# Homework 6 Compression and encryption Answers

Files are compressed using a variety of techniques. An image file is compressed differently from a folder containing text files.

1. Compression reduces the size of a file by removing unnecessary data.
2. Explain the difference between lossy and lossless compression: [3]

1 mark for each point:

* Lossy compression removes data that is considered unnecessary
* Lossless spots patterns in data and summarises it in a shorter format
* Lossless reproduces the original data but doesn’t always compress by a significant factor
* Lossy can never recreate exactly the original data but does reduce file size significantly
1. Explain why Run-Length Encoding work well to compress a sound file without losing any of the original data: [3]

1 mark for each point:

* RLE reduces file size by summarising patterns
* Sound files often have long sequences of the same data
* Therefore RLE will yield significant savings in file size
* RLE doesn’t take out data just shortens the description of it
1. Sound files can also be encoded using lossy compression techniques. Describe why these techniques reduce files more significantly than RLE but can have a detrimental effect on the quality of the file: [3]

1 mark for each point:

* Lossy compression removes unnecessary data
* Sound files contain frequencies the human ear cannot detect
* These can be removed and the listener will not be aware so that the file size is reduced
* If this is taken too far however the sound will start to change and the quality will deteriorate
* RLE doesn’t remove this same data

Encryption is used to obscure data from being understood without authorisation. Files can be encrypted using various methods.

1. Two methods of encryption are the Caesar and Vernam ciphers.
2. Explain why the Caesar cipher can be easily cracked. [1]

1 mark for each point:

* There are only 26 possible combinations using the core alphabet which could easily be attempted using the brute force method.
* Simple frequency analysis could be performed to find the most probable key.
1. The Vernam cipher is proven to be unbreakable. Explain why. [2]

1 mark for each point:

* The key is never transmitted, it is passed to the recipient by hand
* The key is collected from a truly random source, rather than a computer generated ‘random’ source.
* A truly random key offers a normal distribution of characters rendering frequency analysis useless.

 [Total 12 Marks]