1. Who is Bruce Schneier? Why is he noteworthy? \*

He is an internationally renowned security technologist and author. He is commonly called as “security guru" because of his contributions to security.

1. In your own words, describe TwoFish \*

It is a 128 bit symmetric key block cipher which accepts a variable-length key up to 256 bits. It makes use of pre-computed key-dependent S-Boxes to perform substitution.

1. In your own words, describe Blowfish \*

Blowfish is a symmetric key block cipher that takes a variable-length key from 32 bits to 448 bits. It is a general-purpose algorithm to replace the ageing DES and it is also problem free from the constraints of algorithm.

1. In your own words, what are the similarities between TwoFish and Blowfish? \*

They are both symmetric block ciphers that accept a variable-length key to implement strong security over information. Both of them are used for security purposes.

1. In your own words, what are the differences between TwoFish and Blowfish? \*

TwoFish uses 128-bit block cipher which accepts a variable-length key of up to 256 bits while Blowfish takes a variable-length key from 32 bits to 448 bits.

1. In your own words, what is the Advanced Encryption Standard or AES? \*

The Advanced Encryption Standard or AES is standard for encryption adopted by the United States of America (USA) to encrypt data. It is a way for people to have a guide when it comes to encrypting.

1. In your own words, what is Rijndael? \*

It is an algorithm used for substitution linear transformation cipher. It is also a popular key schedule that inflates a key into a number of round keys separately to increase security.

1. Why do you think Rijndael was chosen as the AES? \*

Rijndael's key schedule makes use of a number of operations which will be depicted before describing the key schedule. It is also difficult to attack this kind of algorithm and if some may occur, it will only show little consequences.

1. Who is Phil ZImmerman? Why is he noteworthy? \*

He is the creator of Pretty Good Privacy also known as PGP which is the most widely used email encryption software in the world.

1. What is PGP? Why is it noteworthy? \*

It is a program that uses public-key cryptography for privacy and authentication to information. It is frequently used for encrypting and decrypting e-mails to increase its security.