Introduction to Cryptography  
Problem Set 5  
Due: Thursday, March 11

1. Suppose we have an encryption scheme, where the encryption function is $E$, and a message authentication code (MAC), where the keyed function $f$ is used to produce a tag. If we want to simultaneously encrypt and authenticate a plaintext $P$, we could do so in one of two ways:

- Compute $C = E_k(P)$ and $t = f_{k'}(C)$; the encrypted-authenticated message is the pair $(C, t)$.
- Compute $C = E_k(P)$ and $t = f_{k'}(P)$; again, the encrypted-authenticated message is the pair $(C, t)$.

Comment on the relative security of these two approaches, assuming the encryption scheme is secure against chosen plaintext attack, and that $f$ is a secure MAC.

2. In class, we discussed the use of the keyed function $f_{a,b}(x) = ax + b$, where $a, b, x \in \mathbb{Z}_p$ (and $p$ is prime) as a “one-time secure” MAC, i.e., secure against an adversary who queries the $f$-oracle only once before attempting to forge a tag. Design and analyze a “two-time secure” MAC, i.e., secure against an adversary who queries the $f$-oracle at most twice before attempting to forge a tag.

3. Define the keyed function $f_a(x) = ax + a^2$, where $a, x \in \mathbb{Z}_p$. Prove or disprove: $f$ is a “one-time secure” MAC.