Assignment 2

Course: CS219cr Fall 99

November 3, 1999

Problem 1 We have seen in class how to get a hash function out of a compression function by the trick $G_i = f(G_{i-1}||x_i)$. This is good when we get x as a stream, but no good when x sits in shared memory of a multiprocessor when we can potentially work on different segments of x in parallel. Design such a method and prove it strongly collision free is the compression function is such.

Problem 2 In the "serial" method of converting a compression function to a hash function, we encountered a problem when the compression function compresses just by a single bit. Then we show a scheme the "blows-up" x by a factor of 2. Design a scheme for such a "problematic" compression function whose efficiency on the average (the blow-up factor) will not be worse than the method we have seen in class.

In general. Can we make the case that the problem of hash function from compression function is no different than the communication problem of identifying when an old msg ends and a new starts? Try to write something about it. Not that I know any clear-cut answer.

Problem 3 Suppose we both share a secret key K, but all we care about when I receive a message from you is to know that you sent the message rather than prevent others from reading it. One way to accomplish such goal is to add to the message M a short string $MAC(M,K)$ (MAC= Message Authentication Code) that "intermingles" the secret and the message is such a way the we are assured that only somebody who knows K could have produced the pair $(M,\ MAC(M,K))$.

Show that the proposition of $MAC(M,K) = h(K||M)$ where h is a hash function that is constructed in the "serial" method we have seen in class is insecure (i.e. I can construct a MAC to a message for which I have not seen a MAC given that I can get a hold of the MAC machine for few messages).

Show that same holds for $MAC(M,K) = h(M||K)$ (This is a bit more complex and here you have to argue that if the range of h is 2^b, then in expected time $2^{b/2}$ you can get a forgery. It uses the "birthday paradox" which say that on the average you need 23 people to get a pair whose birthday fall on the same date).

Argue that the *envelope* method is secure $MAC(M,K) = h(K||p||H||K)$, where p is to pad K to length of one block for the compression function to operate on.

Argue that $HMAC$ method is secure $HMA(M,k) = H(K||p_1||h(K||p_2||M)$, where $p_1,\ p_2$ are distinct strings of sufficient length to pad K to full block.

(The last two are hard, so handwaving is acceptable:-)).

Problem 4 Why will the security of the El-Gamal signature be compromised if γ is not verified to be less than $p-1$?