CSCI 445 - Homework 2*

Assigned February 8th; Due 11:59pm on February 22nd

Prof. Adwait Nadkarni

Note: This homework assignment is worth 50 points.

1 Symmetric Crypto and Key sharing {50 points}

(a) {5 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.

(b) {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.

(c) {20 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

*Last revised on February 8, 2024.

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

send a message m, Alice (A) sends to Bob (B) the following:

$$A \to B : \langle \begin{array}{l} r, \\ \mathrm{iv}_1, \\ \mathrm{iv}_2, \\ \mathrm{RC4}_{H(\mathrm{iv}_1|k_1)}(r, m), \\ \mathrm{RC4}_{H(\mathrm{iv}_2|k_2)}(r, m) \end{array} \rangle$$

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 they know the confidentiality key k_1; 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 each property separately (that is, when considering authenticity for a message, you can assume the adversary knows the message). 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.

(d) 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:

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

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.

Submission Instructions

Submit your solution as a single PDF using Blackboard. To upload your assignment, navigate to the "Mobile App Security (Spring 2024)" course. Use the "Homework 2" assignment.

Writeups submitted in Word, ASCII, PowerPoint, Corel, RTF, Pages, and other non-PDF formats will not be accepted. Consider using LaTeX to format your homework solutions. (For a good primer on LaTeX, see the Not So Short Introduction to LATEX.)

Note that you may submit a PDF scan of hand a hand written solution; however, you will receive **0 points** if the instructor cannot read your hand writing. If the instructor has any difficulty reading your hand writing, you may not submit hand written solutions for future assignments.

Please post questions (especially requests for clarification) about this homework to Piazza.