Secret Key Cryptography – I

DES (Data Encryption Standard)
- Developed by the National Security Agency (NSA) around 1977
- Secret key scheme
- No one has been able to break DES
  - Encryption schemes are controlled and developed by U. S.
  - Phil Zimmerman created PGP – free scheme
    - In order to be effective everyone must use it so the government doesn’t suspect anything
- Why are secret key schemes used?

Check sum bit – parity of the other bits – zero if an even # of 1s, one otherwise.

```
0 1 2 3 4 5 6 7  P
1 0 0 1 1 1 0 1  1
```

Last bit is used to check against bit flips during transmission to help keep integrity of data
DES scheme:

Figure 3-2. Basic Structure of DES

- To “crack” means: given input/output examples, you can decipher the key
- DES permutation is public and does not make it any harder to crack
How keys are generated:

- Encryption and decryption are the same
  - From output can get input

\[
L_{i+1} = R_i
\]
\[
R_{i+1} = L_i \oplus \text{mangle}(K_i, R_i)
\]
\[
L_i = R_{i+1} \oplus \text{mangle}(K_i, L_{i+1})
\]
\[
R_i = L_{i+1}
\]

Figure 3-6. DES Round

- Encryption and decryption are the same
  - From output can get input
Using brute force attack:

- $2^{56}$ – possibilities for a key
- $2^{56} \approx 64 \times 10^{15}$

- Why are secret keys used in browsers?
  - Public key is much slower and computationally expensive than secret key. It is much faster to use secret key cryptography.
- 3DES – keys sized 112 → $2^{112}$ possibilities – can’t brute force attack because it would take too long
- Government and large corporations are big spenders in encryption
- As the hardware becomes faster and more powerful the encryption will have to get stronger