CMPT 404 — Cryptography and Protocols

Exercises on Public Key Cryptography.
Due: Thursday, April 5th (at the beginning of the class)

1. Prove the following: if there exists a collision resistant hash function collection mapping $n+1$ bit strings into n bits strings, then there exists a collection mapping arbitrary length bit strings into n bit strings.

2. Consider the following key exchange protocol:
   - Alice chooses $k, r \in \{0,1\}^n$ at random, and sends $s = k \oplus r$ to Bob.
   - Bob chooses $t \in \{0,1\}^n$ at random and sends $u = s \oplus t$ to Alice.
   - Alice computes $w = u \oplus r$ and sends w to Bob.
   - Alice takes k as a key, and Bob takes $w \oplus t$ as a key.

   Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e. either prove its security or show a concrete attack).

3. Suppose we have a set of blocks encrypted with the RSA scheme and we do not have the private key. Assume $n = pq$, e is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us to break the scheme?

4. Fix n, and assume there exists an adversary Eve running in time T for which

$$\Pr[\mathsf{Eve}(x^e) = x] = 0.01,$$

   where the probability is taken over random choice of $x \in \mathbb{Z}_n^*$. Show that it is possible to construct an adversary Eve' for which

$$\Pr[\mathsf{Eve}'(x^e) = x] = 0.99.$$

   The running time T' of the new adversary should be polynomial in T and the size of n.

5. (Non malleability of CCA secure schemes.) An attractive way to perform a bidding is the following: the seller publishes a public key e. Each buyer sends through the net the encryption $\mathsf{E}_e(x)$ of its bid, and then the seller will decrypt all of these and award the product to the highest bidder.

   One aspect of security we need from $\mathsf{E}(\cdot)$ is that given an encryption $\mathsf{E}_e(x)$, it will be hard for someone not knowing x to come up with $\mathsf{E}_e(1.01 \cdot x)$ (otherwise bidder B could always take the bid of bidder A and make into a bid that is one per cent higher). You'll show that this property is also related to CCA security:

   (a) Show a CPA-secure public key encryption such that there is an algorithm that given e and a ciphertext $y = \mathsf{E}_e(x)$, converts y into a ciphertext y' that decrypts to $x + 1$.

   (b) Show that if E is CCA secure then there is no such algorithm. In particular show that if M is any polynomial time algorithm, and X is a set of possible numbers x, then

$$\Pr_{(e,d)\leftarrow K}[\mathsf{D}_d(M(e, \mathsf{E}_e(x))) = 1.01 \cdot x] < \tfrac{1}{|X|} + n^{-\omega(1)}$$

6. Let $p \geq 3$ be a prime number, and let g be a primitive root modulo p. (These are public keys, known to all parties including the adversary.) Assume the discrete logarithm problem is hard. Consider the digital signature scheme $DS = (K; \mathsf{Sign}; \mathsf{Ver})$:

   Key generation K: Choose $x, y \in \mathbb{Z}_p$ uniformly at random, and set $X = g^x$, $Y = g^y$.
   X, Y is a public key, x, y private.

   Signing $\mathsf{Sign}(M)$:
   $z := y + xM \pmod{p}$,
   return z.

   Verification $\mathsf{Ver}(M; z)$:
   if $M \notin \mathbb{Z}_p$ **then return** 0
   if $g^z = YX^M$ **then return** 1
   else return 0

   (a) Show that $\mathsf{Ver}(M; z) = 1$ for any key-pair $((X; Y); (x; y))$ that might be output by K, any message $M \in \mathbb{Z}_p$, and any z that might be output by $\mathsf{Sign}(M)$.

   (b) Show that this scheme is insecure with regard to Chosen Message attacks by presenting a practical adversary Eve. You should specify the adversary, state the number of oracle queries it makes, and justify the correctness of the adversary.

7. Let f be a one-way permutation. Consider the following signature scheme for messages in the set $\{1, \ldots, n\}$:
   - To generate keys, choose random $x \in \{0,1\}^n$ and set $y = f^n(x)$ (that is, f applied n times). The public key is y and the private key is x.
   - To sign message $i \in \{1, \ldots, n\}$, output $f^{n-i}(x)$ (where $f^0(x) = x$ by definition).
   - To verify signature σ on message i with respect to public key y, check whether $y = f^i(\sigma)$.

   (a) Show that the above is not a secure (even one-time) signature scheme. Given a signature on a message i, for what messages j can an adversary output a forgery?

   (b) Prove that no polytime adversary, given a signature on i can output a forgery on any message $j > i$ except with negligible probability

   (c) Suggest how to modify the scheme so as to obtain a one-time secure signature scheme.

8. *(optional)* Write an implementation (using pseudocode or your favorite programming language) of the 'ideal' key exchange protocol. This implementation should include all necessary details and checks of parameters. It can be based on Diffie-Hellman idea, as we did in the class, or any other valid approach. If you need to use a hash function or primality check, imaging you have a library with necessary functions. You also do not need to care about realization of integer arithmetic.