CSE 107 Discussion 3/6

Activity 1: Recall that a digital signature scheme is like a MAC that can be publicly verified: instead of the sender and receiver using the same key, the sender (signer) uses a secret key sk to sign a message, and the receiver (verifier) uses a corresponding public key pk to verify that the signature is valid. To verify a MAC, you just recompute the tag $\text{Tag}_K(M)$ and check that the tag you received is correct; to verify a signature, you use a separate algorithm $\text{Verify}(pk, M, sig)$ to check whether the given signature is valid.

1. Why does there need to be a separate Verify algorithm?
2. Can you think of any cases in the real world where you would want a digital signature instead of a MAC?

Activity 2: ElGamal signatures

The ElGamal signature scheme was invented in 1985 and operates as follows. It has public parameters including a prime p, hash function H, and generator g of $\mathbf{Z}_p^*$.

KeyGen :
$x \xleftarrow{\$} \{1, 2, \ldots, (p-2)\}$ (so $x \in \mathbf{Z}_{p-1}$ but is not allowed to be zero)
$X \leftarrow g^x \bmod p$
Return signing key x and verification key X

$\mathsf{Sign}(x, M)$:
Choose $k \xleftarrow{\$} \mathbf{Z}_{p-1}^*$
$r \leftarrow g^k \bmod p$
$s \leftarrow (H(M) - xr)k^{-1} \bmod (p-1)$
Return signature (r, s)

$\mathsf{Verify}(X, M, (r, s))$:
Return 1 iff $g^{H(M)} = X^r \cdot r^s \bmod p$

(a) Suppose you query to get $(r, s) \leftarrow \textbf{SignOracle}(M)$ and k happens to be chosen so that $k = 1$. How can you recover the secret key x?

(b) Suppose you query to get $(r_1, s_1) \leftarrow \textbf{SignOracle}(M_1)$ and $(r_2, s_2) \leftarrow \textbf{SignOracle}(M_2)$ and it happens to be the case that the same random value $k_1 = k_2 = k$ is chosen during each signature. How can you recover the secret key x?

Activity 3: RSA review

An RSA key consists of private values $p, q, \varphi(N), d \in \mathbf{Z}_{\varphi(N)}^*$ and public values N, e (where $N = pq$ and $ed = 1 \bmod \varphi(N)$). What happens if any of the private values leak?

(a) If q leaks, can you recover the remaining private values $p, \varphi(N), d \in \mathbf{Z}_{\varphi(N)}^*$?

(b) If $\varphi(N)$ leaks, which of the remaining private values can you recover?

(c) If d leaks, which of the remaining private values can you recover?