ECS 227 — Modern Cryptography — Winter 99
Problems 10–12

Phillip Rogaway
Out: 11 February 1999. Due: 25 February 1999.

10. Let $\mathrm{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme and let $\mathrm{MA} = (\mathcal{K}', \mathrm{MACG}, \mathrm{MACV})$ be a message authentication code. Alice (A) and Bob (B) share a secret key $K = (K1, K2)$ where $K1 \leftarrow \mathcal{K}$ and $K2 \leftarrow \mathcal{K}'$. Alice wants to send messages to Bob in a private and authenticated way. Consider her sending each of the following as a means to this end. For each, say whether it is a secure way or not, and briefly justify your answer. (In the cases where the method is good, you don't have to give a proof, just the intuition.)

(a) $M, \mathrm{MACG}_{K2}(\mathcal{E}_{K1}(M))$

(b) $\mathcal{E}_{K1}(M, \mathrm{MACG}_{K2}(M))$

(c) $\mathrm{MACG}_{K2}(\mathcal{E}_{K1}(M))$

(d) $\mathcal{E}_{K1}(M), \mathrm{MACG}_{K2}(M)$

(e) $\mathcal{E}_{K1}(M), \mathcal{E}_{K1}(\mathrm{MACG}_{K2}(M))$

(f) $C, \mathrm{MACG}_{K2}(C)$ where $C = \mathcal{E}_{K1}(M)$

(g) $\mathcal{E}_{K1}(M, A)$ where A encodes the identity of Alice; B decrypts the received ciphertext C and checks that the second half of the plaintext is "A".

In analyzing these schemes, you should assume that the primitives have the properties guaranteed by their definitions, but no more; for an option to be good it must work for *any* choice of a secure encryption scheme and a secure message authentication scheme.

Now, out of all the ways you deemed secure, suppose you had to choose one to implement for a network security application. Taking performance issues into account, do all the schemes look pretty much the same, or is there one you would prefer?

11. Consider strengthening the definition of a message authentication code: after having asked the sequence of messages $M_1, \ldots, M_q$, obtaining MACs $\sigma_1, \ldots, \sigma_q$, the adversary is said to succeed if she outputs a pair (M_*, σ_*) for which $\mathrm{MACV}_a(M_*) = \sigma_*$ but $(M_*, \sigma_*) \neq (M_i, \sigma_i)$ but $(M_*, \sigma_*) \notin \{(M_1, \sigma_1), \ldots, (M_q, \sigma_q)\}$. Call a MAC which resists attacks in this sense *strongly* secure.

(a) Assume you have a good MAC scheme $\Pi = (\mathcal{K}, \mathrm{MACG}, \mathrm{MACV})$. Construct a MAC $\Pi' = (K', \mathrm{MACG}, \mathrm{MACV})$ which is secure (in the ordinary sense) but not strongly secure.

(b) Consider our Wegman-Carter construction, WC[H, F]. We showed that it yields a secure MAC when F is a good PRF and H is an ϵ-AU hash family for some small ϵ. Under the same assumptions, does this construction yield a MAC which is strongly secure?

Your argument should be based on a general observation, not on the specifics of the WC construction.

(c) Can you think of an application where the stronger definition of security is worthwhile?

12. Consider the following variant of the WC[H, F], which we denote UMAC[H, F]. You have a PRF $F : \{0,1\}^\alpha \times \{0,1\}^* \to \{0,1\}^\beta$ and an ϵ-AU family of hash functions H. The key generation algorithm returns a pair (a, h), for $a \leftarrow \{0,1\}^\alpha$ and $h \leftarrow \mathsf{H}$. Now to authenticate message M return $(\text{cnt}, F_a(\text{cnt} \parallel h(M))$, where cnt is an integer counter, initially 0, and it is implicitly encoded into an 8-byte string. After generating that MAC, increment cnt by 1. If cnt ever reaches 2^{64}, return $\perp$ if asked to encrypt any further message. MAC verification works in the obvious way.

Prove the security of the UMAC[H, F] construction.