- **CIA**, a modern definition. Confidentiality: prevent unauthorized reading of information. Integrity: detect unauthorized writing of information. Availability: data is available in a timely manner when needed.

- **Network Security**. Various protocols play a critical role, and cryptography matters a lot in protocol (especially network protocols) design and analysis.

- **Kerckhoof's Principle**. The system is completely known to the attacker; only the key is secret; the crypto algorithms are not secret.

- **Confusion and Diffusion**. Confusion: obscuring the relationship between plaintext and ciphertext. Diffusion: spreading the plaintext statistics through the ciphertext. A little note: hash function can be viewed as *one way cryptography*.

- **Block Cipher**. It's really just an "electronic" version of a codebook, and employs both confusion and diffusion.

Algorithm 1 RC4 Keystream Byte

```
$i = (i + 1) \mod 256$
$j = (j + S[i] \mod 256)$
swap $(S[i], S[j])$
$t = (S[i] + S[j] \mod 256)$
$Keystream\ byte = S[t]$
```

- **Feistel Cipher**. It's a general cipher design principle. $L_i = R_{i-1}$ and $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$.

- **DES**. The security of this cryptosystem has much to do with *S-box*. Steps: an initial permutation before round 1; halves are swapped after last round; a final permutation applied to R_{16}, L_{16}.

-