COS 496: Cryptography Due: Oct 2

Problem Set 1

Professor Amit Sahai

Please list everyone you collaborated with when solving the problems on this problem set. If you make use of outside material, make a note of that as well. Make sure you write up your solutions on your own.

Problem 1. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_k}$, where p_i are distinct *odd* primes and $\alpha_i > 0$. Let $y \in \mathbb{Z}_n^*$ be a quadratic residue.

1. Show that y has *exactly* 2^k distinct square roots (mod n).
2. Why did we require that none of the $p_i = 2$?

Problem 2. Suppose $SQRT(a, p)$ is a polynomial-time algorithm that, if p is prime and a is a quadratic residue $a \in Z_p^*$, outputs (w.h.p.) some square root of a mod p. (Note that such an algorithm does exist.)

1. Prove that the following algorithm is a primality test (i.e. that on a prime input outputs PRIME with high probability, and on a composite input outputs COMPOSITE with probability at least 1/2.)
   (a) If $n = 2$, output PRIME.
   (b) If n is even or of the form $n = p^b$ for some $p, b > 1$, output COMPOSITE.
   (c) Choose a random $r \in \{1, \ldots, n-1\}$. If $gcd(r, n) > 1$, output COMPOSITE.
   (d) Compute $x \leftarrow SQRT(r^2 \bmod n, n)$.
   (e) If $x = \pm r \bmod n$, output PRIME. Otherwise, output COMPOSITE.
2. Suppose $p = 4m + 3$ is a prime and that a is a quadratic residue modulo p. Prove that a^{m+1} is a square root of a modulo p.

Problem 3. In class, we saw the following definition of security for a public-key encryption scheme (G, E, D), which we call *indistinguishability-security*:

For all PPT M, A, there exists a negligible function $\alpha(k)$ such that for all sufficiently large k, when we consider the following experiment:

$$\begin{aligned} (PK, SK) &\leftarrow G(1^k) \\ (m_0, m_1, \sigma) &\leftarrow M(PK) \\ b &\leftarrow \{0, 1\} \\ c &\leftarrow E(m_b, PK) \\ b' &\leftarrow A(c, PK, \sigma) \end{aligned}$$

we have that $\Pr[b' = b] \leq \frac{1}{2} + \alpha(k)$.

- Prove that indistinguishability-security above implies the following definition, which we will call *tri-message indistinguishability*:

  For all PPT M, A, there exists a negligible function $\alpha(k)$ such that for all sufficiently large k, when we consider the following experiment:

$$\begin{array}{rcl} (PK, SK) & \leftarrow & G(1^k) \\ (m_0, m_1, m_2, \sigma) & \leftarrow & M(PK) \\ t & \leftarrow & \{0, 1, 2\} \\ c & \leftarrow & E(m_t, PK) \\ t' & \leftarrow & A(c, PK, \sigma) \end{array}$$

  we have that $\Pr[t' = t] \leq \frac{1}{3} + \alpha(k)$.

- Prove that indistinguishability-security above implies the following intuitive definition of security which we saw in class, which we will call *weak semantic security*:

  For all PPT A, M, there exists a PPT A' and a negligible function $\alpha(k)$ such that for all sufficiently large k, if we consider the following two experiments:

$$\begin{array}{rcl} \multicolumn{3}{l}{Expt_{RealLife}:} \\ (PK, SK) & \leftarrow & G(1^k) \\ m & \leftarrow & M(PK) \\ c & \leftarrow & E(m, PK) \\ x & \leftarrow & A(c, PK) \end{array}$$

  and

$$\begin{array}{rcl} \multicolumn{3}{l}{Expt_{IdealWorld}:} \\ (PK, SK) & \leftarrow & G(1^k) \\ m & \leftarrow & M(PK) \\ x & \leftarrow & A'(PK) \end{array}$$

  then we have that $\left| \Pr_{Expt_{RealLife}}[x = m] - \Pr_{Expt_{IdealWorld}}[x = m] \right| \leq \alpha(k)$.

  Hint: Recall that to prove this, you will need to construct both an A' for the weak semantic security definition **and** an adversary for the indistinguishability-security definition: You have to do this in a way that allows you to prove that the existence of a successful adversary A for weak semantic security implies that your constructed adversary for indistinguishability-security succeeds. (Thus, when you plug the definition of your adversary into the experiment in the definition of indistinguishability-security, it should closely resemble the experiments from the definition of weak semantic security.)

- Does tri-message indistinguishability imply standard indistinguishability-security?