Cryptography

# Symmetric Encryption

What is "symmetric" about symmetric encryption? What are some potential problems with symmetric cryptography (e.g., with keys)? (~50 words)

# Symmetric Encryption: Caesar Cipher

Include a screenshot of using the Cyber Chef website to encrypt your first and last name using the Caesar Cipher (ROT13).



What features of a message encrypted with the Caesar Cipher indicate that it is not a fantastic cipher? For example, how might an attacker crack the ciphertext? (~50 words)

# Symmetric Encryption: One-Time Pad

Use the one-time pad lookup table in the eBook to encrypt your first name using the key: MGPOSLZPQLMSTAQMDUWNCUSHZ.

The one-time pad algorithm is fairly simple. Why is it so secure? (~50 words)

How could one-time pad keys be distributed securely? Brainstorm a list of ~10 ideas.

What are some of the problems with one-time pads that make them impractical for use to secure things like online banking transactions? (~50 words)

# Symmetric Encryption: AES

Include screenshots of encrypting and decrypting data using the AES algorithm with the Gnu Privacy Guard (gpg). You may need to include several screenshots.



AES is commonly used for symmetric encryption. Will quantum computers make AES obsolete? You may need to research this online. (~50 words)

# Asymmetric Encryption

Why isn't asymmetric encryption better than symmetric encryption (and vice versa)? (~50 words)

# Asymmetric Encryption: RSA

Include a screenshot of **clearsigning** a file using **gpg**.



The exercise created a key pair with the name Bugs Bunny. What measures could be put in place to verify the identity of the person who owns the key pair? (~50 words)

# Asymmetric Encryption: Elliptic Curve Cryptography

Include a screenshot of your OpenSSH key using the curve 'ed25519'.



Do you personally need to understand the math behind EC cryptography before trusting it? How well do you know the math? Do you trust EC cryptography? Why? (~100 words)

# Encryption: How HTTPS Works

Should governments be given a master key that lets them unlock HTTPS traffic? Justify your position. (~100 words)

# Hashing Files

List several use cases for hashing files and briefly explain what hashing would accomplish. (~50 words)

# Hashing Passwords

Explain what salt does in password hashing. (~50 words)

Why is a slower algorithm better for hashing passwords? (~50 words)

# Cracking Passwords

Include a screenshot showing passwords cracked using **john**.



How do you personally create passwords that would be hard to crack? (~50 words)

# Password Managers

Include a screenshot of Bitwarden running in your browser unlocked (meaning you logged in). If you use another password manager, include a screenshot of it working in your browser.



Alternatively, if you are a "conscientious objector" to password managers, briefly explain why you hate security and do not want to use one. (This is a sarcastic prompt...sort of.)

# Multifactor Authentication

Multifactor fatigue is a real thing. Write an argument convincing your friend to leave 2-factor authentication enabled, even though he just wants to make life easier by turning it off. (~50 words)