- **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}.

- **Block Cipher Modes**. ECB: encrypt each block independently. CBC: chain the blocks together. For this mode, a random initialization vector is required. CTR: block cipher acts like stream one.

- **Data Integrity**. The encryption process does provide confidentiality, but no guarantee of integrity.

Algorithm 2 Key generation for RSA public key encryption

Ensure: Each entity creates an RSA public key and a corresponding private key. Each entity A should do the following:

1. Generate two large random and distinct primes p and q, each roughly the same size.
2. Compute $n = pq$ and $\phi = (p-1)(q-1)$.
3. Select a random integer e, $1 \leq e \leq \phi$, such that $\gcd(e, \phi) = 1$.
4. Use the extended Euclidean algorithm to compute the unique integer d, such that $ed \equiv 1 \mod \phi$.
5. A's public key is (n, e), private key is d.

- **RSA Validity Proof**.
  - Since $ed \equiv 1 \mod \phi$, there exists an integer k such that $ed = 1 + k\phi$.
  - Now if $\gcd(m, p) = 1$, then by Fermat's theorem, $m^{p-1} \equiv 1 \mod p$.
  - Raising both sides of this congruence to the power $k(q-1)$ and then multiplying both sides by m yields $m^{1+k(p-1)(q-1)} \equiv m \mod p$.
  - On the other hand if $\gcd(m, p) = p$, then this last congruence is valid since each side is congruence to 0 mod p.
  - Hence, in all cases, $m^{ed} \equiv m \mod p$. By the same argument, $m^{ed} \equiv m \mod q$.
  - Finally, since p and q are distinct primes, it follows that $m^{ed} \equiv m \mod n$. And hence, $c^d \equiv (m^e)^d \equiv m \mod n$.

- Life is never that easy.