T-79.5501 Cryptology
EXAM
Thursday, May 20, 2010

1. (6 pts) The DES keys are 64 bits long, where each eighth bit is a parity bit computed as a modulo 2 sum of the preceding seven bits. A key management center uses AES encryption algorithm and a 128-bit "master" key to encrypt DES keys to end-users. Each ciphertext block consists of an encryption of two DES keys. Using the concept of unicity distance give an estimate of how many DES keys can be encrypted until an attacker who sees the ciphertext can uniquely determine the master key given enough computing time.

2. (6 pts) Let S be a sequence of bits and let us consider the complemented sequence $\bar{S}$, that is , the sequence obtained from S by adding 1 *modulo* 2 to each bit. Let L be the linear complexity of S.

   (a) Show that $LC(\bar{S}) \leq L + 1$.

   (b) Show that $LC(\bar{S}) = L - 1$, or L, or $L + 1$.

3. (6 pts) Let $\mathbf{T}_1$, $\mathbf{T}_2$ and $\mathbf{T}_3$ be independent random variables with biases $\epsilon_1 = \epsilon_2 = \epsilon_3 = 1/4$. Show that then $\mathbf{T}_1 \oplus \mathbf{T}_2$ and $\mathbf{T}_2 \oplus \mathbf{T}_3$ are not independent random variables.

4. Bob is using the *Rabin Cryptosystem*. Bob's modulus is $n = 40741 = 131 \cdot 311$. When encrypting x two additional bits b_1 and b_2 of information are computed to make the decryption unique:

   b_1: Jacobi symbol $\left(\frac{x}{n}\right)$ is equal to $(-1)^{b_1}$

   b_2: $b_2 = 0$ if and only if $x < \frac{n}{2}$

   (a) (2 pts) Encrypt $x = 2005$ and determine b_1 and b_2.

   (b) (2 pts) Instead of (b_1, b_2), Alice sends $(b_1 \oplus 1, b_2)$ to Bob with the encryption of $x = 2005$, and asks Bob to show her the decryption. Bob agrees, because he thinks it is Alice's message. What is the message Bob shows to Alice? (Hint: $311^{-1} \bmod 131 = 123$ and $131^{-1} \bmod 311 = 19$. Note also that you can compute all four square roots faster than Bob, since you already know one of the roots.)

   (c) (2 pts) Explain how Alice can now find the factors of Bob's modulus $n = 40741$.

5. (a) (3 pts) $p = 10262009$ and $q = 1282751$ are prime numbers. Find an element of multiplicative order 1282751 in $\mathbb{Z}^*_{10262009}$.

   (b) (3 pts) Let p be a prime and α be an element of multiplicative order q in $\mathbb{Z}^*_p$, where q is a prime and $q \equiv 3 \pmod 4$. Suppose that we have at our disposal an efficient algorithm for solving the discrete logarithm problem in the group generated by α. Using this algorithm, how would you efficicently solve a congruence of the form

   $$(\alpha^x)^x \equiv \beta \pmod p$$

   for any given $\beta \in \mathbb{Z}^*_p$?

Exam Calculator Policy. It is allowed to use a function calculator, however no programmable calculator.