### **Cryptography**

### **Duration: 1 Week**

### **Summary**

This lesson introduces cryptography, one of the primary means of providing security of Internet communication and of data itself. It introduces the simple Caesar Cipher (shitf), and Polyalphabetic crypto algorithms. Readings and videos introduce the concepts and students use tools at the Khan Academy to explore the techniques. The assessment has students encrypt and decrypt binary data (their initials) using a shift cipher and bitwise operations with a key (password).

### **Learning Objectives**

* Define: encryption, decryption, plain text, cipher text.
* Perform a shift Cipher (e.g. Caesar Cipher).
* Perform bitwise encryption of binary data.
* Explain what makes a good encryption algorithm.
* Identify existing cyber security concerns, and potential options that address these issues with the Internet and the systems built on it. [AP CSP P1, 6.3.1]
* Analyze how data representation, storage, security, and transmission of data involve computational manipulation of information. [AP CSP P4, LO 3.3.1]

### **Course Material**

* Watch: [Encryption](https://www.youtube.com/watch?v=6-JjHa-qLPk) [6:39]
* Read: [Blown To Bits - Chapter 5 (Secret Bits)](http://www.bitsbook.com/wp-content/uploads/2008/12/chapter5.pdf)
* Watch: [Ceasar Cipher](https://www.youtube.com/watch?v=sMOZf4GN3oc) [2:35]
* Do: [Caesar Cipher Exploration](https://www.khanacademy.org/computing/computer-science/cryptography/crypt/p/caesar-cipher-exploration)
* Read: [Shift Ciphers](https://www.khanacademy.org/computing/computer-science/cryptography/ciphers/a/shift-cipher)
* Watch: [Encrypted Data](https://www.youtube.com/watch?v=l8srWawACAU&feature=youtu.be) [10:12]
* Read: [XOR Bitwise Operations](https://www.khanacademy.org/computing/computer-science/cryptography/ciphers/a/xor-bitwise-operation)
* Read: [XOR and the One-time Pad](https://www.khanacademy.org/computing/computer-science/cryptography/ciphers/a/xor-and-the-one-time-pad)
* Do: [Bitwise Exploration](https://www.khanacademy.org/computing/computer-science/cryptography/ciphers/e/bitwise-operators)
* Watch: [Advanced Data Encryption](https://www.youtube.com/watch?v=KSu_4dunsdA&feature=youtu.be) [7:39]

### **In Class**

* Optional: [Public Key Encryption Unplugged](http://csunplugged.org/public-key-encryption/)
* Optional: [Cryptographic Protocols Unplugged](http://csunplugged.org/cryptographic-protocols/)
* If you have extra time, or for students who really enjoy the cryptography material, students can do much more in the [Khan Academy Cryptography course.](https://www.khanacademy.org/computing/computer-science/cryptography)

### **Assessments**

* Conceptual Quiz:
  + [Cryptography](https://docs.google.com/document/d/1qB85xV0CoCWs5yRdRtQ2zebLCfab3hiZcCsmu_O-71Q/edit?usp=sharing) (requires access)
* Practical Assignment:
  + [Cryptography](https://drive.google.com/open?id=1NDHSAGL9ako3nW4pPCsZwP_ls-wHghCV4f52DHUbrDg) | [Grading Rubric](https://drive.google.com/open?id=1En_2qnCzSznqqfoRmQ-Refv3OHLluSuQPNuwn9ziDqo) | [Answer Key](https://docs.google.com/document/d/1Fm_aVP-K97VWDTqA9FycGdJAsvVYgD7CIAKdpydGEuY/edit?usp=sharing)
  + [BB Ch 5: Secret Bits](https://drive.google.com/open?id=1nojb5W1z-lc8lM7_n2XhkNYr2aCV80LtDsLto_rzNk0)