Homework 7: Signatures

Submission policy. Submit your answers on Blackboard by 11:59pm Friday, **Dec. 3**, 2021. Your submission should include a .PDF file with all the answers to the theoretical problems. You should try to typeset your homeworks. Latex is especially recommended. No late submissions will be accepted. Your writeup MUST include the following information:

1. Your name and whether you take the class at **487** or **587** level.
2. List of references used (online material, course nodes, textbooks, wikipedia, etc.)

The homework will be graded by the class TA Anuj Pokhrel (apokhre@gmu.edu).

Exercise 1. Modular Construction [20 points] Assume a secure signature scheme for messages of size k-bits. Let $\sigma(m)$ denote a signature on message m (we omit the secret key to simplify notation). Consider the following constructions for messages $|M| > k$:

- To sign a message $M = m_1 \parallel m_2 \parallel ... \parallel m_n$, where $\parallel$ denotes concatenation and each $|m_i| = k-$ bits (assume no need for padding and that M can be conveniently broken into m_i blocks), output

$$\Sigma(M) = \sigma(m_1), \sigma(m_2), \ldots, \sigma(m_n)$$

  where all $\sigma(m_i)$'s are signed under the same secret key.

- To sign a message $M = m_1 \parallel m_2 \parallel ... \parallel m_n$, output

$$\Sigma(M) = \sigma(1 \parallel m_1), \sigma(2 \parallel m_2), \ldots, \sigma(n \parallel m_n)$$

  where all $\sigma(m_i)$'s are signed under the same secret key. (Assume sizes of messages work out, i.e. concatenation of index i with m_i add up to k bits.

For both schemes explain why they do not satisfy existential unforgeability as defined in class.

Exercise 2. Weaker Definition [40 points] In class we described the "plain RSA" signature scheme and we explained why it cannot be proved unforgeable. In this exercise, we will prove plain RSA signature secure under a different (weaker) definition of security.

Consider an adversary who is given the RSA public key (N, e) and a message $m \in \mathbb{Z}_N^*$ selected *uniformly at random* by the challenger. The adversary wins if it outputs a valid signature on m *without* making any signing queries.

Prove (via a reduction), why the plain RSA signature satisfies the definition above.

Exercise 3. RSA Signature Scheme [40 points] In class we discussed the RSA digital signature scheme where the message needs to be hashed before its signature is computed. Alice and Bob exchange signed messages. For the next round Alice suggests that instead of hashing the message first she will use some version of (non-cryptographic) encoding function f such that $f : \{0,1\}^\ell \to \mathbb{Z}_n^*$ and sign $f(m)$ instead of $H(m)$.

1. (5 points) What are the steps that Bob needs to follow in order to verify a signature-message pair coming from Alice (assuming of course he knows Alice's public key)?

2. (20 points) Explain why the scheme is insecure if f is defined to be $f(m) = 0||m||0^{\ell/10}$, and ℓ is the size of RSA modulus N in bits. (Hint: start by arguing why $0||m||0^{\ell/10} = m2^{\ell/10} \bmod N$ and then show how an adversary can construct a forgery.)

3. (10 points) In class we saw a definition of existential unforgeability for digital signatures. An alternative definition is that of a *target-message*: an adversary who attempts a forgery on a specific message. Write down the formal definition for target-message signature unforgeability (i.e. describe the game between adversary and challenger, say what it means for the adversary to win and state the definition of when a signature scheme is target-message unforgeable.)

4. (5 points) Is a scheme that is target-message unforgeable more or less secure than an existential unforgeable one? Why?

Exercise 4. Only if in 587 [20 points] (Continue from previous exercise) We now describe a new signature scheme. We assume that the public key of the signer is a Blum integer $n = pq$ (a Blum integer has the property that -1 is a non-square mod p and mod q). The secret key is n's factorization. The message space is $\mathrm{QR}_n \cup \mathrm{QNR}_n$ (look at textbook Section 13.4.1 to understand this group). A signature σ on message m is computed as follows: if m is a quadratic residue, then σ is some arbitrary square root of m. Otherwise, σ is some arbitrary square root of $-m$.

Prove that this scheme is target-message unforgeable if the adversary is only given the public-key (i.e. does *not* have access to the signer - only its public key). For your proof you need to give a reduction showing that if an adversary A can break target-message unforgeability knowing only the public key then we can build an algorithm B that breaks factoring.