AbdelRahman Adel
17012296

Date: \ \

Assignment 3

(1) The assurance that no third party is masquerading as either A or B comes from the fact that only the authentic parties (A and B) and the trusted authentication server possess the necessary keys to decrypt and encrypt messages correctly. Any attempt by a third party to masquerade as one of the authentic parties would fail because they wouldn't posses the correct secret keys needed for encryption and decryption.

(2) nonce = "number used once". A value that is only used once in a cryptographic communication session. They are typically random or unique values

They are used to prevent replay attacks.

(3) 1- User Authentication
2- Single Sign On (SSO)
3- Secure Communication between Networked Systems
4- Authentication

(4) Generic Security Services - Application program Interface.

GSS-API serves as a bridge between applications and the Kerberos authentication system

(5) Algorithmically Generated Random Numbers:
- Generate random numbers using deterministic algorithms that start with a seed value and a formula and can be predictable if you know the seed

True Random Numbers:
- Generated from a source of entropy from a physical property which is truly unpredictable

Date:

(6) 1- key and Seed

2- Pseudorandom Number Generator (PRNG)

3- Initial Vector (IV)

4- Cryptographic Operations

5- Periodicity & Reproducibility

6- Security Analysis