Jaleel Rogers
Professor Mukhopadhyay
CIS 4362.01
31 January 2024

1. **Why is a one-time pad considered to be the most secure form of encryption?**

   A one-time pad is a symmetric cipher with a string of random bits generated by a Cryptographically Secure Pseudorandom Number Generator (CSPRNG). Each key letter is used once for only one message encryption while the message is decrypted with each letter of the ciphertext. In both cases, the sender and receiver destroy the pad pages after the message has been encrypted or decrypted. The attacker can't compute the plaintext from the ciphertext without information about the key, even with brute force, because no portion of the key is reused for another encryption.

2. **What are the properties of a good hash function?**

   Properties of a good hash include being collision resistant so that it's infeasible for a computer to find a duplicate string to create a collision, deterministic so that the expected input has the same hash output, computationally efficient for speed, and at least 128 bits for a decent length for the key size including padding the message to such a length.

3. **Consider the following function:**

   P is a plaintext in binary. P is divided into blocks of 8 bits. If the length of P is not a multiple of 8, then a necessary number of 0s is added to the LSB so that (length of P + number of padded 0s) mod 8 == 0. Therefore, the total amended length of P is 8n, where n is the number of 8-bit blocks. Each of these blocks are then exclusive ORed with each other to obtain a final string of 8 bits, which we name HashX. Is HashX a good hash? Which properties of a good hash are present in HashX, and which are excluded? Explain.

   HashX is a reasonably good hash, and some information is excluded from HashX. Properties that are good for this hash are that it uses padding to keep a consistent size of the hash, uses a logical operator XOR, which is excellent for providing

Jaleel Rogers
Professor Mukhopadhyay
CIS 4362.01
31 January 2024

unique hashes compared to OR and helps against the likelihood of a collision, and there is a buffer to compute the values for the message digest by dividing the blocks into 8 bits. Excluded is the number of bits in the whole message before hashing and the size of the output in bits after the value has been hashed.

4. **Write the principal differences between symmetric and asymmetric cryptography.**

   The main difference between symmetric and asymmetric cryptography is that symmetric cryptography uses the same key for encrypting and decrypting the message for the sender and receiver, along with it having a less complex algorithm compared to asymmetric cryptography, making it faster and simplicity of key management due to one key. For asymmetric cryptography, there are two keys: one for encryption and the other for decryption. The key used for encryption is the public key, while the message is decrypted using the private key. In addition, key management is more complex than symmetric cryptography because there are two keys with different goals and security, and the quality of the keys is crucial for asymmetric cryptography.

5. **How does entropy correlate to the strength of a cryptosystem?**

   The correlation between entropy and the strength of a cryptosystem lies in the number of bits required to represent the space, reflecting the level of uncertainty or unpredictability. Entropy can be viewed as a measure of the system's randomness. A higher entropy implies greater unpredictability, making it more challenging to brute-force the algorithm. In practical terms, the larger the entropy of a cryptosystem, the more resilient it is against brute-force attacks. For instance, a cryptosystem using only a 3-bit key is considerably more susceptible to cracking than one employing an 8-bit key for encryption. Higher entropy contributes to increased security by introducing complexity and making it more difficult for attackers to guess or systematically try all possible keys.

Jaleel Rogers

Professor Mukhopadhyay

CIS 4362.01

31 January 2024