Encoding or Encrypting Payloads

Why encode, why encrypt?

- To prevent Antivirus and Reverse Engineers from detecting the malware as a malware.
- AV uses patterns of bytes to detect malware signatures
- Shellcode payloads have well-known malware signatures
- Encoding and encryption scrambles the data to make it different from well-known signatures

Difference encode vs encrypt

- Encode transforms data from one format to another format for use by another system, eg, sending binary data over email
- Encryption transforms data from one format (plaintext) to another format (ciphertext) using a secret key so that others cannot read the hidden information

Examples of Encoding and Encryption Algorithms

- Base64 (Encoding Algorithm)
- XOR (Encryption Algorithm)
- AES (Encryption Algorithm)