Encryption - create ciphertext from plaintext using algorithm
Symmetric encryption - key shared between multiple people
Attack encryption using knowledge of key + algorithm
DES - data encryption standard, most widely used, 56-bit key
Triple DES - uses 3 keys
Use hash function to ensure no tampering
DES - 56-bit key is greatest weakness
3DES - 168-bit key helps overcome this weakness
Hard to break encryption without repeating pattern
Block cipher - process blocks at a time
Stream cipher - continuously process input
Hash func. must be relatively easy to compute, collision resistant
Hash func. used to store passwords on computers