T-79.5501 Cryptology
Exam
May 15, 2007

1. (6 pts) A PIN code for Bluetooth Pairing consists of four independently and randomly selected alfanumeric characters (36 possible characters). The PIN is inserted through a key pad of a mobile device, where each character is encoded into eight bits. Determine the entropy of the resulting 32-bit PIN code. Compare it with the maximum entropy of a string of 32 bits.

2. (6 pts) A *linear structure* of a Boolean function $g$ of $n$ variables is defined as a non-zero vector $w$ of length $n$ such that $g(x \oplus w) \oplus g(x)$ is constant. Consider the Geffe function $g(x) = g(x_1, x_2, x_3) = x_0 x_1 \oplus x_0 x_2 \oplus x_2$. Show that $g$ has exactly one linear structure.

3. (6 pts)

   (a) Evaluate the Jacobi symbol
   $$\left(\frac{784}{2041}\right).$$
   You should not do any factoring other than dividing out powers of 2.

   (b) Show that 2041 is an Euler pseudoprime to the base 784. Hint: $784^{12} \equiv 1 \pmod{2041}$.

4. Bob is using the *Rabin Cryptosystem.* Bob's modulus is $40741 = 131 \cdot 311$. Alice knows Bob's modulus but not its factors. Alice wants to remind Bob of an important date and sends it to Bob encrypted. The ciphertext is 24270.

   (a) (3 pts) Show how Bob decrypts the ciphertext. One of the possible plaintexts is a date, which Bob accepts and discards the other decryptions.

   (b) (3 pts) Alice happens to see one of the decryptions discarded by Bob. It is 5959. Show how Alice can now factor Bob's modulus.

5. (6 pts) Element $\alpha = 14$ is of order 13 in the multiplicative group $\mathbb{Z}_{157}^*$. It is given that element $\beta = 93$ is in the subgroup generated by $\alpha$. Using Shanks' algorithm compute the discrete logarithm $x$ of $\beta = 93$ to the base $\alpha = 14$, that is, solve the equation
   $$14^x \equiv 93 \,(\text{mod}\, 157).$$