2 Modern ciphers

Answers

1. Alice and Bob living in 2020 make use of modern crypto systems. You are in the role of Mallory and got hold of some exchanged ciphertexts. There are various attack models in cryptography. A good overview that allows to dive into each attack models detail is provided at Wikipedia, Attack Models. However, I want you to think about some simple cases. Can you run a brute-force attack (cryptographers call this exhaustive key search) against the ciphertexts if
    1. you know the plaintext is random?
        - Answer: no as it is not possible to determine when the plaintext was found (statistics on word/character distributions won't work)
    2. you know part of the plaintext but not the algorithm used?
        - From my understanding this makes the brute force attack difficult. What could be done is to not only try different keys but also different algorithms with each key. However, this would make the brute force attack go longer and when an unknown algorithm is used, we might not succed.
    3. you know part of the plaintext and the algorithm used?
        - yes, the attacker can search the known plaintext in the result of every iteration of the brute force attack.
2. Symmetric ciphers can be categorized in either stream or block ciphers. Could you
    1. briefly explain the difference of the two approaches
        - block: based on a key of a certain length, a plaintext is encrypted by applying and algorithm that operates on groups of bits (blocks)
        - stream: derived from a key, an endless pseudo random stream is generated which is combined with the plaintext (XOR) to generate the cybertext.
    2. name algorithms as an example for both
        - block: AES, 3DES
        - stream: RC4
    3. discuss speed of stream and block ciphers
        - block ciphers take longer to encrypt than stream cipers as the every bit of the output depends on every bit of the input (plaintext and key) which has to take time (and in practice multiple rounds). A stream ciphery only has to generate the random stream and apply an XOR operation combining the stream with the plaintext.
    4. describe the differences in error propagation
        - error propagation means (from my very modest understanding) that a transmission error (bit swapped) in an encrypted block makes it not only impossible to decrypt this block but also others as they depend on that particular block for decription. There are multiple encryption modes (ECB, CBC...) which affect error propagation characteristics.
            - also see http://paper.ijcsns.org/07_book/200611/200611B14.pdf
    5. explain the term "message dependency"
        - Not really sure.. but here my guess: In a block cipher when, the blocks are encrypted independently, the same plaintext results in the same ciphertext which facilitates breaking the ciphertext. Message dependency means that each blocks gets some input from the

previous block ensures that the same input block, will have a different cipher (withing the same text of course)
    - some hints
      https://www.tutorialspoint.com/cryptography/block_cipher_modes_of_operation

Notes

Some attacks (not conclusive, also see wikipedia: https://en.wikipedia.org/wiki/Attack_model)

- brute force attack
- known-plaintext attack: attacker has access to some plaintext and the derived cybertext (plaintext > cipher)
- chosen-cipertext attack: attacker can choose ciphertext and can access the plaintext (cipher > plaintext)
- Open key model attacks: attacker has some knowledge about the key
- side-channel attach: not attacking the cipher itself but using other data (e.g.: sound produced by keystrokes, measuring time that is needed to compute)

Block cipher modes (AES and probably others)

- ECB Electronic code book
- CBC Cipher block chaining
- CBF Cipher feedback
- OFB Output Feedback
- CTR Counter mode
- see:
    - https://www.tutorialspoint.com/cryptography/block_cipher_modes_of_operation
    - https://www.cs.columbia.edu/~smb/classes/f20/l_crypto-3-modes.pdf