# Assignment

1. Diffie-Hellman Research. How does Diffie-Hellman key exchange protocol works? Use the Internet to research this key-exchange protocol. Explain the man-in-the-middle attack and provide a numerical example that shows how the ‘man-in-the-middle’ attack works in this protocol.
   * The Diffie-Hellman key exchange protocol is a method of securely exchanging cryptographic keys over a public channel. It was one of the first public-key protocols as it was part of the first widely recognized public-key agreement protocol.
   * Two parties, Alice and Bob, agree on a large prime number, p, and a base, g, in advance. For our example p=23 and g=5.
   * Alice chooses a secret value a and sends Bob A = g^a mod p. Let's say a=6, so A = 5^6 mod 23 = 8.
   * Bob chooses a secret value b and sends Alice B = g^b mod p. Let's say b=15, so B = 5^15 mod 23 = 19.
   * Alice computes s = B^a mod p. In our example, s = 19^6 mod 23 = 2.
   * Bob computes s = A^b mod p. In our example, s = 8^15 mod 23 = 2.
   * Now, both Alice and Bob share a secret (s=2) that can be used as a key for further encryption of their communication. The man-in-the-middle attack in the context of the Diffie-Hellman protocol involves an attacker, Eve, intercepting the public keys sent over the network by Alice and Bob. Here's how it works:
   * Alice sends A to Bob, but Eve intercepts it and sends her own E\_a = g^e\_a mod p to Bob.
   * Bob sends B to Alice, but Eve intercepts it and sends her own E\_b = g^e\_b mod p to Alice.
   * Alice computes s = E\_b^a mod p and Bob computes s = E\_a^b mod p.
   * Now, Eve shares a secret key with Alice and a different secret key with Bob, and can decrypt, read, and re-encrypt messages between them without their knowledge.
   * For example, if Eve chooses e\_a=9 and e\_b=14, she sends E\_a = 5^9 mod 23 = 4 to Bob and E\_b = 5^14 mod 23 = 10 to Alice. Alice computes s = 10^6 mod 23 = 12 and Bob computes s = 4^15 mod 23 = 12. Now, Eve can decrypt, read, and re-encrypt all messages between Alice and Bob.
   * What code of ethics, as set by the ACS (Australian Computer Society), are in direct confrontation with the attitudes of the CEO and directors?
     1. The Public Interest: This principle requires members to place the interests of the public above those of personal, business or sectional interests. Opting for a less secure system could potentially harm the public, especially if sensitive data is leaked.
     2. Integrity: This principle requires members to be honest, trustworthy, and to uphold the values of truth and honesty. By agreeing to build a less secure system, you could be compromising your integrity, especially if you believe that the system is not adequate to protect sensitive data.
     3. Competence: This principle requires members to work to the best of their ability, to keep their skills up to date, and to only undertake work that they are competent to perform. If you believe that the less secure system is not up to standard, then agreeing to build it could be seen as a breach of this principle.
   * If opting for the less secure system is a must, how do you avoid or lessen the repercussion of a security violation in the future (from both reputational and legal implication points of view).
     1. Implement robust monitoring and auditing systems: This will help to identify any potential breaches as soon as they occur, allowing for quick action to be taken.
     2. Regularly update and patch the system: This can help to protect against known vulnerabilities.
     3. Educate employees: Make sure all employees are aware of the importance of security and the potential risks of a breach. This could include training on how to identify and avoid potential threats.
     4. Develop a comprehensive incident response plan: This should outline the steps to be taken in the event of a security breach, including how to contain the breach, how to communicate with stakeholders, and how to recover lost data.
     5. Legal protection: Consult with legal experts to understand the potential legal implications of a breach and to ensure that the company is adequately protected.
   * Create a frequency table of English letters.
   * Create a frequency table of the letters in the cryptogram.
   * Sort both frequency tables in descending order.
   * Map the letters in the cryptogram to the English letters based on the frequency.
   * Replace the letters in the cryptogram based on this mapping.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| T |  |  |  |  |
|  |  |  |  |  |
| A | G | L | Q | V |
| B | H | M | R | W |
| C | I | N | S | X |
| D | J | O | T | Y |
| E | K | P | U | Z |
| F |  |  |  |  |