TIK-110.503 Basics of Cryptology
Final exam
December 16, 2000

1. (6 points) Define a stream cipher as follows:

$$\begin{aligned}
\mathcal{P} &= \mathcal{C} = \mathbb{Z}_7,\ \mathcal{K} = \{(a,b)\,|\,\gcd(a,7)=1\} \\
z_i &= (a \times i + b) \bmod 7,\ i = 1,2,\ldots,\ \text{where } (a,b) \text{ is the key.} \\
e_z(x) &= (x+z) \bmod 7
\end{aligned}$$

   a) Using (5,3) as the key, compute the decryption of the message 25542531.

   b) If you know that some part of the plaintext is 110503, and this encrypts to give the ciphertext 501153, then derive as much as you can about the unknown key (a,b). What additional information you need to derive the entire key?

2. (6 points) Given positive integers n and r and a combiner function $f : \mathbb{Z}_2^n \times \mathcal{K} \to \mathbb{Z}_2^n$ a *Feistel cipher* is defined as follows: $L_i = R_{i-1}$, $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$, where $K_i \in \mathbb{Z}_2^n$, and $i = 1,2,\ldots,r$, and L_j, $R_j \in \mathbb{Z}_2^n$, $j = 0,1,2,\ldots,r$. The plaintext is $X = (L_0, R_0)$ and the ciphertext is $Y = (R_r, L_r)$.

   Consider a Feistel cipher as follows. Use $n = 3$ for the half-block size, and $r = 2$ rounds, and use independent 3-bit round keys K_1 and K_2. We define the combiner function f by $f(A,K) = F(A \oplus K)$, where $F(x) = x^3$ in the Galois field $GF(2^3)$ with the polynomial $x^3 + x + 1$.

   a) Describe a known plaintext attack against this cipher that will recover the secret key.

   b) Carry out the attack on the plaintext/ciphertext pair

$$\begin{aligned}
X &= 000000 \\
Y &= 111111
\end{aligned}$$

3. (6 points) The T function used in the hash-function SHA-1 is defined as follows. Let X_0, X_1, X_2 be three 32-bit blocks. Then $T(X_0,X_1,X_2) = (X_0 \wedge X_1) \vee (X_0 \wedge X_2) \vee (X_1 \wedge X_2)$, where $\wedge$ is bitwise "and" multiplication, and $\vee$ is bitwise "or" addition.

   Let $t(x_0,x_1,x_2)$ denote the Boolean function of three variables which is the one-bit component of T. Let $L_w(x_0,x_1,x_2) = w_0x_0 \oplus w_1x_1 \oplus w_2x_2$, for $w = (w_0,w_1,w_2) \in {\mathbb{Z}_2}^3$. Show that the function t has the following correlations with the linear functions L_w:

$$c(t, L_w) = \begin{cases} 0, & \text{if } H_W(w) = 0 \text{ or } 2 \\ \frac{1}{2}, & \text{if } H_W(w) = 1 \\ -\frac{1}{2}, & \text{if } H_W(w) = 3 \end{cases}$$

4. (6 points) Bob is using the Rabin public key cryptosystem with $n = 1999 \times 499$ and $B = 0$. Find the four possible decryptions of the ciphertext $y = 2000$.

5. (6 points) Suppose Bob is using the El Gamal Signature Scheme in $\mathbb{Z}_p$, and he signs two messages x_1 and x_2 with signatures (γ_1, δ_1) and (γ_2, δ_2), respectively. Alice sees the messages and their respective signatures, and she sees that $\gamma_1 = \gamma_2$.

   a) Describe how Alice can now derive information about Bob's private key.

   b) Suppose $p = 13$, $x_1 = 1$, $x_2 = 4$, $\delta_1 = 11$, and $\delta_2 = 2$, and $\gamma_1 = \gamma_2 = 7$. What can Alice say about Bob's private key?

   (For your convenience: $\gamma = \alpha^k \bmod p$ and $\delta = (x - a\gamma)k^{-1} \bmod (p-1)$.)