CSC474 Fall 2022 - Homework 1 Written Question*

Prof. William Enck

1 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

*Last revised on August 29, 2022.

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.