1. Define (4)

Principle of security:
If an access is not permitted within an individual system, it must not be permitted under secure interoperation.

Principle of autonomy:
If an access is permitted within an individual system, it must also be permitted under secure interoperation.

2. True or false (6)

[F] $D_k(E_k(D_k(y))) = E_k(D_k(E_k(x)))$ for $x = y$

[F] $D_k(E_k(D_k(y))) = E_k(D_k(E_k(z)))$ for $y = E_k(x)$ and $z = (D_k(E_k(x)))$

[F] Product of two relatively prime numbers is a prime.

[T] For an RBAC configuration with no role hierarchy, `assigned_users(r)` and `authorized_users(r)` would be the same each role $r$.

[T] Even if each security domain is secure, when we allow cross-domain accesses, they can introduce security holes in a system.

[T] In known plaintext attack, the attacker's primary goal is to find the key $K$ used.

[F] Caesar is a transposition cipher and its key weakness is that the key is too short.

[T] The key to attacking Vigenere cipher is to find out the period of the key.

[F] For $k = 5$, “ALIVE” would mean “FQMAJ”.

[T] If $(a \equiv r \mod m)$ then for some integer $q$, $a = m.q + r$.

[T] If $(RS, n) = (\{r_1, r_2, r_3\}, 2)$ defines a SSD constraint, then the user assignment $UA = \{(u, r_1), (u, r_2)\}$ is not valid.

[F] If $(RS, n) = (\{r_1, r_2, r_3\}, 2)$ defines a DSD constraint, then the user assignment $UA = \{(u, r_1), (u, r_2)\}$ is not valid.