1. There are two types of encryption algorithms: symmetric key encryption and asymmetric key encryption (also called public key encryption). To reach the same level of security, the key length for different algorithms can vary greatly. Please answer: to reach the same level of security as the 128-bit key for symmetric encryption algorithms, how long does the key need to be for RSA algorithm, and how long does the key need to be for elliptic curve cryptography?

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: NIST Recommended Key Sizes

For the same level of encryption as that of symmetric 128 bit key, RSA needs to have 3072 bits and Elliptic curve graph needs to have 256 bits of key.

2. Please describe one example in computer security to show that cryptography cannot solve all problems in security

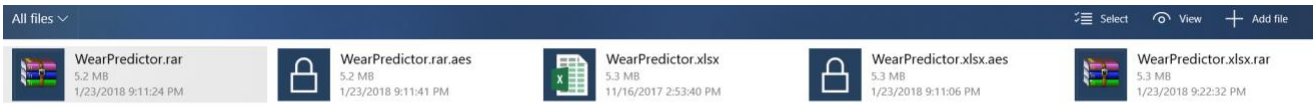
Cryptography can't protect against most denial-of-service attacks:

- By using Encryption, our information can be saved and can be made sure only the recipient can read the message. However, the attacker might not have the intentions just to intercept the message. Denial of service attacks are the best example for this.
- Hacker can send lot of unwanted/ garbage messages to the server and the server might stop responding due to overload of the messages to be processed. This makes the actual users from using the system.
- Also, the attacker might simply choose to delete the message while it is about to reach the other person.
- We can make some hardware changes in the router or the switches to handle lots of packets coming in the network from a source. But, this can't be just handled alone with just by encryption/cryptography.

***3.* Alice has a large text file (try a file at least 500KB). She wants to apply two operations to the file: compression (zip), and AES encryption. Please answer: when she applies the two operations in different orders, what will be the impacts and why?**

- As far as security is concerned, both the ways, the file is secure. But, it's mathematically safer to compress before encryption.
- Encryption works better on short messages, with a uniform distribution of symbols. Compression replaces a message with a non-uniform distribution of symbols by another, shorter sequence of symbols that are more uniformly distributed.
- Compression after encryption doesn't affect the encryption, which remains relatively weak due to the uniform distribution of plaintext.

(1) Generate (or download) a large text file (at least 500KB). Locate two software: one for AES encryption and one for compression. Now to the same source file, you apply the two operations in different orders. At the end, you will get two result files: one is encrypted then zipped, and the other is zipped then encrypted. Now write down the file size of all five files: the original file, two intermediate files, and two result files. Which result file is smaller?



- The zipped and then encrypted file is smaller.

(2) Please explain why the zipped-then-encrypted file is smaller in size.

When you discuss the size of the files, please consider the following question. Which type of files has better compression ratio? A file that contains a lot of repeated patterns? Or a file that looks totally random? Which type of files contain higher randomness (or higher entropy): a text file or an encrypted file?

- Compression software looks for patterns and replaces them with placeholders, so that those placeholders can then be replaced with the original patterns. The goal, of course, is to find patterns that take up more space than the placeholders.
- Say, we encrypt first and then compress, the resulting file will have random patters and almost impossible to find a common pattern to compress. Therefore, the encrypt and compress has more file size compared to other.
- On other hand, when you compress it first, the plain text would generally have lot of repeated patters which can be compressed. This result in smaller file. We can use this for encryption.