Marc Hosecloth

February 15, 2016

hw1-part2, question 1

(a) Because the Substitution Cipher (specifically a simple monoalphabetic cipher) uses fixed substitution over an entire message, any pair of identical character strings contained in the plaintext message will map to identical strings of ciphertext. For example, consider the plaintext message “The council will meet at the secret location tomorrow.” If we utilize a simple monoalphabetic cipher that maps each character 13 spaces forward relative to its position in the alphabet (ROT13), then we will obtain “Gur pbhapvy jvyy zrrg ng gur frperg ybpngvba gbzbeebj.” as ciphertext. We see that the string “gur” appears twice in the ciphertext, mapping from the plaintext string “the.” Hence, an adversary has the potential to learn something about the plaintext other than its size, violating perfect secrecy.

(b) Since |P1| = |P2|, P1 XOR P2 will produce another unique pad, which we will call P’. Note that |P’| = |P1| = |P2| = |M|, so P’ can be used as a one-time pad if we XOR it with M. We know that any given one-time pad will provide perfect secrecy unless it is reused, so there is no reason to believe that P’ will not achieve the same effect as a sufficient one-time pad for the message M, preventing the adversary from learning anything about M except for its size. Further, M XOR P’ will encrypt M in such a way that the search space of a brute-force attack will be 26^size(M).

(c) Electronic Code Book (ECB) mode encryption shares a weakness with the Substitution Cipher, in that identical pairs of plaintext blocks are encrypted into identical blocks of ciphertext. Hence, under this protocol, Professor Pedantic will find that transmitting recurring strings of

information (i.e. passwords and common commands) will allow an adversary to learn about his encryption scheme. Further, ssh can already provide both confidentiality (encrypted information sent through tunneling) and authenticity (use of passwords to log into the shell), while AES in ECB mode will only provide confidentiality whose strength lies in the key used for AES encryption.

(d) Although multiple vulnerabilities have been discovered in RC4, it can still theoretically provide some level of confidentiality so long as the confidentiality key k1 is not compromised. I am, however, dubious of this confidentiality's strength and would not place much trust in it, but it is nonetheless confidentiality. My main problem with Professor Pedantic's scheme is his claim that it achieves authenticity. An authenticity scheme's strength should depend solely on the size of the authentication key (akin to standard encryption) and the strength of the algorithm used to provide authenticity (for SHA-256: resistance against birthday attacks, collision resistance, etc). If an adversary were able to intercept the messages and knew both k1 and k2, they could decrypt both messages, alter them arbitrarily while making sure that the altered messages match, and encrypt them again with assistance from r, iv1, and iv2. Bob would then execute Professor Pedantic's authentication scheme, see that the decrypted messages match, and assume that the message did indeed come from Alice. If he instead used a scheme that employed a function with deterministic mappings from a plaintext message space to an output space (i.e. a hash function *on the message*), he could then attach that function's output to the encrypted messages to provide authenticity. Then, if they were altered by an adversary with knowledge of k1 and k2, Bob would detect the spoofed messages after seeing that the hash function's output from the received message does not match the attached output from the original message.