Design in security from the start

- When building a new system, include security as part of the design considerations rather than patching it after the fact.
- A lot of systems today were not designed with security from the start, resulting in patches that don't fully fix the problem!
- Keep these security principles in mind whenever you write code!

Human Factors:

•The users

•Users like convenience (ease of use)

•If a security system is unusable, it will be unused

•Users will find way to subvert security systems if it makes their lives easier

•The programmers

•Programmers make mistakes

•Programmers use tools that allow them to make mistakes (e.g. C and C++)

•Everyone else

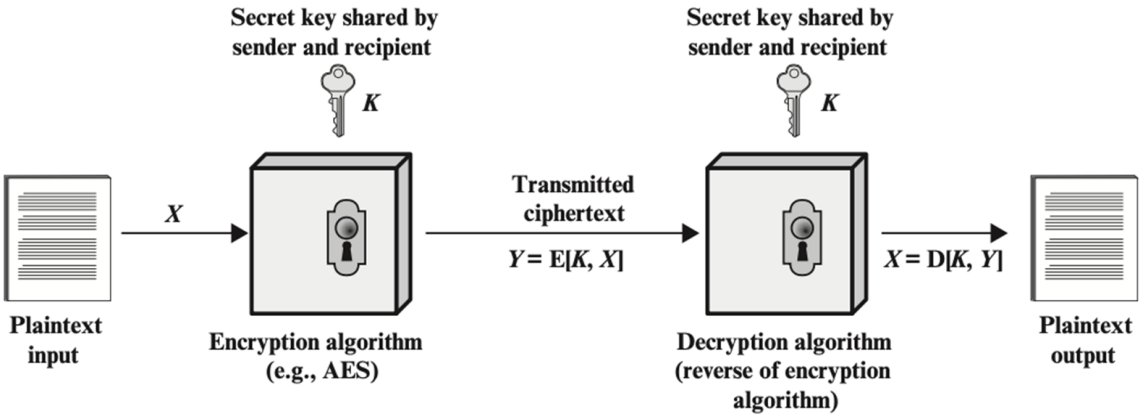
•Social engineering attacks exploit other people's trust and access for personal gain

Symmetric encryption

•Sender and recipient share a common/same key

•Was the only type of cryptography, prior to invention of public-key in 1970's

Symmetric Encryption Principles



Symmetric encryption:

Has five ingredients

- **Plaintext**: the original message or data
- **Encryption algorithm**: performs various substitutions and transformations on the plaintext
- **Secret key**

- **Ciphertext**: the coded message
- **Decryption algorithm**: takes the ciphertext and the same secret key and produces the original plaintext

Other basic terminology

•**cipher** - algorithm for transforming plaintext to ciphertext

•**encipher (encrypt)** - converting plaintext to ciphertext

•**decipher (decrypt)** - recovering plaintext from ciphertext

•**cryptography** - study of encryption principles/methods

•**cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key

Requirements

Two requirements for secure use of symmetric encryption:

- a strong encryption algorithm
- a secret key known only to sender / receiver

$$Y = E_K(X)$$

$$X = D_K(Y)$$

•assume encryption algorithm is known

•the security of symmetric encryption depends on the secrecy of the key

•implies a secure channel to distribute key