Modern Cryptography Jan 31, 2019

Solutions to Final Exam

Lecturer: Daniel Slamanig, TA: Karen Klein

Put your name and student ID (if applicable) on every sheet that you hand in. Leave space in the top left corner of every sheet to allow for stapling. Any permanent pen is allowed, but text written in erasable pens (e.g. pencils) will not be considered during grading.

1. (12 points)

True or False

(a) Let p be prime, then $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$.

(b) The Fermat primality test on input candiate integer n picks $a \xleftarrow{\$} \{1, \ldots n-1\}$ and if $a^{n-1} \neq 1 \bmod n$ outputs "composite" and "prime" otherwise. If the input n is prime, then the algorithm will err with a certain probability.

(c) Textbook RSA encryption is OW-CPA secure under the Factoring assumption.

(d) If the message space of a public key encryption scheme is large enough, even a deterministic scheme can be $\mathsf{IND\text{-}CPA}$ secure.

(e) Every $\mathsf{IND\text{-}CCA}$ secure public key encryption scheme is also $\mathsf{IND\text{-}CPA}$ secure.

(f) The hash-and-sign paradigm is used to extend signature schemes to support arbitrarily long messages.

2. (15 points)

(a) Specify the algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ for ElGamal encryption with respect to group parameters (G, q, g), where G is a group of prime order q generated by g.

(b) Suppose that you use exponential ElGamal where the message m is represented as $m \in \mathbb{Z}_q$ and you encrypt g^m with the ElGamal scheme from above. Show that when you intercept a ciphertext of this scheme that encrypts an unknown message $m \in \mathbb{Z}_q$, you can change the message to $m' = 10 \cdot m$ without decrypting. What does this say about the CCA security of ElGamal (explain in one to two sentences)?

3. (10 points)

Write down the $\mathsf{OW\text{-}CPA}$ and the $\mathsf{IND\text{-}CPA}$ experiments for public key encryption. Show, by providing an explicit reduction, that $\mathsf{IND\text{-}CPA}$ security implies $\mathsf{OW\text{-}CPA}$ security.

4. (10 points)

Consider the following variant of the Schnorr signature scheme. Let $\mathsf{pp} := (G, q, g) \leftarrow \mathcal{G}(1^n)$ be public group parameters that are the description of a cyclic group G of prime order q

and a generator g. These parameters pp are implict input to the Sign and Vrfy algorithms. Furthermore, we fix hash functions $H_1 : \{0,1\}^* \to \mathbb{Z}_q$ and $H_2 : \mathbb{Z}_q \to \mathbb{Z}_q$.

Gen: on input pp, choose $x, z \overset{\$}{\leftarrow} \mathbb{Z}_q$, compute $y := g^x$, $w := x+z \bmod q$ and output the public and private key $(\mathsf{pk}, \mathsf{sk}) := ((y, w), (x, z))$.

Sign: on input a secret key $\mathsf{sk} = (x, z)$ and a message $m \in \{0,1\}^*$, compute $k := H_2(z)$, $I := g^k$, $r := H_1(I, m)$ and $s := rx + k \bmod q$. Output the signature $\sigma := (r, s)$.

Vrfy: on input a public key $\mathsf{pk} = (y, w)$ a message $m \in \{0,1\}^*$, a signature $\sigma = (r, s)$, compute $I := g^s \cdot y^{-r}$ and output 1 if $H_1(I, m) = r$.

Construct an adversary that can recover the secret key (x, z) of the scheme given the public key pk and two valid message-signature pairs (m, σ) and (m', σ') with $m \neq m'$.

5. (10 points)

(a) What is the random oracle model (ROM)? Explain the term “programming” in context of random oracles and how is this technique used?

(b) The Diffie-Hellman key-exchange protocol only provides passive security (i.e., security in the presence of an eavesdropper). Which measures could be taken to obtain active security (i.e., counter man-in-the-middle attacks)? Would your so obtained version of the protocol intuitively also provide forward-secrecy? Forward-secrecy means that breaking into the server and receiving the server state does not allow to compute shared keys from previous sessions.