T-79.5501 Cryptology
Homework 3
February 6, 2007

1. 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 DES encryption algorithm and a "master" DES key to encrypt DES keys to end users. Each ciphertext block consists of one encrypted DES key. Estimate the unicity distance of this cryptosystem, that is, estimate the number of encrypted DES keys that an attacker needs to determine the master key uniquely given enough computing time.

2. (Problem 6 from Hw 2 continued) Consider a cryptosystem where $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$ and keys are chosen equiprobably. This cryptosystem is used to encrypt language L, which consists of strings of plaintext characters in $\mathcal{P}$. Let n_0 denote the unicity distance. The language L is modified in such a way that s plaintext letters are chosen uniformly random from $\mathcal{P}$ and inserted to the plaintext after each block of d characters. What is the unicity distance for the modified language?

3. Compute $\gcd(9211, 4880)$, and find integers s and t such that $9211s + 4880t = \gcd(9211, 4880)$.

4. Solve the following congruence equations and systems.

   a)

   $$5x \equiv 4 \,(\mathrm{mod} 668)$$

   b)

   $$15x \equiv 12 \,(\mathrm{mod} 2004)$$

   c)

   $$\begin{aligned} 15x &\equiv 12 \,(\mathrm{mod} 2004) \\ 11x &\equiv 5 \,(\mathrm{mod} 2005) \end{aligned}$$

5. Consider the finite field $\mathbb{F} = \mathbb{Z}_2[x]/(f(x))$, with the polynomial $f(x) = x^5 + x^2 + 1$.

   a) Compute $(x^4 + x)(x^3 + x^2 + 1)$.
   b) Using the Euclidean Algorithm, compute $(x^3 + x)^{-1}$.
   c) Compute x^{35}. (Hint: $x^5 = x^2 + 1$.)

6. Consider the finite field $\mathbb{F} = \mathbb{Z}_2[x]/(f(x))$, where $f(x) = x^4 + x + 1$. Plaintext consists of strings of 4 bits with a single bit `1` and 3 bits `0`. Each such string occur independently and with probability $\frac{1}{4}$. The encryption method is a stream cipher with $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{F}^*$. Given a key $K = \beta \in \mathbb{F}^*$ and a plaintext sequence x_i, $i = 1, 2, \ldots, n$ the ciphertext sequence is computed as follows

   $$y_i = \beta^i x_i,\ i = 1, 2, \ldots, n.$$

   It is given that the 3rd and 4th terms of the ciphertext sequence are

   $$y_3 = 1100 \text{ and } y_4 = 0111.$$

   Then exactly two keys are possible. What are they? (Hint: To facilitate the computations you may represent the elements of $\mathbb{F}^*$ as powers of a primitive element α. For example, if you choose $\alpha = 0010$, then the four possible plaintext terms are 1, α, α^2 or α^3.)