SHA-1 is considered to be very secure. **False**

HMAC can be proven secure provided that the embedded has function has come reasonable cryptographic strengths. **True**

The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computer discrete logarithms. **True**

A token is the best means of authentication because it cannot be forged or stolen by an adversary. **False**

Depending on the supplication, user authentication on a biometric system involves either verification or identification. **True**

Memory cared store and process data. **False**

The authentication function determines who is trusted for a given purpose. **False**

External devices who is trusted for a given purpose. **False**

The default set of rights should always follow the rule of least privilege or read-only access. **True**

Traditional RBAC systems define the access rights of individual users and groups of users. **False**

A **brute-force** attack involves trying all possible private keys.

Although the **timing** attack is a serious threat, there are simple countermeasures that can be used such as constant time calcs, random delays or binding computations.

**RSA** was the first published public-key algorithm.

Presenting or generating authentication information that corroborates the binding between the entity and the identifier is the **identification step.**

The **user education** strategy is when users are told the importance of using hard to guess passwords and provided with guidelines for selecting strong passwords.

To counter threats to remote authentication, systems generally rely on some form of **challenge-response** protocol.

**Access control** implements a security policy that specifies who or what may have access to each specific system resource and the type of access that is permitted in each instance.

**DAC** is the traditional method of implementing access control.

**RBAC** is based on the roles the users assume in a system rather than the user’s identity.

An approval to perform an operation on 1 or more RBAC protected objects is **permission.**