Assignment 1 Solutions

1. Advantages of OTP:

Verifiable plaintext - The sender and the receiver will ensure that the exact same message that was sent will be received because it’s just a simple modulo addition of 26(in most cases). Given that the key is with both the sender and receiver, it’s quite easy to apply the key and know if the message is garbled or not, because if the message doesn’t make sense, (since there’s no concept of a checksum in OTP), the receiver will immediately know if the message makes sense or not.

The hotline between Moscow and Washington, established in 1963 after the Cuban Missile crisis, used teleprinters protected by a commercial one-time tape system. Each country prepared the keying tapes used to encode its messages and delivered them via their embassy in the other country. A unique advantage of the OTP in this case was that neither country had to reveal more sensitive encryption methods to the other. (Source: Wikipedia)

This is possible only while using the OTP method of encryption and not the CBC mode.

The OTP also gives a high level of security,(along with easy computation since there is just one operation of XOR-ing with the key) albeit at a higher cost and it is considerably less vulnerable to brute force attacks because there is just one key that exists to decrypt the message which has to be right, or there is no way that the adversary will know how to crack the cipher text.

The above advantage applies over all the three techniques described.

Inherent Disadvantages of CBC:

* The CBC mode allows only for an entire block to be encrypted. The OTP lets every single character be encrypted with no dependency on any other part of the message.
* Along with the key, even the IV needs to distribute to both parties who are to be privy to the information (plaintext).
* The sender and receiver have to encrypt and decrypt twice and there’s an additional overhead. This doesn’t exist in the OTP.
* When introducing a degree to randomness to the cipher text, if the first block is supposed to be random (varying the plain text) to make a random IV to encrypt the actual data, and if the adversary knows the IV, it would still help in some way for the adversary to gain a possible advantage in decrypting the data by guessing the key. So any random text that may be introduced in the data to obtain a random IV can be guessed by simply guessing the key (which is slightly easier than attempting to guess both the IV and the key together)
* If the adversary modified the encrypted block cipher text, say Yk, then it is very predictable that the next cipher block Yk+1 is going to be garbled. So in essence, if the adversary can’t decrypt the message, he can at least gargle up the block and the recipient can’t read the original message if he applies the modified Yk as the IV. This however, can be solved by adding a 64-bit CRC .

1. Advantages over the use of RSA used as a block cipher

The advantages of the OTP considerably remain the same over RSA using cipher blocks.

Verifiable plaintext - The sender and the receiver will ensure that the exact same message that was sent will be received because it’s just a simple modulo addition of 26(in most cases). Given that the key is with both the sender and receiver, it’s quite easy to apply the key and know if the message is garbled or not, because if the message doesn’t make sense, (since there’s no concept of a checksum in OTP), the receiver will immediately know if the message makes sense or not, by applying a checksum.

The OTP also gives a high level of security, albeit at a higher cost and it is considerably less vulnerable to brute force attacks because there is just one key that exists to decrypt the message which has to be right, or there is no way that the adversary will know how to crack the cipher text, and decrypt the message. However, in the case of the RSA used as a block cipher, the private key is always the inverse of the public key. Through brute force analysis, the decryption by the adversary can be done, if it is computationally feasible. However, the feasibility of cracking the one key to break the OTP encryption is close to impossible.

The main disadvantage of using the RSA when used as a block cipher is that it is vulnerable to impersonation.

The distribution of the private key and public key pose a significant overhead to both the sender and the receiver, and the private key must be sent over a secure communication channel. In the case of the OTP, we just have to distribute the common key used to encrypt and decrypt.

Although the RSA can provide data and origin authentication which is not provided by the OTP, it does present the problem of significant calculations, beginning with the calculation of the totient function, and then eventually assigning e and d, all to send a bunch of numbers, which is altered cannot be deciphered whatever happens. The private key is useless if the adversary changes the cipher text. The OTP just uses one key, for both sender and receiver and is relatively much less complex. Further, the adversary could just re arrange the blocks and change the meaning of the message with no way for the receiver to get the original message back.

RSA using block ciphers also means there is a lot of random data inserted before the actual data (character) is sent to add another layer of security, further making it easier for the adversary to rearrange the blocks, and make the actual character that was to be enciphered not readable. The OTP replaces word for word cipher text in the block, so if one character does not make sense, it’s slightly easier to figure out what the original word would have been. The main disadvantage of this again is that the padded cipher texts, large in number may lead to similar texts in the dictionary. If the adversary can figure out the dictionary, then he can openly interpret the message. (Source: Wikipedia)

Using the RSA as a cipher block can also be very impractical if there are a very large number of users. This problem will not present itself in the OTP.

Lastly, the 1024 bit key used in the RSA can easily be broken in the near future as most experts suggest, the OTP’s key size is always equal to the size of the block that it is encrypting.

1. Advantages of OTP over the use of AES in output feedback mode

Main disadvantage with the OFB is the prefix problem. Since every block is encrypted using the same key and the IV, we can easily replace any one of encrypted blocks with another block, (say block 7) and it’ll always remain block 7. Since there’s no dependency in this case on the previous cipher block generated, anything is essentially replaceable.

The size of the key is 64 bits, with the last 8 bits used for parity, making it less secure. (Source: Old Dominion University)

If one block is lost, the rest of the blocks will not end up making any sense, however hard the receiver tries to decrypt the message.

No data can be read, if stored on any disk unless the preceding blocks are decrypted(Source: Old Dominion University)

Also, since the adversary is free to change any cipher text, and there’s no repercussions, like the next block being garbled, the adversary can essentially change any cipher block and the receiver will get information which has been tampered with. Although this could be potentially the same problem as with the OTP, this type of encryption is more of a disadvantage because the complexity of it is relatively higher than the OTP, but it is still vulnerable to these kinds of attacks.

The advantages of the OTP still hold good in this case because it still holds a significant advantage over the OFB mode of operation for a block cipher.

Verifiable plaintext - The sender and the receiver will ensure that the exact same message that was sent will be received because it’s just a simple modulo addition of 26(in most cases). Given that the key is with both the sender and receiver, it’s quite easy to apply the key and know if the message is garbled or not, because if the message doesn’t make sense, (since there’s no concept of a checksum in OTP), the receiver will immediately know if the message makes sense or not.

The OTP also gives a high level of security, albeit at a higher cost and it is considerably less vulnerable to brute force attacks because there is just one key that exists to decrypt the message which has to be right, or there is no way that the adversary will know how to crack the cipher text, and decrypt the message.