Understanding your kit

Hexadecimal

Description: Hexadecimal describes a base-16 number system. That is, it describes a numbering system containing 16 sequential numbers as base units (including 0) before adding a new position for the next number. The hexadecimal numbers are 0-9 and then use the letters A-F.

How to identify: If there are only 2 length pairs of numbers/letters/combinations, high chances are that it is encrypted in Hexadecimal.

Binary

Description: Binary is a base-2 number system invented that is made up of only two numbers: 0 and 1. This number system is the basis for all binary code, which is used to write data such as the computer processor instructions used every day.

How to identify: If the ciphertext is just 1's and 0's, high chances are that it is Binary.

Base64

Description: Base 64 is a group of binary to text schemes that represent binary data (more specifically a sequence of 8-bit bytes) in an ASCII string format.

How to identify: If it is a jumble of both alphabetic letters and numbers, but ends in =, high chances are that it is in Base64.

Decimal

Description: Decimal is the numeric representation of ASCII characters.

How to identify: If there are plenty of random numbers, including those higher than 100, high chances are that it is enciphered in Decimal.

ROT13

Description: A Caesar shift of 13 for any letter. For example, “A” is enciphered as “I” because “A” is shifted to the right by 13 positions. Similarly, to decipher, you shift the letter backwards by 13. For example, “Z” is deciphered as “M” as it is shifted to the left by 13. Any non-alphabetic letter is left untouched.

How to identify: If the ciphertext is mostly jumbled letters or structured like a sentence, high chances are that it is encoded with ROT13.