MATC16 Cryptography and Coding Theory
Gábor Pete
University of Toronto Scarborough
gpete at utsc dot utoronto dot ca

Homework Assignment 4 (Due April 7 Thu)

Problem 1. Peggy claims she knows an RSA plaintext. That is, n, e, c are public, and she claims to know an m such that $m^e \equiv c \pmod{n}$. She wants to prove this to Victor using a zero-knowledge protocol. They perform the following steps:

1. Peggy chooses a random integer r_1 with $\gcd(r_1, n)=1$, and computes $r_2 \equiv m \cdot r_1^{-1} \pmod{n}$.
2. Peggy computes $x_i \equiv r_i^e \pmod{n}$ for $i = 1, 2$, and sends x_1, x_2 to Victor.
3. Victor checks if $x_1 x_2 \equiv c \pmod{n}$.

Give the remaining steps of the protocol. Victor wants to be at least 99% sure that Peggy is not lying. **(2 pts)**

Problem 2. List the points on the elliptic curve $\{(x, y) : y^2 \equiv x^3 - 2 \pmod{7}\}$. **(2 pts)**

Problem 3. Factor $n = 35$ by the elliptic curve method, using the curve $y^2 = x^3 + 26$ and calculating $P \boxplus P \boxplus P$ for $P = (10, 9)$. **(2 pts)**

Problem 4. On Thursday we will prove that, for any random variable X and any function f, we have $H(f(X)) \leq H(X)$. (In words, we cannot increase the entropy by doing something deterministic to X.)

(a) Letting X take on the values ± 1, and letting $f(x) = x^2$, show that it is possible that $H(f(X)) < H(X)$. **(1 pt)**

(b) Show that $H(f(X)) = H(X)$ if and only if f is one-to-one on the set of values that are taken by X with positive probability. **(2 pts)**

Problem 5. Consider the Hadamard matrix H that is used in defining the Hadamard code, Example 6 of page 397. Namely, H is the 32×32 matrix whose entry h_{ij} in the ith row and jth column, for $0 \leq i, j \leq 31$, is given by

$$h_{ij} = (-1)^{a_0 b_0 + a_1 b_1 + \cdots + a_4 b_4},$$

where $i = a_4 \dots a_0$ and $j = b_4 \dots b_0$ in binary. For instance, for $i = 31$ and $j = 3$, we have $i = 11111$ and $j = 00011$, hence $h_{31,3} = (-1)^2 = 1$.

Prove that the dot product of any two different rows of H is 0. **(2 pts)**

Problem 6. The following is a parity check matrix for a binary $[n, k]$ code C:

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

What is n and k? Find a generating matrix for C. List the codewords in C. What is the minimal distance in C? What is the code rate of C? **(4 pts)**

(Max possible score: 15 pts)