ECS 227: Modern Cryptography
Homework 3

Phillip Rogaway

Out: Tuesday, 7 November 1996. Due: Tuesday, 26 February 1996

7. I give you a coin of some unknown bias, p. You want to estimate p. Develop and analyze the running time of an algorithm $A(\epsilon, \delta)$ which does this. Your algorithm returns an estimate p^* which is within ϵ of p a fraction $1 - \delta$ of the time.

8. Suppose I give you an oracle I that takes an input (N, e, y), and has the following behavior: for every N which is the product of two distinct primes, for every $e \in \mathsf{Z}^*_{\varphi(N)}$, for 1% of the values $y \in \mathsf{Z}^*_N$, the oracle I finds an $x \in \mathsf{Z}^*_N$ such that $x^e \bmod N = y$. Use I to develop an efficient algorithm A that has the following behavior: for every N which is the product of two distinct primes, for every $e \in \mathsf{Z}^*_{\varphi(N)}$, for 99% of the values $y \in \mathsf{Z}^*_N$, the oracle I finds an $x \in \mathsf{Z}^*_N$ such that $x^e \bmod N = y$. Count how many calls to I your algorithm requires. *Hint: "randomize" the points you work on.*

9. Let $\Pi = (\mathcal{E}, \mathcal{D}, \mathcal{K})$ be a secure encryption scheme and $\mathcal{M} = (\mathrm{MAC}, \mathrm{MACV})$ a secure message authentication scheme. Two parties Alice (A) and Bob (B) share a pair of secret keys (K_1, K_2). They want to send messages to each other in a private and authenticated way. Consider 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 it seems good, you don't have to give a proof, just some intuition.)

- **(a)** $M, \mathrm{MAC}_{K_2}(\mathcal{E}_{K_1}(M))$
- **(b)** $\mathcal{E}_{K_1}(M, \mathrm{MAC}_{K_2}(M))$
- **(c)** $\mathrm{MAC}_{K_2}(\mathcal{E}_{K_1}(M))$
- **(d)** $\mathcal{E}_{K_1}(M), \mathrm{MAC}_{K_2}(M)$
- **(e)** $\mathcal{E}_{K_1}(M), \mathcal{E}_{K_1}(\mathrm{MAC}_{K_2}(M))$

(f) $C, \mathrm{MAC}_{K_2}(C)$ where $C = \mathcal{E}_{K_1}(M)$

(g) $\mathcal{E}_{K_1}(M, A)$ 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. That is, Π is a secure encryption scheme but has no property that does not follow from this; analogously for the message authentication scheme. 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?