Base64

Base64 is an encoding technique, used to encode data (text or images), into readable characters. The particular characters are: A-Z, a-z, 0-9, +, /

Its not encryption, it's just a way to represent binary data using text.

Working:

1. lets take a word "mist"

2. Finding ASCII values and their binary representation for each letter:

m	109	01101101
i	105	01101001
s	115	01110011
t	116	01110100

3. joining them together into one long binary string (4 × 8 = 32 bits):

01101101 01101001 01110011 01110100

4. Base 64 uses 6 bits per symbol

11011 010110 100101 110011 011101 00

The last group only has 2 bits (00), so we'll pad it with four 0s → 000000

011011 010110 100101 110011 011101 000000

5. converting each 6-bit group into decimal and its base 64 character (there is this index table)

011011 27 b

010110 22 W

100101 37 l

110011 51 z

011101 29 d

000000 0 A

6. adding padding (=)

since we started with 4 bytes of data (which isn't a multiple of 3)

Base64 encodes in 3-byte chunks, so we need padding.

for t: we have 011101 00

and we add zeros to get 011101 000000

that's 2 Base64 characters worth of data, and 4 bits short (since 2×6 = 12 bits, but we only had 8 real bits).

So Base64 adds two "=" signs to fill out the last 4-character group.

final Base64 encoded text: ` bWlzdA==`

Note:

Bytes	Bytes in final group	Padding required
3	4	none
2	3	=
1	2	==

so for a 3 letter word, no padding is required. for a 4 letter word, `==` is required, and for a 5 letter word `=` is required.

my understanding:

when given text is divided into groups of 3 characters, let the number of characters in the end be n. the padding required is 3-n.

How to decode (summary):

1. Convert each character to its 6-bit binary value, according to base 64 index table.

2. Combine all bits into one long stream.

3. Split the stream into 8-bit chunks (bytes).

4. Translate each byte to its ASCII character to get the original text.

Caesar Cipher

Cipher is a simple substitution cipher, where each letter shifts a fixed number of places in the alphabet. This fixed number of places is called the "key". Both the sender and receiver has to know this key.

It is only applicable to letters (and sometimes numbers too). spaces stay the same.

Example:

“Mist” (when shifted by 5 letters): “Snxy”

Note:

It’s named after Julius Caesar, who reportedly used it to send secret military messages.

Vigenère Cipher

This is a smarter version of the Caesar cipher. it uses a keyword to decide how much to shift each letter.

Formula: `C=(P+K)mod26`

C is Ciphertext.

P is Plaintext.

K is keyword.

Let the word be MIST. Let the keyword be KEY

M I S T

K E Y K

(A-Z ---> 0-25 respectively)

M(12)	K(10)	12+10=22	W
I(08)	E(04)	8+4=12	M
S(18)	Y(24)	18+24=42---->16	Q
T(19)	K(10)	19+10=29---->3	D

Encoded Text: `WMQD`

Formula for decoding: `P=(C−K)mod26`