T-79.4501 Cryptography and Data Security
EXAM
Tuesday, October 27, 2009

1. A Hill cipher is defined over Galois field $GF(2^4)$ with polynomial $x^4 + x + 1$. The encryption key is the 2×2-matrix
$$\begin{pmatrix} x+1 & 1 \\ 1 & x^2 \end{pmatrix}.$$
   a) (3 pts) Compute the encryption of the words $(x+1, x^2)$ and $(x^2, x^3 + x^2)$.
   b) (3 pts) Compute the decryption key.

2. Suppose that f is a function which maps a 32-bit string X to a 32-bit string $f(X)$. Using it, we define a function F, which maps two 32-bit strings A and B to two 32-bit strings A' and B' as follows:
$$\begin{aligned} A' &= f(A) \oplus B \\ B' &= f(f(A) \oplus B) \oplus A. \end{aligned}$$
   (a) (4 pts) Show that the function F is its own inverse.
   (b) (2 pts) Which well-known block cipher uses such a function?

3. (6 pts) Consider the following two methods of computing a 256-bit hash code H for a given message M:
   1. Using SHA-1: Split the message into three disjoint parts M_1, M_2 and M_3, compute $H_1 =$ SHA-1$(M_1||M_3)$ and $H_2 =$ SHA-1$(M_2||M_3)$ and form $H = H_1||H_2$ as the concatenation of the two 128-bit hash codes.
   2. Using SHA-256: Compute the hash code as $H =$ SHA-256(M).

   Which of the two methods, in your opinion, gives better resistance against collision attack, or are the methods about equally strong? Justify your answer.

4. (6 pts) Alice is using a toy version of the DSA signature scheme with a $p = 27109$ and $q = 251$. Explain how Alice can now generate an element of order 251 in the multiplicative group modulo 27109.

5. (6 pts) Alice and Bob are using a block cipher in CBC mode. It is known that CBC mode encryption has the following property: if some bits are changed in a ciphertext block then, after decryption, the same bits are changed in the next plaintext block, while the current plaintext will look completely garbled. Explain how Malice can make use of this weakness of CBC mode, and make meaningful changes to Bob's encrypted message to Alice.

Exam Calculator Policy: It is allowed to use any ordinary, non-programmable calculator.

Course Feedback: Please give feedback about the course. You find links to the feedback forms at NOPPA by opening the news item *Course Feedback*.