Week 4
Brute Force Attack

Brute Force Attack

- In general, we assume that the attacker knows the algorithm used for encryption
- If the algorithm is truly strong, the only way to decrypt the algorithm's ciphertext without the key is
  - To try every possible key until the right one is found that decrypts the ciphertext
- Example in the decimal system
  - One-numbered lock: 10 possible numbers (0 to 9)
  - Two-numbered locks: 10 x 10 = 10^2 = 100 possible numbers (00 to 99)
  - Three-numbered locks: 10 x 10 x 10 = 10^3 =1000 possible numbers (000 to 999)
  - N-numbered locks: 10^n numbers
    - 10^n is the maximum number we need to try to find the key!

Brute Force Attack on DES

- A DES key is 56 bits long (binary system)
  - There are 2^{56} (approximately 7.2×10^{16}) possible keys
  - After 7.2×10^{16} trials, the attacker can find the key
  - In 1998, Electronic Freedom Foundation (EFF) designed a chip ($250,000), which was able to find a DES key in 56 hours
  - NIST (National Institute of Standard and Technology) declared DES officially obsolete (May 2004)
- Replacement algorithms for DES have been introduced.
  - Double DES, Triple DES, AES

SYRACUSE UNIVERSITY
SUOS
CULTORES
SCIENTIA
CORONAT