

1. Explain Kerchoff's principle of cryptosystem security.
2. Encrypt *this is an example of the scytale cipher* using a Scytale cipher with circumference 5. Partition the plaintext to leave the least number of unused spaces, and fill these spaces with random letters.
3. Explain the difference between decryption and cryptanalysis.
4. Encrypt *arrest conspirators asap* using the railfence cipher.
5. In the plot to overthrow Mary, who were each of G W B P, and what were their roles?
6. What does Arabic *ilm* mean in English? And what does this have to do with our story?
7. In typical English, what are the frequencies of the 9 most common letters ?
8. Give the first two and last two letters of the Hebrew alphabet, and explain the word origin of the atbash cipher.
9. The Kama Sutra cipher is more advanced than the Caesar cipher, but the Caesars cipher is more recent. This does not make sense from an evolutionary point of view. Explain.
10. Encrypt *this message is secret* using (i) atbash (ii) Caesar shift 10 (iii) Kama Sutra, with letter pairs ab cd ef ... (iv) Vigenere with key *black* (v) the homophonic cipher given in Singh's text.
11. Explain the relationship of the novel *The Man in the Iron Mask* by Dumas to the story of cryptography.
12. According to the text, where and when was the man in the iron mask seen? what are two possible identities for this person?
13. Explain how the use of Morse code led to the popularity of the Vigenere cipher.