Crypto Revision Exercises

1. (a) Let $p = 71$ be a prime, let $g = 31$ be a primitive root modulo p. Then use the baby step, giant step algorithm to compute the index $I(6)$.

   (b) Bob has an RSA public key of the form $(n, 3)$, i.e. $e = 3$. When Alice wants to send a number $0 \leq x < n$ to Bob, she encrypts it using Bob's public key. For some reason, Bob fails to receive the message correctly, he informs Alice on the matter, and she retries to send the message again. However, this time, to prevent repeating the same message, Alice encrypts $x + 1$ instead and sends it to Bob. Suppose that Eve has intercepted both encrypted messages successfully and she knows that the second time Alice encrypted $x + 1$ and sent it to Bob. Show how Eve can exploit this information to easily obtain x. (Hint: First try to compute $x^2 + x$ from this information).

   (c) Alice is signing messages using the Elgamal signature scheme with a public prime p and a primitive root g. Her public verification key is $y \equiv g^\alpha \bmod p$. Suppose that she signs two different messages m_1 and m_2 with signatures (r, s_1) and (r, s_2) respectively. Here you may assume that $0 < m_1, m_2 < p - 1$ and $\gcd(s_1 - s_2, p - 1) = \gcd(r, p - 1) = 1$. Show how this information can be used to find Alice's private key α.

2. (a) Alice is using the following elliptic curve version of a Hash function to a compute hash of a message $0 \leq m < N$:

   She fixes an elliptic curve E over a finite field $\mathbb{F}_p$ where p is a large prime, approximately of size $\sqrt{N}$. She fixes two points $P_1, P_2 \in E(\mathbb{F}_p)$ with orders n_1 and n_2 respectively, where $n_1 \neq n_2$ are two large primes. Alice makes $E(\mathbb{F}_p)$, P_1, P_2 and their orders n_1, n_2 public. The message $0 \leq m < N$ is further assumed to be co-prime to both n_1 and n_2. The hash function H is then defined as:

   $$H(m) = [m^{-1} \bmod n_1]P_1 \oplus [m^{-1} \bmod n_2]P_2.$$

   Prove that H is pre-image resistant (or one way) but not strongly collision free.

   (b) Let $n = pq$, where p and q are odd primes such that $|p - q| < 12\sqrt[4]{n}$. We use Fermat's factorisation method to factorise n. Give an upper bound for the number of steps needed. Your answer should be an integer not depending on n. Justify your answer rigorously.

3. (a) Let E be an elliptic curve defined over $\mathbb{Q}$ by the equation

   $$y^2 = x^3 + 2p,$$

   where p is a prime. Compute the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ for all possible values of the prime p.

(b) Alice wants to send the same secret message m to both Bob and Oscar. Suppose she has already shared $n \times n$ block cipher matrices M_1 and M_2 with Bob and Oscar respectively. The matrix M_1 is supposed to be only known to Alice and Bob (and similarly M_2 is only known to Alice and Oscar).

i. Using the matrices M_1 and M_2, devise a way for Alice to securely send the message m to both Bob and Oscar in such a way that they can not decipher m on their own just using their respective keys. However, Bob and Oscar can jointly figure out what m is by communicating with each other on public channels. Note that Bob and Oscar should never share their respective keys M_1 and M_2 with each other.

ii. Suppose Alice is wary of a further issue that either Bob or Oscar could lie to the other in the above process. So she wants to further devise a way to help both Bob and Oscar verify that the message m that they obtain at the end of this process is the correct one. How can she further ensure this? For this part, you should just indicate which public key cryptosystem she can use to achieve this.

Codes Revision Exercises

1. (a) i. Show that $x^2 + 2x + 2$ is irreducible in $\mathbb{F}_3[x]$, and is a primitive polynomial over $\mathbb{F}_3$.

   ii. Let $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + 2x + 2)$, and let $C \subseteq \mathbb{F}_9^6$ be given by

   $$C = \langle \{ (2x, 0, 1, 0, 2x, x + 2), (2x + 1, x, 0, 0, 2x + 2, x + 1), (2x, x, x + 2, 2, 2, 2x + 2) \} \rangle.$$

   What are the parameters $[n, k, d]$ of C?

   iii. Calculate the parameters $[n', k', d']$ for the code $C^{\{6\}}$.

2. (a) Alice is sending messages to Bob, using the code $C \subseteq \mathbb{F}_5^5$ with generator-matrix $G = \begin{pmatrix} 1 & 2 & 0 & 3 & 4 \\ 0 & 0 & 1 & 2 & 3 \end{pmatrix}$.

   i. Find the parameters $[n, k, d]$ and a check-matrix H for this code.

   ii. Alice encodes message $\mathbf{m}_1$ as $\mathbf{c}_1$, and sends it to Bob.
   In the channel it suffers one symbol-error, and Bob receives the word
   $\mathbf{y}_1 = (1, 2, 4, 2, 0)$. Show how, *without* making a whole syndrome table, Bob can use $S(\mathbf{y}_1)$ to find $\mathbf{c}_1$ and then $\mathbf{m}_1$.
   How does he know that $\mathbf{c}_1$ is the *unique* nearest neighbour of $\mathbf{y}_1$?

   iii. If the channel is a q-ary symmetric channel with symbol-error probability $\frac{1}{2}$ (for suitable q), what was the probability that $\mathbf{y}_1$ was received if $\mathbf{c}_1$ is the word that was sent? Explain why syndrome decoding is a suitable decoding technique if this code is sent using such a channel.

   (b) Let the code $C \subseteq \mathbb{F}_3^4$ have check-matrix $H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$.

   i. Find the parameters $[n, k, d]$ of C, and show that C is MDS.

   ii. Show that C is self-dual - that is, $C = C^{\perp}$.

   iii. Show that C is perfect.

   iv. In a *simplex* code, the Hamming distance $d(\mathbf{c}_1, \mathbf{c}_2)$ between any two distinct codewords is the same. Show that C is a simplex code.

3. In this question we use $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$.
   To construct our code we also use some polynomials $\phi(y) = ay^2 + by + c$ over $\mathbb{F}_4$.
   (So the coefficients a, b, c are from $\mathbb{F}_4$, and we write y for the variable to avoid confusion. We can then 'plug in' elements of $\mathbb{F}_4$ for y.)

   The hexacode $C \subseteq \mathbb{F}_4^6$ is given by

   $$C = \{ (\, a,\, b,\, c,\, \phi(1),\, \phi(x),\, \phi(x^2)\,) \mid \phi(y) = ay^2 + by + c \text{ with } a, b, c, \in \mathbb{F}_4 \}$$

(a) How many words are in this code?

(b) Show that $G = \begin{pmatrix} 1 & 0 & 0 & 1 & x^2 & x \\ 0 & 1 & 0 & 1 & x & x^2 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$ is a generator-matrix for C.

(c) Find a check-matrix H for C, and show that $C^\perp \neq C$, but $C^\perp$ is permutation equivalent to C.

(d) By puncturing C at the 6th and 3rd position respectively, we make new codes C_6 and C_3. Show that these are Hamming codes.

(e) Consider the extended code $\widehat{C}_6$. Is it equal, or equivalent, to C? You may use the fact that $d(C) = 4$. (*Hint:* First show that $(x^2, x, 1, 0, 0) \in C_6$.)