Homework 3 - Solutions

5.3

The probability that a given Type 2 message has the same message digest as one of the $2^{32}$ Type 1 messages is roughly $2^{32} / 2^{64} = 1/2^{32}$, so it is likely that one of the $2^{32}$ Type 2 messages matches one of the $2^{32}$ Type 1 messages.

5.6

Otherwise it would be easy to find two messages with the same hash – any message that was not a multiple of 512 bits and that message padded as if by MD4.

5.12

No. The expected number of messages you would need to try is $2^{128}$ in either case.

5.19

By calculating $p_i = c_i \otimes b_i$.

This method has the weakness that patterns in plaintext will show up in corresponding patterns in ciphertext.

On the other hand it is stronger than the unmodified scheme, when the attacker is trying to modify a block of plaintext. In the unmodified scheme this action will result in unpredictable changes in the next block. In the proposed scheme it would result in unpredictable changes in the rest of the message.

Problem 1.

One way to protect Diffie-Hellman against the Man-in-the-Middle attack is to encrypt the Diffie-Hellman value with the other side’s public key. Why is this the case, given that an attacker can encrypt whatever it wants with the other side’s public key?

Solution

The attacker will not be able to decrypt the Diffie-Hellman values sent to him and so will not be able to compute the shared secrets.
Problem 2
Each node N of a network is been assigned a unique secret key Kn. This key is used to secure communications between the node and a trusted server. That is, all the keys are stored on a server. User A, wishing to send a secret message M to user B, initiates the following protocol:

1. A generates a random number R and sends to the server his name A, destination B, and $E_{Ka}[R]$
2. Server responds by sending $E_{Kb}[R]$ to A
3. A sends $E_{R}[M]$ together with $E_{Kb}[R]$ to B.
4. B knows Kb, thus decrypts $E_{Kb}[R]$ to get R and will subsequently use R to decrypt $E_{R}[M]$ to get M.

Analyze this protocol. Is it safe?

Solution

The protocol is not secure. The server doesn’t authenticate the sender. So an intruder Z can intercept $E_{Ka}[R]$ and $E_{R}[M]$. Then Z sends to the server the source name A, the destination name Z (his own), and $E_{Ka}[R]$, as if A wanted to send him the same message encrypted under the same key R as A did it with B.

The server will respond by sending $E_{Kz}[R]$ to A and Z will intercept that

Because Z knows his key Kz, he can decrypt $E_{Kz}[R]$, thus getting his hands on R that can be used to decrypt $E_{R}[M]$ and obtain M.

Problem 3

Devise a protocol based on a pre-shared secret key that hides identities and gives PFS for identity hiding. Make two variants, one in which an active attacker can learn only the initiator’s identity, and one in which an active attacker can learn only the target’s identity.

Solution

Messages 1 and 2 are Diffie-Hellman exchange.

Variant in which attacker can learn only the initiator’s identity:
In message 3, initiator sends identity, and proof of knowledge of the shared key, encrypted with the Diffie-Hellman key. In message 4, the target sends its identity and proof of knowledge of the shared key encrypted with the Diffie-Hellman key.

Variant in which attacker can learn only the target’s identity:
Message 2 consists of Diffie-Hellman number and, encrypted with the Diffie-Hellman key, the target’s identity and proof of knowledge of shared key. Message 3 is as in the previous variant.