Computer Security - IV10113
Quiz 2

1,

True

2,

False

3,

False

4,

True

5,

-Nonces help to protect against playback(replay) attacks
The nonce is already used and cant be reused, next nonce is what I get from reciever.

-Nonces help to protect from attacks where an imposter claims to be Alice and reuses previous information to prove it.

-Bob generates a nonce and challenges Alice to encrypt it. If Alice can encrypt the nonce, Bob knows that she has the key, and she has been authenticated

---

6,

Collectability

7,

Random numbers
Time stamps
Sequence numbers

8,

Trojan hourse
Spyware

9,

Contains user records but no password-related information. - /etc/passwd

Contains passwords hashes - /etc/shadow

Contains information about hashing algorithm: /etc/shadow

A password is hashed many times in order to harden the hashing operation - Password stretching

Randomization of the password hashing operation - salting

10,

Showing your boarding pass when entering: what you have

Using the door phone(voice) to ask your friend to unlock the entranche: who you are

Signing a contract by putting your name in handwriting on paper:
what you have

unlocking a door by entering a passcode: what you know

11,

Prevent the use of dictionary words in password

Use a slower function for computing password hash

Blocking an account after too many unsuccessful login attempts

---

12,

Buffer overflows are possible because of mistakes or oversights by the programmer.

With a properly designed buffer overflow attack, the attacker may take control over the program being attacked.

13,

The salt is generated by the server

The salt makes offline dictionary attacks more difficult

The hash is computed from the salt and Alice's password