CSC474 Fall 2023 - Homework 1*

Due Fri Sep 22, 2023, 11:59pm ET

Prof. William Enck

1 Perfect Secrecy {20 points}

(a) {10 points} A cryptosystem that offers *perfect secrecy* prevents an eavesdropper who observes an encrypted transmission from learning anything about the plaintext, other than its size.

Show with a counterexample that the Substitution Cipher doesn't provide perfect secrecy.

(b) {10 points} Consider the following modification to one-time pad (OTP) encryption. Rather than share a single one-time pad, Alice and Bob have shared knowledge of two pads, P_1 and P_2.

Given a plaintext M, Alice creates the ciphertext $C = M \oplus P_1 \oplus P_2$, where $\oplus$ denotes xor and $|M| = |P_1| = |P_2|$ (i.e., the size of the message and the two pads are all equal). To decrypt, Bob takes the ciphertext and xors it with P_1 and P_2; i.e., $D(C) = C \oplus P_1 \oplus P_2$.

Argue that if a one-time pad offers perfect secrecy, then the above scheme must also be perfectly secure.

2 Modes of Operation {10 points}

Prof. Pedantic, the esteemed Ineptitude Professor of Computer Science and Quackery at Wikipedia University, is developing a new terminal program (and associated service) to log into the servers in his lab. Although he is aware of `ssh`, he refuses to use it because he doesn't like being hushed.[1] Instead, he decides to construct his own novel protocol. Like `telnet` and `ssh`, his remote console/terminal program should allow a remote user to type commands and execute them on a remote machine. Since Prof. Pedantic doesn't trust anyone — particularly the students in his network security class — he decides that all communication should be encrypted.

Prof. Pedantic decides to use the AES encryption algorithm in ECB mode. Is this a good choice? Give **two** reasons why or why not.

*Last revised on August 27, 2023.

[1] Extra credit {0.0000001 points}: Explain that joke.

3 Reasoning about Confidentiality and Authenticity {10 points}

Prof. Pedantic designed a "secure" communication protocol for two parties (Alice and Bob) that have preshared secrets k_1 (the confidentiality key) and k_2 (the authenticity key).

Prof. Pedantic doesn't believe in traditional MACs, so he constructs his protocol as follows: to send a message m, Alice (A) sends to Bob (B) the following:

$$\begin{aligned} A \rightarrow B : \langle \quad & r, \\ & \mathrm{iv}_1, \\ & \mathrm{iv}_2, \\ & \mathrm{RC4}_{H(\mathrm{iv}_1|k_1)}(r, m), \\ & \mathrm{RC4}_{H(\mathrm{iv}_2|k_2)}(r, m) \quad \rangle \end{aligned}$$

where r is a nonce (to prevent replay attacks), iv_1 and iv_2 are fresh initialization vectors (IVs), $\mathrm{RC4}_k(r, m)$ denotes the encryption of message m using RC4 (a stream cipher) with key k and nonce r, and $H(x|y)$ is the SHA-256 hash of x concatenated with y. (Note that RC4 does not natively accept an IV; hence, Prof. Pedantic embeds the IV into the effective encryption/decryption key using the hash function.)

The professor claims that the protocol achieves *confidentiality* and *authenticity*, **as defined as follows**:

- *confidentiality:* an eavesdropper that observes a run of the protocol cannot learn the message m unless it knows the confidentiality key k_1 (you should also assume k_2 is not known to the eavesdropper); and
- *authenticity:* if Bob receives $\langle r, \mathrm{iv}_1, \mathrm{iv}_2, \mathrm{RC4}_{H(\mathrm{iv}_1|k_1)}(r, m), \mathrm{RC4}_{H(\mathrm{iv}_2|k_2)}(r, m)\rangle$ and r is a fresh nonce and the decryption of $\mathrm{RC4}_{H(\mathrm{iv}_1|k_1)}(r, m)$ equals the decryption of $\mathrm{RC4}_{H(\mathrm{iv}_2|k_2)}(r, m)$ (using the corresponding IVs and keys), then message m must have been transmitted by a party that knows both the confidentiality and authenticity keys (i.e., k_1 and k_2).

The professor's intention is that Bob obtains m by decrypting $\mathrm{RC4}_{H(\mathrm{iv}_1|k_1)}(r, m)$ using key k_1 and iv_1. Further, Bob performs an authenticity check by ensuring that the decrypted message matches the decryption of $\mathrm{RC4}_{H(\mathrm{iv}_2|k_2)}(r, m)$ (via key k_2 and IV iv_2). He reasons that only a sender that knows *both* k_1 and k_2 can cause the decryptions to match.

Does Prof. Pedantic's scheme achieve confidentiality and/or authenticity, as defined above? Briefly argue why or why not, for both confidentiality and authenticity. **Consider these two properties *independently* of one another**. That is, when considering authenticity, assume the adversary knows the message and is attempting to forge a message. Also, assume that k_1 and k_2 are random 128-bit keys that have been securely shared apriori between Alice and Bob, that $k_1 \neq k_2$, and that the two IVs are also fresh.

4 Key Sharing, The Pedantic Way {15 points}

At a recent conference, Prof. Pedantic met a potential collaborator, Prof. Feckless. Over drinks, Prof. Pedantic and Feckless outlined a new super-secret research project that they would collaborate

on throughout the year. Due to the nature of the work, both professors agreed that any future email between the two parties should be encrypted.

(a) {7 points} Suppose that during their encounter, Prof. Pedantic and Feckless securely exchanged a random, 16 bit key, k_{16}. Later, back at their respective institutions, they realize that 16 bits is too small. They decide to use the short key to communicate a longer secret, chosen by Prof. Pedantic, as follows:

$$\text{Prof. Pedantic} \rightarrow \text{Feckless} : E_{k_{16}}(k_{256}, \text{MAC}_{k_{16}}(k_{256}))$$

They then communicate using the 256 bit key k_{256} as follows:

$$\text{Prof. Pedantic} \leftrightarrow \text{Feckless} : E_{k_{256}}(M, \text{MAC}_{k_{256}}(M))$$

What is the flaw in the two professors' logic?

(b) {8 points} Suppose that the two professors each share a (separate) key with a trusted mutual friend, Dean Bureaucracy. With Dean B's help, can they now securely exchange a key such that an external eavesdropper (i.e., anyone who is not the professors or the Dean) cannot learn it? If so, how? If not, why not? You can assume that Dean B is honest.

5 Written questions - Key Sharing, Done Right {15 points}

Assume Alice, Bob, and Charlie are all honest, and that Alice and Bob want to share a key – potentially in the presence of a malicious, active adversary. Further assume that Alice and Charlie share a symmetric key $k_{a,c}$, and that Bob and Charlie share a symmetric key $k_{b,c}$. Charlie's public key, k_c^+, is known a priori by all parties.

Revise the Diffie-Hellman (DH) protocol such that (i) Alice and Bob can share a symmetric key $k_{a,b}$ and (ii) the exchange is not vulnerable to a man-in-the-middle attack. Your solution must utilize DH as its core mechanism, and should not allow Charlie to learn (without misbehaving) the shared key between Alice and Bob. That is, your protocol should work against an active eavesdropper (who is not Alice, Bob, or Charlie) and should ensure that only Alice and Bob know the key $k_{a,b}$ even if Charlie is "honest-but-curious".

6 RSA {30 points}

(a) {5 points} Prof. Pedantic generates an RSA keypair, consisting of a public key $\langle e, n\rangle$ and a private key $\langle d, n\rangle$. He saves the large (2048-bit) prime factors p and q used to compute n (i.e., $n = pq$) as well as his public key $\langle e, n\rangle$. Ever forgetful, he forgets to save his private key $\langle d, n\rangle$. D'oh! Will Prof. Pedantic be able to recover and re-generate his private key? That is, can he learn d given the information that he recorded? Why or why not?

(b) {10 points} Prof. Pedantic decides to create a variant of RSA, which he calls RASP (the P is for Pedantic). In RASP, the private key exponent d is computed as $d = e^{-1} \bmod n$ (the modular inverse of the public key exponent e, modulo n), as opposed to $d = e^{-1} \bmod \Phi(n)$.

The encryption and decryption functions also differ between RSA and RASP, but knowing what these functions are isn't important for this question.

What **major** security flaw does RASP's key generation algorithm introduce?[2]

(c) {5 points} Prof. Pedantic gives you (securely) his RSA public key:

$$K^+ = \langle e = 13, n = 77 \rangle$$

What is the corresponding ciphertext for the plaintext message $M = 2$, encrypted with Prof. Pedantic's public key? Show your work.

(d) {5 points} Given his public key $\langle e = 13, n = 77 \rangle$, what is Prof. Pedantic's private key?

(e) {5 points} Why were you able to answer the previous question?!? That is, is RSA broken? If it isn't broken, then why were you able to derive his private key from his public key?

[2]Note that the notation $a = b^{-1} \bmod q$ is equivalent to $ab \bmod q = 1$. Both reflect the fact that a and b are modular inverses under modulo q.