CAS CS 538. Solutions to Problem Set 5

Due electronically via gradescope, Tuesday February 24, 2026 11:59pm

Om Khadka, U51801771

Problem 1. (50 points)
In Discussion 5 we introduced the Signal symmetric ratchet and we showed that even if a subsequent key is leaked to the adversary, it is hard to recover the previous key. In this problem, we will prove something stronger: even if a subseuqent key is leaked (and the previous key has been deleted), past encryptions are still semantically secure.

Specifically, let $\mathcal{E} = (\mathsf{Enc}, \mathsf{Dec})$ be a semantically secure cipher over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. Let $G : \mathcal{S} \to \mathcal{S} \times \mathcal{K}$ be a secure PRG such that $G : \{0,1\}^\ell \to \{0,1\}^{2\ell}$. Define the symmetric ratchet scheme as $\mathsf{Enc}^1(s, m) = \mathsf{Enc}(G(s)_2, m)$ and $\mathsf{Dec}^1(s, c) = \mathsf{Dec}(G(s)_2, c)$. Here $G(s)_2$ denotes the second part of the output of $G(s)$, i.e. the key part. We refer you to Figure 1 of Discussion 5 for a diagram of the symmetric ratchet.

At time step n, participants will advance the state of the ratchet by computing $(s_n, k_n) \twoheadleftarrow G(s_{n-1})$. Then, the past is erased by deleting the old seed s_{n-1} from memory. The new ciphertext is computed as $c_n = \mathsf{Enc}(k_n, m_n)$.

Prove that $\mathcal{E}^1$ is *semantically secure* for the previous encryption c_{n-1} even if a subsequent seed and key (s_n, k_n) is leaked to the adversary.

Getting started. To get started, you should consider an adversary $\mathcal{A}$ playing a new game called the SSKeyLeak game against $\mathcal{E}^1$. The SSKeyLeak is the same as the Semantic Security Game (Boneh + Shoup Attack Game 2.1) except that in addition to a ciphertext c_{n-1}, the adversary *also* receives a leaked seed and key (s_n, k_n) where s_n, k_n are pseudorandom values produced by G^n with an initial random seed.

In particular, say $\mathcal{A}$ outputs two messages m_0, m_1. Let Game 0 be when $c_{n-1} = \mathsf{Enc}^1(k_{n-1}, m_0)$ and Game 1 be when $c_{n-1} = \mathsf{Enc}(k_{n-1}, m_1)$. $\mathcal{A}$ receives the tuple (c_{n-1}, s_n, k_n) and outputs a bit $\hat{b}$. Let W_b be the event that $\hat{b} = 1$ in Game b of the SSKeyLeak game. Then we define the key-leakage advantage as SSKeyLeakadv$[\mathcal{A}, \mathcal{E}^1] = |\Pr[W_0] - \Pr[W_1]|$.

Building a hybrid argument. Use a hybrid argument to prove that $\mathcal{E}^1$ is semantically secure against leaked keys by showing that SSKeyLeakadv$[\mathcal{A}, \mathcal{E}^1]$ is negligible.

Hint: you will have to introduce two hybrid games in between Game 0 and Game 1 of SSKeyLeak game. Then you will give three reductions with wrapper adversaries $\mathcal{B}_1$, $\mathcal{B}_2$, and $\mathcal{B}_3$. In no particular order, two of these reductions yield a PRG distinguisher for G^n and one of them yields an SS adversary for $\mathcal{E}$.

Solution. Your solution goes here

Problem 2. (50 points at 10 each) Let $p > 2$ be an odd prime. For this problem, suppose the order of g is $p-1$ (which is even). Such a g is called a *generator* of $\mathbb{Z}_p^*$. Such a g exists for every p (we won't prove this fact; see, for example, Section 7.5 of Victor Shoup's book at http://www.shoup.net/ntb/ntb-v2.pdf for the existence proof and Section 11.1 for how to sample it efficiently).

(a) Let $a = g^x$ for some $x \in \mathbb{Z}_{p-1}$ (the exponent works modulo $p-1$ due to Fermat's little theorem). We can talk about the exponent x being even since $p-1$ is even, and therefore $x + k(p-1)$ has the same evenness as x for any $k \in \mathbb{Z}$.

Clearly if x is even, then a has a square root $g^{x/2}$ modulo p. Now show the converse: if a has a square root modulo p, then x is even. *(Hint: you can rewrite any element $b \in \mathbb{Z}_p^*$ as $b = g^y$ for some $y \in \mathbb{Z}_{p-1}$.)*

Solution. Your solution goes here

It'd be nice to check if a value is a square modulo p without having to explicitly know what power of g it is. Luckily we have the following test: a is a square iff $a^{(p-1)/2} \equiv_p 1$.

(b) Prove the forward direction: if a is square then $a^{(p-1)/2} \equiv_p 1$.

Solution. Your solution goes here

(c) Now prove the converse: if $a^{(p-1)/2} \equiv_p 1$, then a is square. *(Hint: Assume not and find a contradiction. Begin by writing a as g^x.)*

Solution. Your solution goes here

We have thus shown that exactly half the values in $\mathbb{Z}_p^*$ have square roots, and we know how to identify them: by raising to $(p-1)/2$. Note also that values that do have square roots have at least two of them: if $r \in \mathbb{Z}_p^*$ is a square root of $a \in \mathbb{Z}_p^*$, then so is $-r$, because $(-r)^2 = (-1) \cdot r \cdot (-1) \cdot r = (-1)(-1)r^2 = 1 \cdot r^2 = r^2$. The two square roots are different, because $p - r \neq r$ as p is odd. Therefore, each square cannot have more than two square roots by a simple counting argument: if some square had more than two square roots, there wouldn't be enough square roots for all the $(p-1)/2$ squares, because just two square roots per square already takes up all the $p-1$ possible square root values in $\mathbb{Z}_p^*$. Thus, each square has exactly two square roots.

(d) Show that if $(g^x)^2 \equiv_p a$, then $\left(g^{x+(p-1)/2}\right)^2 \equiv_p a$, as well. Show that these two square roots are distinct: that is, show that $g^x \not\equiv_p g^{x+(p-1)/2}$.

Solution. Your solution goes here

We know from the paragraph above that a has only two square roots. But we have three values that all when squared give us a: g^x, $g^{x+(p-1)/2}$, and $-g^x$. Thus, it must be that $g^{x+(p-1)/2} \equiv_p -g^x$.

(e) Given that $g^{x+(p-1)/2} \equiv_p -g^x$, show that that $g^{(p-1)/2} \equiv_p -1$. Now show that for any $b \in \mathbb{Z}_p^*$ that is a non-square, $b^{(p-1)/2} \equiv_p -1$.

This refines our previous test for squares from parts (b) and (c): to test if something is a square, you raise it to $(p-1)/2$ modulo p and check if the result is 1 or -1. By the way, the value of $a^{(p-1)/2} \,\%\, p$ is called the Legendre symbol of a and is often written as $\left(\frac{a}{p}\right)$. The Legendre symbol can be generalized for composite p and this generalization is called the Jacobi symbol (we will not cover it here).

Solution. Your solution goes here