University of Gloucestershire BSc Cyber Security Open Day Activity

Cryptography is an essential concept that exists for users, businesses and the internet itself. By having cryptography, we can ensure sensitive data meets the 3 pillars of cyber security in confidentiality, integrity and availability. However, to sometimes understand cyber security, we need to be able to think like the criminals especially hacking and cryptanalysis. This short activity is around using code to decrypt different ciphers.

In the code is 10 different cyphertexts you must decrypt using the code. You will need to change some parts of it based on the hints or however you deem fit. It is your task to figure out which text have been encrypted with what cipher and match them up with the correct decryption functions.

Activity Instructions

1. Download the code from <https://github.com/J-P-C01/UoG-Cyber-Open-Day-Activity> if you haven’t already
2. Save to the desktop and then open the python file in VS code or any other editor
3. Run the file
4. Select which of the 10 text you want to try to decrypt first
5. Choose which cipher you would like to try to decrypt with
6. Use the hints below to deduce the likely cipher.
7. Refer to the example code and try applying the right decryption function.
8. When you decrypt a message, write the answers to a notepad
9. Once all are decrypted, find one more phrase that is found when all 10 originals are decrypted

A: He marched bravely into the storm. (Caesar, 3)  
B: EACHCHALLENGEREVEALEDAHIDDENSTRENGTH (Baconian)  
C: Lions guarded the ancient city walls. (Vigenere, “key”)  
D: Logic often solves what brute force cannot. (Atbash)  
E: OVERTHEHILLSAQUIETWHISPERECHOEDXXXX (Columnar, 5)  
F: WISDOMHIDESINPLAINSIGHTFORTHEPATIENT (Baconian)  
G: Ordinary men dream of extraordinary things. (Caesar, 7)  
H: Reality bends when imagination takes over. (Atbash)  
I: LATEATNIGHTTHESTARSTOLDSTORIES (Columnar, 6)  
J: Dragons were more than just myths in this realm. (Vigenere, “world”)

Cipher Techniques, Descriptions, and Examples

Caesar Cipher

How it works:  
The Caesar cipher is a substitution cipher that shifts each letter in the plaintext a fixed number of positions down the alphabet. A Caesar shift of 3 turns A into D, B into E, and so on. It's simple to crack by brute-forcing all 25 shifts.

Examples:

**Key:** Shift = 5  
**Plaintext:** The treasure is buried   
**Ciphertext:** Ymj ywfzxwjw nx gzwnji

Once selecting a cipher text try shifting a few with:

1. “The magic number”
2. A number that can be written in 2 ways

Vigenère Cipher

How it works:  
The Vigenère cipher uses a repeating keyword to determine the letter shift. Each letter in the plaintext is shifted by an amount determined by the corresponding letter in the keyword.

1. Try different keywords to see how the output changes
2. Try short words, repeat the keyword manually if needed

To try:

1. One of the words is the item needed to crack this cipher
2. One of these words is part of WWW.

Atbash Cipher

How it works:  
The Atbash cipher is a monoalphabetic substitution cipher that maps A↔Z, B↔Y, C↔X, and so on. It doesn't require a key, and decryption is reversing the encryption process

**Plaintext:** Knowledge is power   
**Ciphertext:** Pmlwovwtv rh kldvi

Simply Reverse the original, look at patterns in the text!

Bacon’s Cipher

How it works:  
Bacon's Cipher encodes letters using 5-character binary strings of A and B (e.g., A=AAAAA, B=AAAAB). Each group of five characters represents one letter. Ensure the ciphertext is in correct 5-letter blocks.

**Plaintext:** Secret mission accomplished.  
**Ciphertext:** AABAB AABBA ABABA ABBAB ABBBA ABBAA ABBAB AABAA ABABB ABBBA AABBA AABBA ABBAB AABAB ABBBA ABBAB ABBAB AABBA ABBAA ABBAB

Hint: look at the A’s and B’s

Columnar Transposition

How it works:  
This cipher involves writing the message in rows of a fixed number of columns, then reading the message down the columns in a specific order. The number of columns determines how the text is reordered.

**Plaintext:** WELCOMETOTHEUNIVERSITYOFGLOUCESTERSHIRE  
**Ciphertext:** WEUSGSIETNILTRLOITOEECTVYURXOHEOCSXMERFEHX

| **C1** | **C2** | **C3** | **C4** | **C5** | **C6** |
| --- | --- | --- | --- | --- | --- |
| W | E | L | C | O | M |
| E | T | O | T | H | E |
| U | N | I | V | E | R |
| S | I | T | Y | O | F |
| G | L | O | U | C | E |
| S | T | E | R | S | H |
| I | R | E | X | X | X |

1. One of the text columns is the first value in maths we can round up with
2. The other is the level of the final year of an undergraduate degree