptography and Attacks

Cybersecurity

Cryptography Day 3

Class Objectives

By the end of today's class, you will be able to:

Apply steganography in order to hide a message within non-secret data, such as an image.

Use SSL certificates to help authenticate a website.

Use cryptographic attack methods to crack a password.

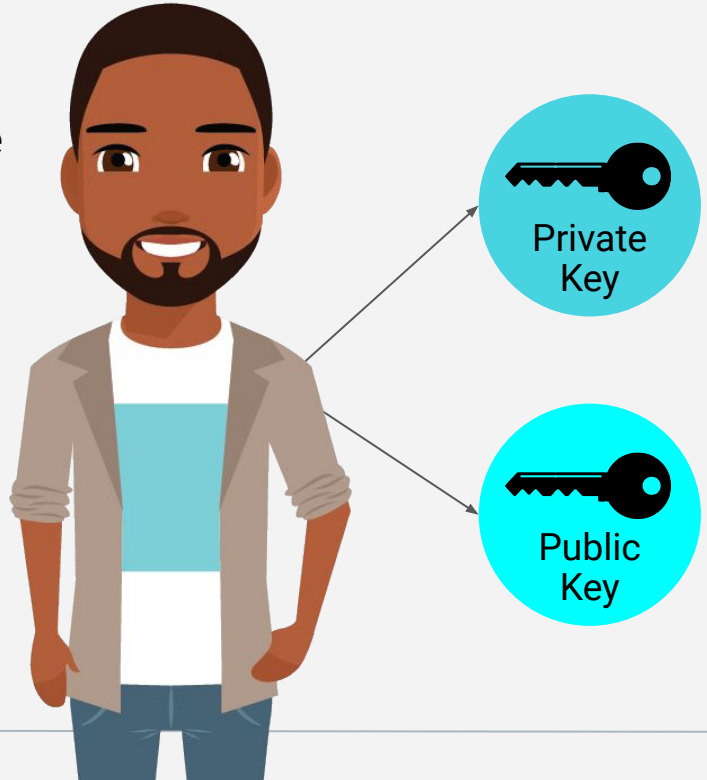
Use Hashcat to uncover the plaintext value of a hash.

Cryptography Review

Asymmetric Key Encryptions

While symmetric encryption has many advantages, its primary disadvantages are key exchange and key management.

As an alternative, we can use asymmetric key encryption, also known as public-key encryption, in which each individual has a two-key pair.



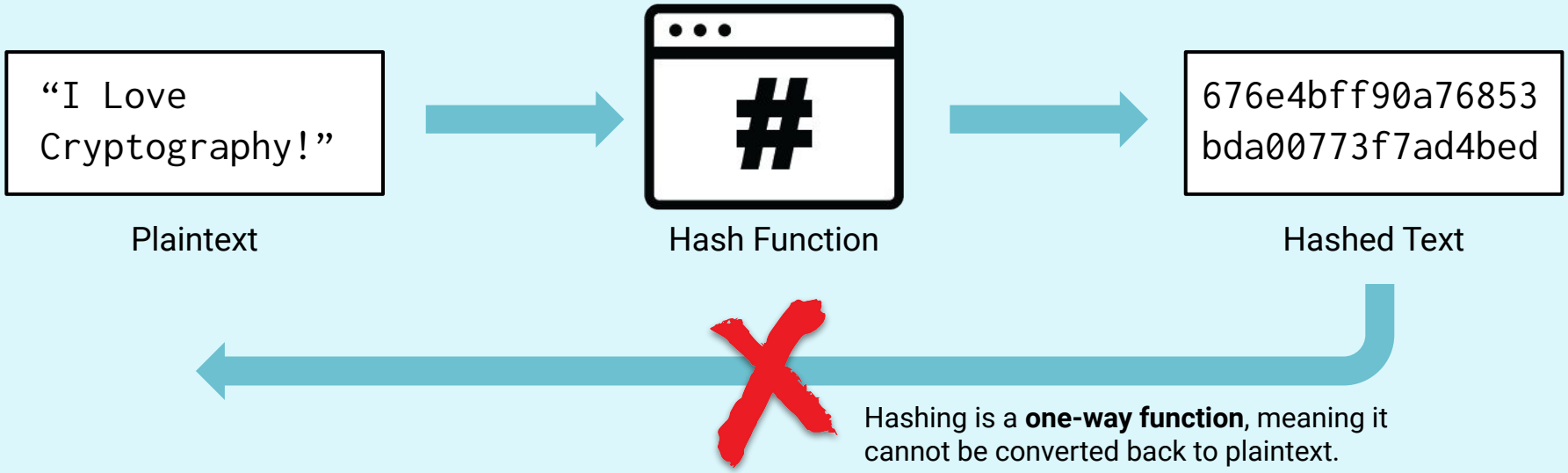
Private keys are kept secret and can affect confidentiality of messages if exposed.

Public keys are public and accessible to all.

Hashing

While encryption is used to protect confidentiality, hashing is a cryptographic method used to protect integrity.

Hashing uses algorithms to convert a plaintext message into a message digest, also known as a hash.



Digital Signatures

A digital signature is a mathematical scheme used to verify the authenticity of digital data.

Like encryption, digital signatures use public key cryptography.

However, a user uses their own private key to sign a document, and the public key is used by other users to validate the signature.

Activity: Cryptography Refresher

In the activities today, you will continue your role of security analyst at Hill Valley Police Department.

In this review activity, you will create a plaintext message and clearsign it using GPG.

Suggested Time:

20 Minutes

Time's Up! Let's Review.

Questions?

Introduction to Applied Cryptography

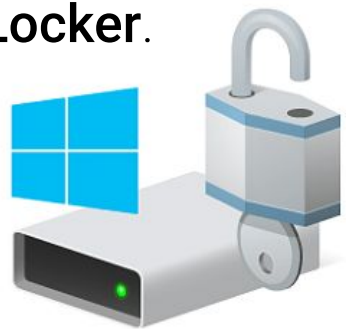
So far, we've mostly covered the foundations of cryptographic concepts. Now we will apply these concepts to modern technology and security challenges.

Cryptography and Portable Devices

Encryption can be used to secure portable devices like laptops and cell phones. Most current operating systems use **disk encryption** to prevent unauthorized parties from viewing the data on the machine.

BitLocker

Microsoft Windows uses a symmetric disk encryption program called **BitLocker**.



FileVault

Macs use a symmetric disk encryption program called **FileVault**.

Cryptography and Email

Encryption can be used to secure emails.

- Emails are not natively encrypted.
  They are sent and received in plaintext.
- Programs like **S/MIME** and **PGP** can apply public key cryptography to provide email confidentiality and use digital signatures to ensure authenticity and integrity.

Cryptography and Websites

Public key cryptography can be used to secure websites.

- **Secure Socket Layer (SSL)** is a protocol designed to encrypt web traffic.
  - HTTPS actually stands *HTTP over SSL*.
- Websites use SSL certificates as seals of approval to confirm that you are communicating with the certificated website.
- These certificates use public key cryptography to establish a secure connection between the browser and the server.

Cryptography and Websites

Websites use hashing to store passwords.

- When websites store their passwords in plaintext, a breach can reveal valuable data.
- By using hashing algorithms to hash stored passwords, even after a breach passwords will not be revealed.
- Additionally, a user's password is verified against the password hash.

Digital Forensics

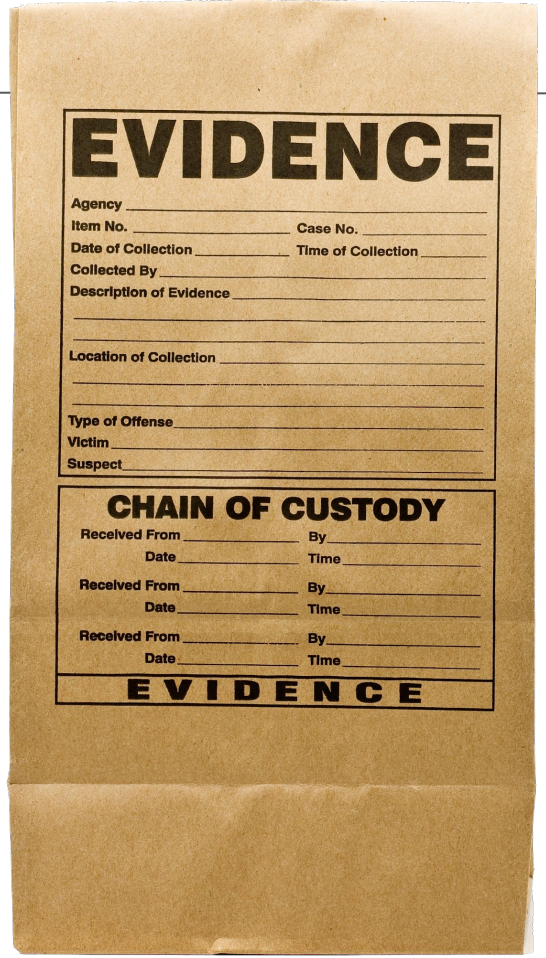
A **forensic examiner** is a cybersecurity professional who captures and investigates digital evidence from computers, cell phones, and other devices containing digital data.

Evidence is used in private industry and public legal and criminal investigations.

Digital Forensics

Forensic examiners make a hash of a device when it is initially collected for investigation.

The hash can be later used to verify that the digital data was not modified during the investigation.



Steganography is the cryptographic technique of placing hidden messages within files, images, or videos.

Steganography

For example, a forensic investigator can investigate an employee suspected of selling insider trading information. The employee has no obvious or suspicious files, only family photos. The investigator can apply steganographic tools to analyze these photos for hidden data.

Instructor Demonstration

steghide

Activity: Steganography

In this activity, you will use steganography tools to determine if images contain any hidden messages.

Suggested Time:

15 Minutes

Time's Up! Let's Review.

Questions?

SSL Certificates

SSL certificates are small data files that contain data elements including a public key and cryptographic signature to secure TLS connections between the browser and the web server.

SSL Certificates

To get an SSL certificate, an organization must first reach out to a **certificate authority** (CA), an organization responsible for issuing SSL certificates.

An X.509 certificate is the current standard of SSL certificates for securing online communications.

SSL Certificates

Next, the CA will need additional information from the organization.

01

Company documents help the certificate authority validate that the application was submitted by the company, preventing scammers from getting a real certificate for a fraudulent website.

02

A unique **IP address or Full Qualified Domain Name (FQDN)**

The **public key** that will be included in the certificate (often created during the CSR generation)

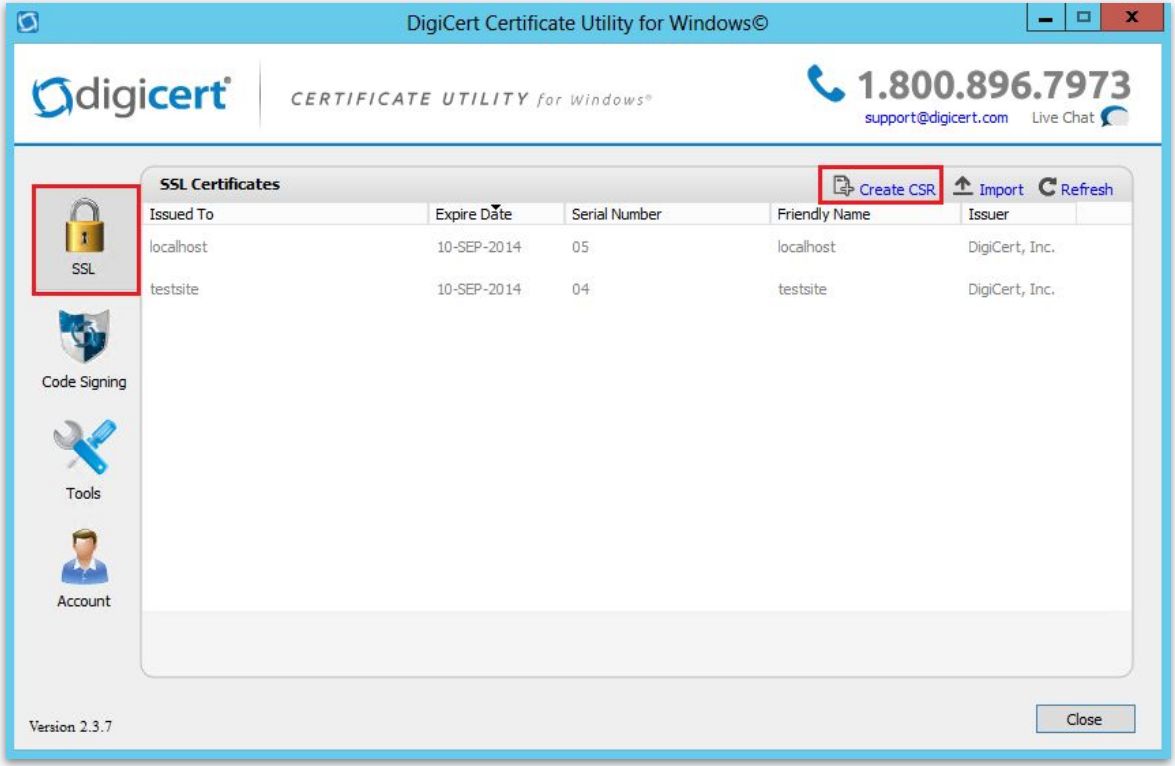
03

A **certificate signing request (CSR)**, a block of data that is created on the web server where the SSL certificate will eventually be installed.

SSL Certificates

When generating the CSR, a private and public key pair are created.

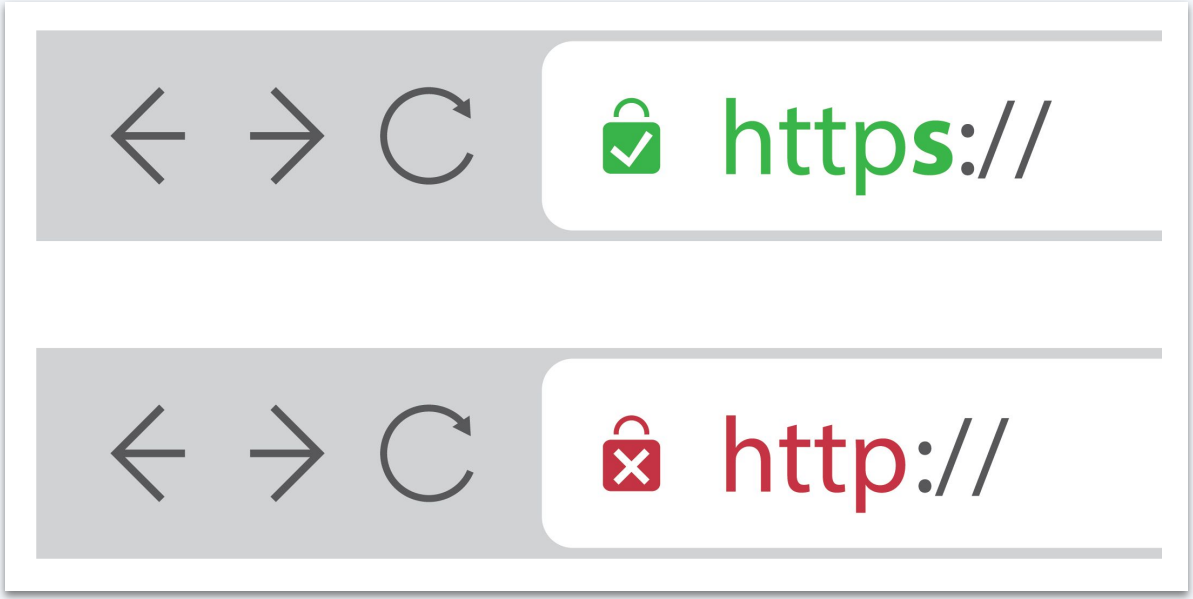
- Only the public key is sent to the CA.
- The private key remains hidden on the web server.



SSL Certificates

After the CA validates and approves the requested information, they send the SSL certificate back to the company.

The organization will see the SSL certificate installed on the web server.

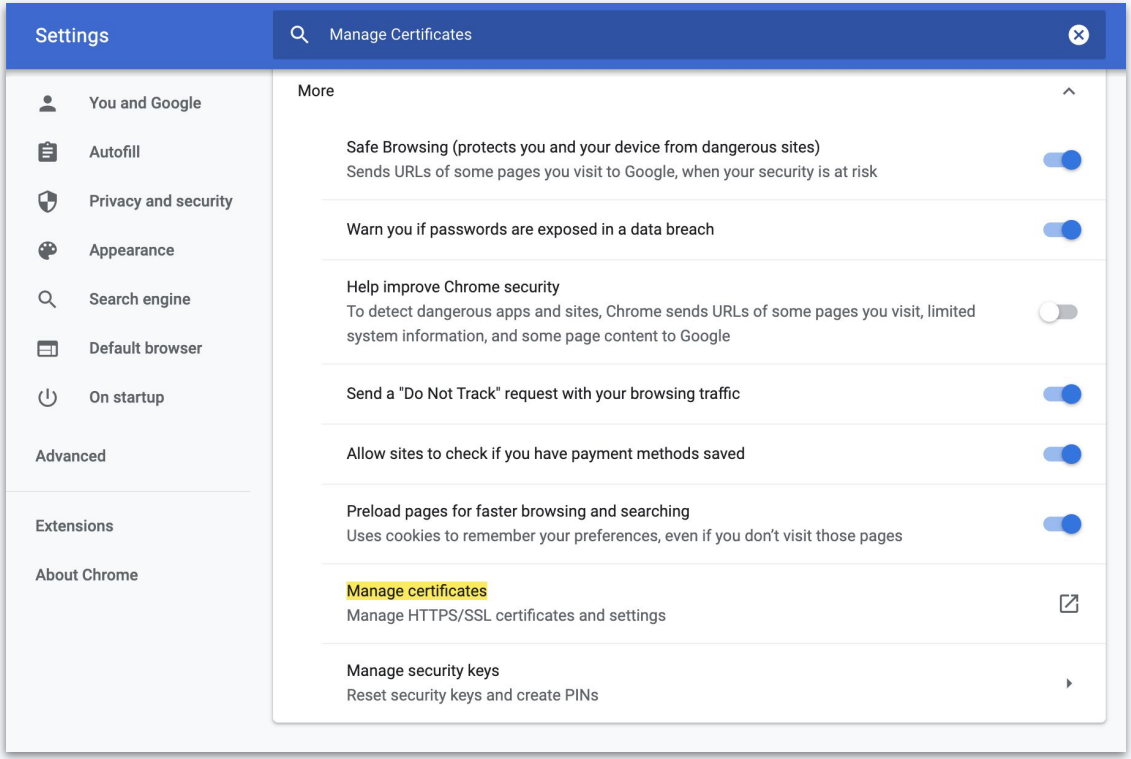


SSL certificates validate authenticity using a chain of trust.

SSL and Authenticity

Browsers have a pre-established list of trusted CAs, called a root store.

- **Root certificate authorities** are a list of CAs trusted by your browser. They're at the top of the trust chain and are typically not the organizations that issue SSL certificates.
- **Intermediate certificate authorities** usually issue certificates and report up to a root certificate authority.



Instructor Demonstration

Valid and Invalid Certificates

The Role of SSL in securing web traffic

Servers use TLS to secure web traffic through SSL Certificates.

01 When we access a secure website, the browser asks the web server for certificate details.

02 The server responds with a copy of the SSL certificate containing the public key.

03 The browser validates the certificate by checking the validity date and root CA.

04 The browser uses the server's public key to create, encrypt, and send a session key.

05 The server decrypts the key, sends an acknowledgement, and starts an encrypted session.

06 Secure web traffic begins. Server and browser encrypt/decrypt data with the session key.

Activity: SSL Certificates

In this activity, you will investigate a suspicious website and analyze its certificates to determine if it’s legitimate.

Suggested Time:

15 Minutes

Time's Up! Let's Review.

Questions?

Countdown timer

15:00

(with alarm)

Cryptographic Attacks

Now we will examine the methods and vulnerabilities used in cryptographic attacks.

A **statistical attack** exploits weakness in cryptographic algorithms by attempting to determine if the “random” values produced are actually predictable.

Statistical Attacks

For example: Some technology professionals use a token-generation program that creates a random number that they use to securely log in to their computer.

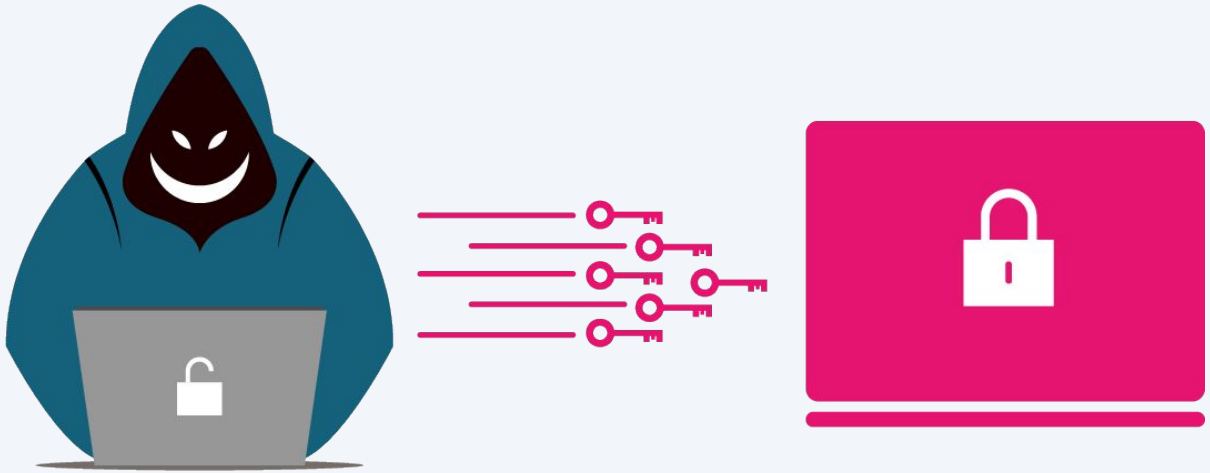
If the number generated is in fact predictable and not random, a hacker can determine the number and access unauthorized data.

Mitigation

Be sure algorithms are using random values.

Brute Force Attack

In a brute force attack, attackers use many passwords or user and password combinations until one eventually works.



Brute Force Attack

If we wanted to brute force a root account:

```
User: root, Password: abc123
User: root, Password: 123abc
User: root, Password: 123456
User: root, Password: 654321
User: root, Password: aaaaaa
User: root, Password: bbbbbb
```

Mitigation

- Apply lockout features to limit the number of login attempts a user has before getting locked out.
- Applications can use firewalls that detect and stop large volumes of attempted logins from a single source IP address.

Birthday attacks exploit the probability that two separate plaintexts that use the same hash algorithm will produce the Same ciphertext.

*(Also known as **collision** and **hashing collision**.)*

Birthday Attack

The birthday attack is named after a probability theory called the **Birthday Problem**, which states that for a given number of people, the probability that two that share a birthday is higher than you would expect (50% for 23, 99.9% for 70)!

Mitigation

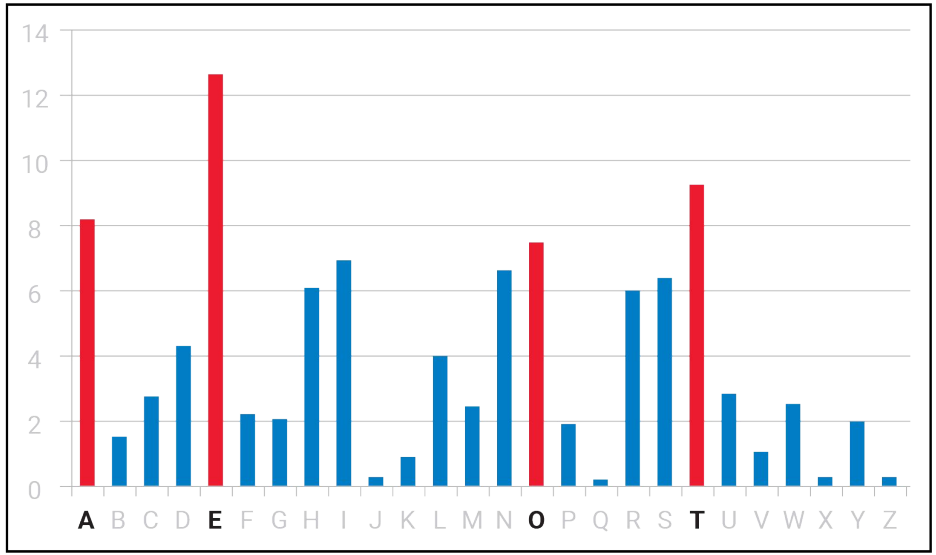
Stronger hashing algorithms limit the possibilities of hashing collision.

https://en.wikipedia.org/wiki/Birthday_problem

Frequency analysis is a method for cracking substitution algorithms.

Frequency Analysis

An attacker can note the most frequently used letters in the ciphertext and substitute them with the most frequently used letters in the English language (e, t, o, a). After inferring the ciphertext, the plaintext can be cracked.



Mitigation

This method targets standard ciphertext ciphers. Mitigate by using more advanced encryption algorithms.

In **replay attacks**, an attacker intercepts an encrypted message and replays it to the receiving party to get access.

Replay Attack

For example: An attacker can obtain an encrypted signal from a garage door opener.

The attacker can replay the encrypted signal at a later time to open the garage.

Mitigation

Add an expiration time for the encrypted data, so it can't be replayed at a later date.

When an attacker has access to a **ciphertext** and its associated **plaintext**, they can analyze the two to determine the encryption algorithm and decrypt future messages.

Known-Plaintext

If we know:

Plaintext Hello

Ciphertext 8 5 12 12 15

We can determine that the plaintext letter corresponds to a number in alphabetical order:

A =1, B = 2, etc.

So we know:

7 15 15 4 2 25 5

Can be decrypted to:

goodbye

Mitigation

Use advanced encryption and limiting access to ciphertext and associated plaintext.

When an attacker has access to the encryption program and ciphertext, **but not the plaintext**, they can encrypt several plaintext messages to learn how the ciphertext is generated.

Chosen-Plaintext

If we have the ciphertext **act** and the encryption program, we can enter plaintext messages into the program:

Plaintext	boy	red	hot
Ciphertext	oby	erd	oht

We can then determine that the transposition cipher is using the following key:

```
{1,2,3} = {2,1,3}
```

t **act**, we can determine that the plaintext is **cat**.

Activity: Cryptographic Attacks

In this activity, you will use cryptographic methods to crack a cipher and reveal a plaintext password.

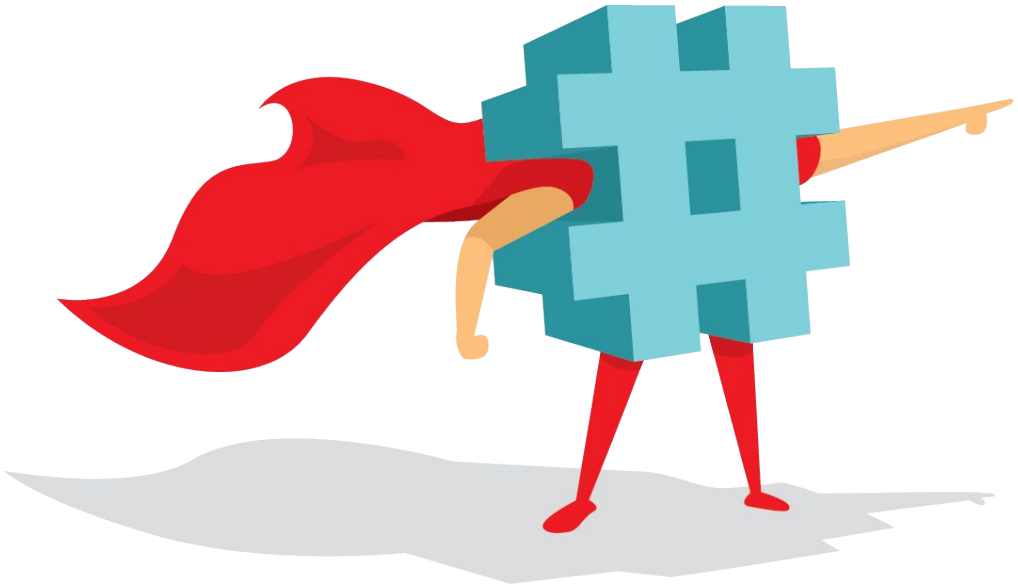
Suggested Time:

20 Minutes

Time's Up! Let's Review.

Questions?

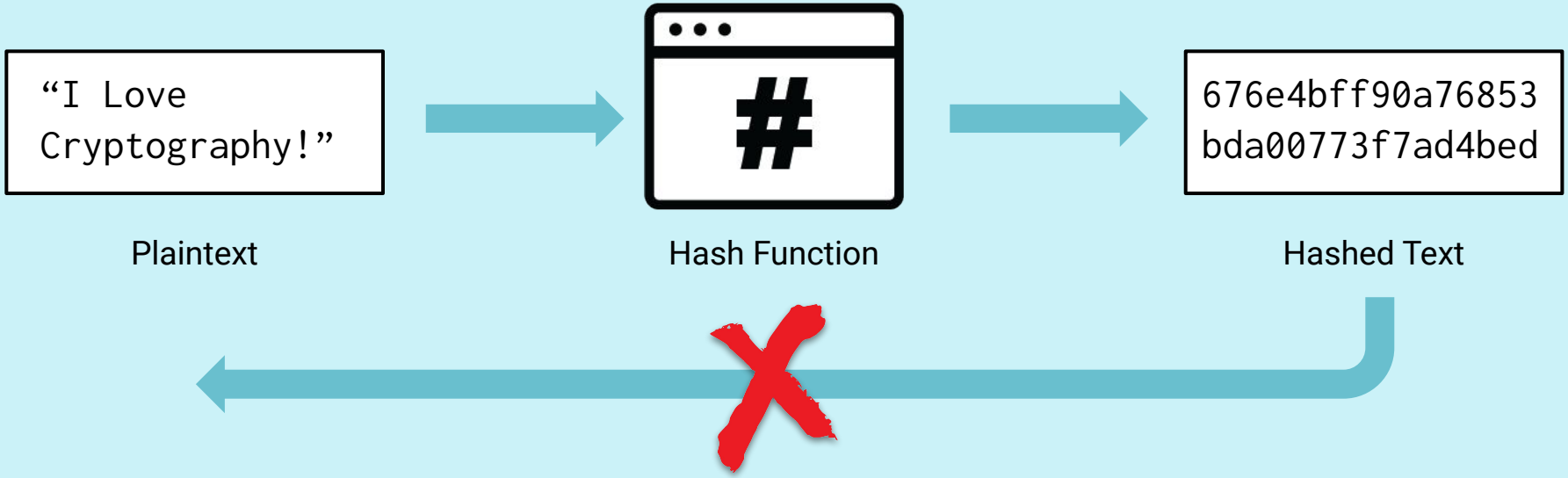
Rainbow Tables



Some types of cryptography, such as **hashing**, require more advanced methods and technologies.

Rainbow Tables

Remember: Hashing creates a one-way ciphertext. It is almost impossible to decipher the algorithm and figure out the plaintext from the ciphertext.



Hashing is a **one-way function**, meaning it cannot be converted back to plaintext.

Rainbow tables are resources that contain precomputed hashes with the associated plaintext passwords.

Rainbow Tables

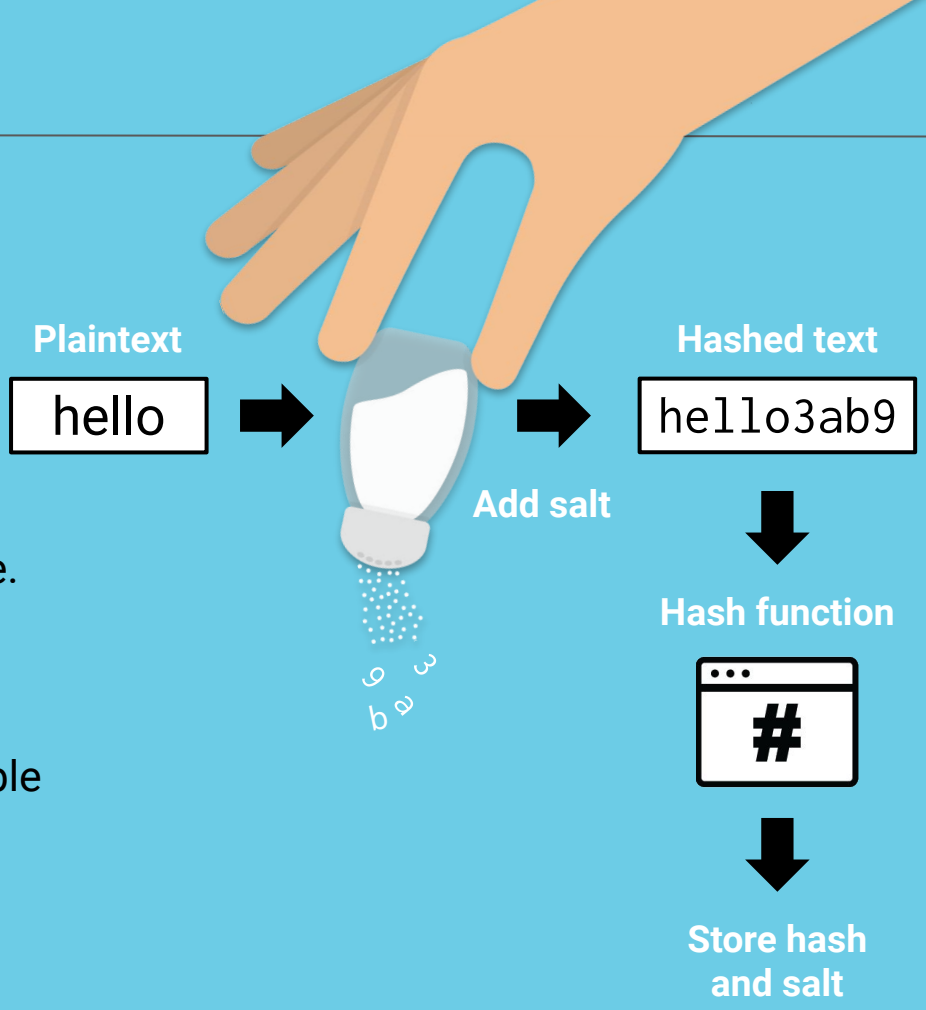
Using rainbow tables is as simple as searching for the password associated with a hash.

- Some rainbow tables are extremely large.
- They can take up a lot of storage space and CPU to use effectively.

Rainbow Tables

We can defend against rainbow tables by **salting** – a cryptographic method of combining salt (a random value) with the plaintext into the hash function.

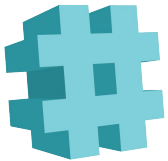
- Salting is simply adding a random value.
- The output is a salted hash.
- Once the salted hash is saved, the password hash listed in the rainbow table will not match the new salted hash.



Hashcat is a command-line tool that can automate the cracking of hashes.

Hashcat

Hashcat uses dictionary wordlists, rainbow tables, and brute force methods to figure out plaintext passwords from hashes.

Password		5f4dcc3b5aa765d61d8327deb882cf99
admin123		0192023a7bbd73250516f069df18b500
g1w2e3r4t5y6		1cd87f5976c0893cb50d0758f528963f

Hashcat

We'll demonstrate using Hashcat with the following scenario:

01

A security professional is tasked with testing the security of a company's website. They must check if they can log in as the root user.

02

They are able to conduct an attack on the website and capture an unsalted hash value of the root user's password: **ea847988ba59727dbf4e34ee75726dc3**

03

From the length of the hash, they know it is an MD5 hash.

This walkthrough will demonstrate the steps necessary to determine the root user's plaintext password with **Hashcat**.

Instructor Demonstration

Hashcat

Activity: Hashcat

In this activity, we will use Hashcat to figure out the plaintext representation of a hash.

Suggested Time:

20 Minutes

Time's Up! Let's Review.

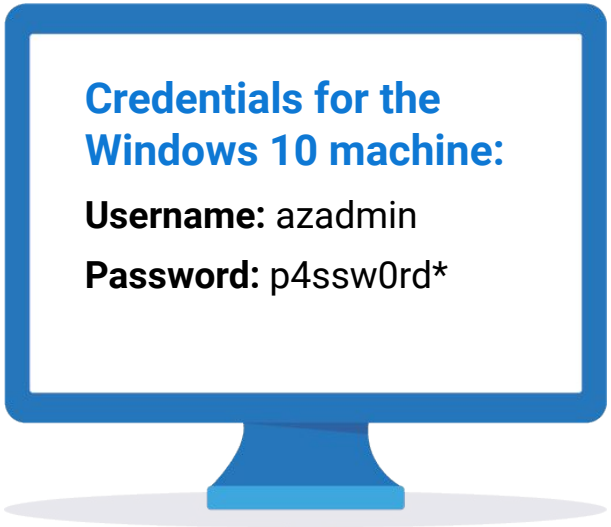
Questions?

Next week, we will return to Azure Lab Services, using a new environment: NetSec.

Next Week's Lab Environment

Return to your local computer environment and click the registration link for the NetSec environment. *(Sent out by instructor.)*

Inside of the NetSec instance, you will find a Windows 10 machine hosting a Security Onion machine and two virtual Linux machines named UFW and firewalld.




The End