Homework 3 Paper and pencil problems Cody Williams

- 2.2. (3 pts): Random J. has been told to design a scheme to prevent messages from being modified by an intruder. Random J. decided to append to each message a hash of that message. Does this solve the problem? Why?

Answer: Random. J's method does not solve the problem because a hash message can be created and appended to a message by anybody. The appending of a hash value to the end of a message can be undetectable to Random. J.

- 2.3. (4 pts): Suppose Alice, Bob, and Carol want to use secret key technology to authenticate each other. If they all used the same secret key K, then Bob could impersonate Carol to Alicia (actually any of three can impersonate the other to the third). Suppose instead that each had their own secret key, so Alice uses K_A, Bob uses K_B, and Carol uses K_C. This means that each one, to prove his/her identity, responds to a challenge with a function of his/her secret key and the challenge. Is this more secure than having them all use the same secret key K? (Hint: what does Alice need to know in order to verify Carol's answer to Alice's challenge?)

Answer: This method of Communication is more secure than the first method of Communication. Assigning Seperate Secret Key Values to Seperate people provides a mechanism for the prevention of Impersonation. This method is effective for preventing Impersonation because each person must know their place in a randomly hashed Value Without knowing the values/ places of other people participating in the random generation.

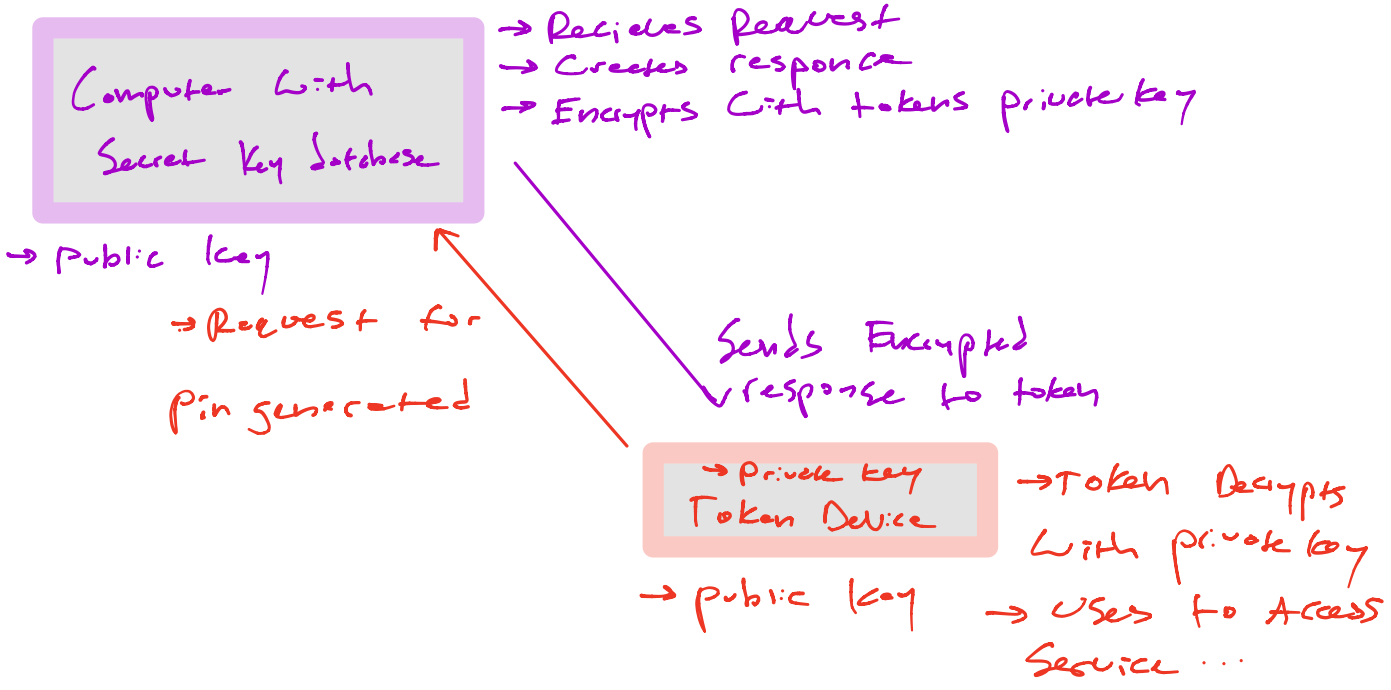
- 2.4. (4 pts): It is common, for performance reasons, to sign a message digest of a message rather than the message itself. Why is it so important that it be difficult to find two messages with the same message digest?

Answer: Yes, it is common to sign the digest (hash) of a message instead of the message itself to improve performance. If a message is sent along with a hash that has been encrypted, message integrity will still be retained because validation of the message will fail when the encrypted and generated hashes are compared.

It is important for finding 2 messages with the same hash to be hard because if an attacker finds that 2 hashes map to the same message, it is possible for the attacker to change an intercepted message without the message receiver knowing

- 3.2. (7 pts): Token cards display a number that changes periodically, perhaps every minute. Each such device has a unique secret key. A human can prove possession of a particular such device by entering the displayed number into a computer system. The computer system knows the secret keys of each authorized device. How would you design such a device?

Answer: This Question is describing a form of 2-factor authentication "2FA", similar to the "duo" Service used by TAMU. the process of multi factor Authentication



- 3.3. (7 pts): How many DES keys, on the average, encrypt a particular plaintext block to a particular ciphertext block? Please explain.

Answer: (from discovery.csc.ncsu)

→ 2^{56} possible DES keys

→ 2^{64} possible Ciphertext blocks

$2^{56} - 2^{64} = 2^{-8} = 1/256$ Cipher text blocks for every DES key

- 3.5. (7 pts): Suppose the DES mangler function mapped every 32-bit value to zero, regardless of the value of its input. What function would DES then compute?

Answer: The Des Mangler function follows the process below

1. Initial permutation
2. Swap left and right halves of word
3. final permutation

With 16 rounds of the DES function running, and the initial & final rounds of permutation, the Output of the DES is the same as the input. Therefore, DES mangler would be Computing the Identity function.

- 4.2. (7 pts): The psudo-random stream of blocks generated by 64-bit OFB must eventually repeat (since at most 2^{64} different blocks can be generated). Will $K\{IV\}$ necessarily be the first block to be repeated?

Answer: Block IV will be the first block to be repeated. because the previous block to any encrypted block $K\{x\}$ must be the decryption of that encrypted block. Therefore, for any 2 encrypted blocks $K\{x\}$ & $K\{y\}$, their decrypted blocks will also be equal.

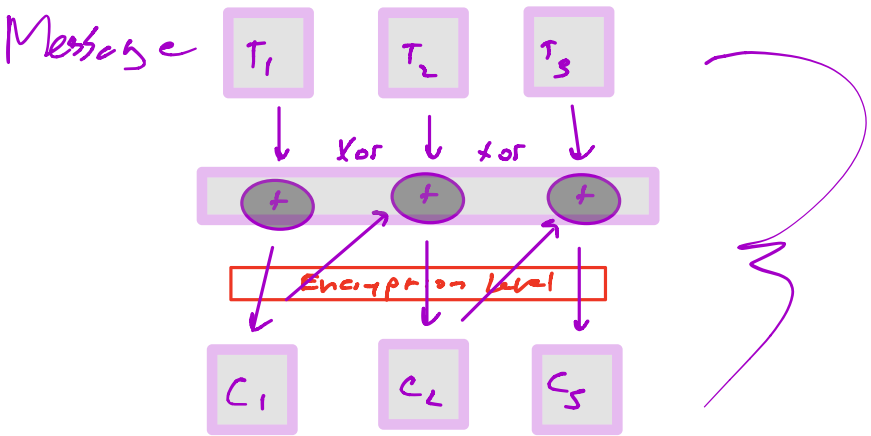
Example..

These blocks are the same and occur before K{n3

- 4.6. (7 pts): Consider the following alternative method of encrypting a message. To encrypt a message, use the algorithm for doing a CBC decrypt. To decrypt a message, use the algorithm for doing a CBC encrypt. Would this work? What are the security implications of this, if any, as contrasted with the "normal" CBC?

Clarifying question: If we encrypt a message using CBC decryption and decrypt using CBC encryption, does this achieve the same result?

Answer: In CBC encryption, some given plain text is encrypted using an initialization vector (whose contents are chosen at random and an assigned encryption key.

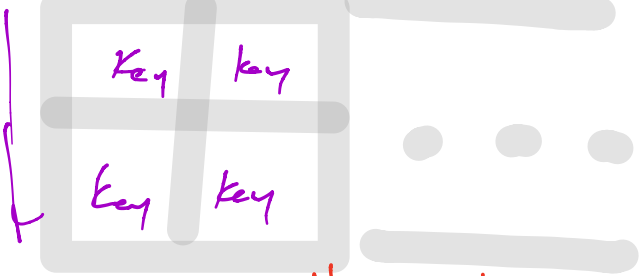


CBC decryption is essentially reverse process of CBC encryption: Because of this, if CBC decryption happened before CBC encryption the same function could be achieved.

Security Implications: Because cbc encryption → decryption and decryption → encryption Achieve the same goal, the security implications should be the same as the standard CBC process.

- 4.4. (Bonus question, 7 pts): What is a practical method for finding a triple of keys that maps a given plaintext to a given ciphertext using EDE? Hint: It is like the meet-in-the-middle attack mentioned in the class (detailed in the KPS textbook).

1. Select a random pair of keys, Encrypt the Cipher text with the Second key
2. Create some sort of table that utilizes a loop to choose a key at random



3. Encrypt the message with the randomly Selected key, Store key & Encrypted message In that table
4. Select a key pair, Encrypt our Cipher with one of the randomly Selected keys
5. encrypt the newly encrypted plain text message with the key and check the table, If the result is in the table, then we have found the result.