QUIZ 1, Crypto

Name: **Himesh Buch** NetID: **hnb17** Grade:

1. In the three security properties, crypto protects **privacy** and **secrecy** , but not **authenticity**.
2. There are two types of attackers we consider in crypto: the ones that can eavesdrop, known as **passive** attacker, and the ones who have full control of the channel, known as **active** attack.
3. **Steganography** covers the existence of the information while crypto hides the meaning of the message.
4. To find the key length of Vignere cipher, we use **kasisky** test by starting finding repeating patterns of length at least **3** .
5. The adversarial model for ciphers include **Ciphertext-only** attack,

**Known-plaintext** attack, **Chosen plaintext** attack and

**Chosen-ciphertext** attack.

1. In the binary version of One-time Pad, we use **XOR** (bit) operation to encrypt/decrypt.
2. To achieve perfect secrecy, one key can be used for **0 (never)** time(s) in OTP.
3. Perfect secrecy implies that key-length **>=** message length.
4. The idea of stream cipher is to replace the random key in TOP with

**pseudo random**

1. A cryptographically secure PRNG satisfies the **next-bit** test.
2. The same plaintext always gets the same ciphertexts. [True | **False**]
3. We propose two methods to formalize computational security:

**concrete** and **asymptotic** .

1. The encryption modes for black ciphers: **counter mode (CTR)** ,

**ECB(Electronic Code Book)** and **Cipher Block Chaining (CBC)**.

1. A MAC (message authentication code) scheme is a **hash family** .
2. An RSA algorithm gives public key (e, n) and private key d. To encrypt, we should use

**public key (e, n)**and to decrypt, we use **private key d**. To generate a signature, we use **private key d** and to verify the signature, we use **public key (e, n)**.

1. In IND-CPA security, IND stands for **indistinguishability**. And digital signature provides authentication, data integrity and **Non-Repudiation**.
2. Diffie-Hellman protocol can be used for **establishing a shared secret between parties (creates cryptographic keys for encryption algorithms)**
3. In Kerberos, if there are N parties and they are allowed to talk to each other, **N**  keys are needed.