YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467b: Cryptography and Computer Security *Handout #15 (vers. 2)*
Professor M. J. Fischer *March 28, 2005*

Problem Set 5

Due in class on Tuesday, April 5, 2005.

Problem 15: Authenticated Broadcasting

User A is broadcasting packets to n recipients $B_1, ..., B_n$. Privacy is not important but integrity is. Each of $B_1, ..., B_n$ wants to be assured that the packets he is receiving were sent by A. They decide to use a MAC.

(a) Suppose A and $B_1, ..., B_n$ all share a secret key k. User A adds a MAC to every packet she sends using k, which each user B_i can verify. In at most two sentences, explain why this scheme is insecure. Namely, show that user B_1 is not assured that packets he is receiving are from A.

(b) Suppose user A has a set $S = \{k_1, ..., k_m\}$ of m secret keys. Each user B_i has some subset $S_i \subseteq S$ of the keys. When A transmits a packet, she computes the MAC ξ_i of the packet for each key k_i and sends along all of the MACs $\xi_1, \ldots, \xi_m$. When user B_i receives a packet he accepts it as valid only if all MACs corresponding to keys in S_i are valid. What property should the sets $S_1, ..., S_n$ satisfy so that the attack from part (a) does not apply? We are assuming all users $B_1, ..., B_n$ are sufficiently far apart so that they cannot collude.

(c) Show that when $n = 6$ (i.e., six recipients) the broadcaster A need only append 4 MACs to every packet to satisfy the condition of part (b). Describe the sets $S_1, ..., S_6 \subseteq \{k_1, ..., k_4\}$ you would use.

Problem 16: Combining Signatures and Encryption

Let (S_A, V_A) be Alice's digital signature scheme, and let (E_B, D_B) be Bob's public key encryption scheme. Alice wants to send a private signed message m to Bob. She thinks of several possible ways to proceed:

i. Encrypted signed message: Alice sends $E_B(\langle m, S_A(m)\rangle)$ to Bob.

ii. Signed encrypted message: Alice sends $\langle E_B(m), S_A(E_B(m)\rangle$ to Bob.

iii. Hybrid scheme: Alice sends $\langle E_B(m), S_A(m)\rangle$ to Bob.

(The notation $\langle x, y\rangle$ denotes the ordered pair (x, y), suitably encoded as a string.)

(a) For each scheme, describe how Bob decodes the message and verifies the signature.

(b) Alice comes to you for a recommendation of which scheme to use. Your job is to write a brief report giving your best professional advice to her. You should consider in your report any aspects that you feel would be important in practice, e.g., overall security and reliability of each scheme, possibility of known or unanticipated attacks, efficiency of implementation, and so forth.

Problem 17: Strong Collision-Free Hash Functions

Let h be a given strong collision-free hash function that maps bitstrings of length $2n$ to bitstrings of length n. We wish to construct a new strong collision-free hash function that maps bitstrings of length $4n$ to bitstrings of length n. Write $x = x_1 \cdot x_2 \cdot x_3 \cdot x_4$, where each x_i has length n. Consider the following candidates:

i. $h_1(x) = h((x_1 \oplus x_2) \cdot (x_3 \oplus x_4))$.

ii. $h_2(x) = h(h(x_1 \cdot x_2) \cdot h(x_3 \cdot x_4))$.

iii. $h_3(x) = h(x_1 \cdot x_2) \oplus h(x_3 \cdot x_4)$.

iv. $h_4(x) = h(h(h(x_1 \cdot x_2) \cdot x_3) \cdot x_4)$.

(Here, "$\oplus$" denotes bitwise exclusive-or and "$\cdot$" denotes concatenation.)

For each function h_i, say whether or not you think it is a strong collision-free hash function. If you think it is, show that the ability to find collisions for h_i would allow one to find collisions for h (contradicting the assumption that h is a strong collision-free hash function). If you think it is not, exhibit a pair of (distinct) colliding words for h_i.