CS 198 Spring 2023 — Codebreaking at Cal Makeup Assignment — Week 7

Question 1

Alice wants to send a message M to Bob and sign it with an RSA signature. Mallory has the ability to read and modify Alice's messages. Alice doesn't care if Mallory can read her message, but she needs Bob to know if the message was tampered with.

Alice decides to use $(p,q) = (5,11)$ and $e = 3$ to generate her keypair. She finds $N = 55$, and computes $d = 27$.

1. Alice wants to send $M = 4$ to Bob. What signature S does she send along with M?
2. When Bob receives (S,M), how does he verify that the message was not modified?
3. Unfortunately, Alice did not use the version of RSA signatures with hashing, so Mallory can come up with a message M' and corresponding signature S' that Bob verifies. Find an example of such an M' and S'.
4. Alice now sends a signature on $H(M)$ instead of M, where H is some cryptographic hash function. Prove that Mallory can no longer find an (M',S') pair that Bob verifies unless she can break the hash function.

Question 2

Alice is trying to send a message M to Bob, but Mallory can read or tamper with the message. Both Alice and Bob have trusted public keys PK_A and PK_B, and they each have secret keys SK_A and SK_B respectively. They use the RSA encryption scheme and the RSA signature scheme without hashing; specifically, they have access to the following functions:

$$\begin{aligned}
&\text{Enc}(PK,M) = M^e \pmod N \\
&\text{Dec}(SK,C) = C^d \pmod N \\
&\text{Sign}(SK,M) = M^d \pmod N \\
&\text{Verify}(PK,S) = (S^e \stackrel{?}{=} M) \pmod N
\end{aligned}$$

They also have access to H, a cryptographic hash function.

1. Suppose Alice sends $\text{Enc}(PK_B,M)$ and $H(M)$. Can Mallory find out what M is? Can she modify it without being detected?

2. Now suppose Alice sends $\text{Enc}(PK_B, M)$ and $\text{Sign}(SK_A, M)$. Can Mallory learn what M is? Can she modify it without being detected?

3. (Optional) Design a scheme where Mallory can't find out what M is and can't modify it without being detected. You may change the Sign and Verify functions if needed.

(This was a modified version of a question from this semester's 161 midterm.)

Question 3

Given that signatures work and are asymmetric, why do we ever use MACs, which require a symmetric key?

Contributors:

- Ryan Cottone, Will Giorza