Exercise Set 1

Prof. Kenny Paterson
Kien Tuong Truong

Problem 1 (Warm-up for Problem 5). Let p be a prime. For $a, b \in \mathbb{F}_p$, let

$$E_{a,b} = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

denote an elliptic curve over the field $\mathbb{F}_p$. Show that for *any* pair $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, there exists a choice of (a, b) such that (x, y) is a point on the curve $E_{a,b}$.

Problem 2 (Rejection Sampling). Let q be a k-bit integer. Suppose we have an oracle that when queried outputs uniformly random k-bit outputs. Describe a simple procedure that samples an integer uniformly at random from $\{1, \ldots, q-1\}$ using the given oracle. Give an evaluation of how many oracles calls are needed on average by your procedure. What is its worst-case performance?

Problem 3 (Known Nonces). Show that an attacker who learns the nonce value k corresponding to an ECDSA signature (r, s) for a known message m can efficiently recover the secret signing key x. (Hint: recall that in ECDSA, $s = k^{-1}(h + xr) \bmod q$ where h is derived from the message.)

Problem 4 (Repeated Nonces). Suppose that a signer manages to prevent the aforementioned attack by making sure that the nonce is concealed from the attacker. However, due to a bug in the implementation, a nonce value gets repeated after every 10 signatures.

- Suppose an attacker sees two signatures (r_1, s_1) and (r_2, s_2). Argue that the attacker can trivially detect if a nonce k has been repeated across these two signatures.
- Now suppose that these two signatures (r_1, s_1) and (r_2, s_2) generated using the same nonce k correspond to messages m_1 and m_2, respectively, such that $m_1 \neq m_2$. Show that the attacker can recover the secret signing key x.

Problem 5 (Invalid Curve Attacks). Recall the formulae for point addition and doubling from slide 13 of the lecture. What do you notice about the dependence of these formulae on the values a and b? What might the potential security consequences of this be when using ECDHE (as per slide 23)? (Hint: what if Alice chooses what she sends to Bob in an adversarial manner, such that Alice's point is not of the expected form $[x]P$ but is actually a point on another curve altogether?)