VE475 Intro to Cryptography Homework 8

Taoyue Xia, 518370910087

2021/07/15

Ex1 — Missile or not missile

We can simply use a (t, w)-*threshold scheme*, or to be more specific, the Shamir threshold scheme, to solve this problem. First we can calculate $lcm(1, 2, 5) = 10$, so we can divide the secret into 10 shares. The general has 10 shares, each colonel has 5 shares and each desk clerk has 2 shares. For the previous setting, the problem is solved.

Ex2 — Asmuth-Bloom Threshold Secret Sharing Scheme

The Asmuth-Bloom Threshold Secret Sharing Scheme uses the Chineses Remainder Theorem to determine a secret based on multiple modulos.
We consider a sequence of pairwise coprime positive integers $m_0 < \cdots < m_n$, with $2 \leq k \leq n$ be an integer, and $m_0 \cdot m_{n-k+2} \cdots m_n < m_1 \cdots m_k$. For this sequence, we can choose the secret S in the set $\mathbb{Z}/m_0\mathbb{Z}$.
We then pick a random integer α such that $S + \alpha \cdot m_0 < m_1 \cdots m_k$. We will compute the reduction modulo m_i of $S + \alpha \cdot m_0$, for all $1 \leq i \leq n$, as s_i, then these are the shares $I_i = (s_i, m_i)$.
Now for any k different shares $I_{i_1}, \cdots, I_{i_k}$, we consider the system of congruences:

$$\begin{cases} x \equiv s_{i_1} \ mod \ m_{i_1} \\ \quad\quad \vdots \\ x \equiv s_{i_k} \ mod \ m_{i_k} \end{cases}$$

Then according to the Chinese Remainder Theorem, since all m_i are pairwise coprime, the system will have a unique solution S_0 modulo $m_{i_1} \cdots m_{i_k}$.
We can say that the Asmuth-Bloom scheme is perfect since α is independent of S and

$$\left.\begin{array}{r}\prod_{i=n-k+2}^{n} m_i \\ \alpha\end{array}\right\} < \frac{\prod_{i=1}^{k} m_i}{m_0}$$

Therefore, α can be any integer modulo

$$\prod_{i=n-k+2}^{n} m_i$$

This product of $k-1$ moduli is the largest of any of the n choose $k-1$ possible products, therefore any subset of $k-1$ equivalences can be any integer modulo its product, and no information from S is leaked.

Ex3 — Shamir' s Threshold Secret Sharing Scheme

The Lagrange Interpolation method can be expressed as:

$$\ell_i(x) = \prod_{\substack{0 \le m \le k \\ m \ne i}} \frac{x - x_m}{x_i - x_m} = \frac{(x - x_0) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_k)}{(x_i - x_0) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_k)}$$

$$L(x) = \sum_{i=0}^{k} y_i \ell_i(x)$$

Using the example on slide 6.10, we set $p = 1234567890133$, $m = 190503180520$, $r_1 = 482943028839$, and $r_2 = 1206749628665$. We can first construct $S(X)$ as:

$$S(X) = 190503180520 + 482943028839X + 1206749628665X^2$$

We take three values x_i and corresponding $S(x_i)$ as y_i:

$$x_0 = 2, \quad y_0 = 1045116192326$$

$$x_1 = 3, \quad y_1 = 154400023692$$

$$x_2 = 7, \quad y_2 = 973441680328$$

Then we can calculate each $\ell_i(x)$ as follows:

$$\ell_0(x) = \frac{(x-3)(x-7)}{(2-3)(2-7)} = \frac{1}{5}(x-3)(x-7)$$

$$\ell_1(x) = \frac{(x-2)(x-7)}{(3-2)(3-7)} = -\frac{1}{4}(x-2)(x-7)$$

$$\ell_2(x) = \frac{(x-2)(x-3)}{(7-2)(7-3)} = \frac{1}{20}(x-2)(x-3)$$

After combining, the final polynomial is:

$$\begin{aligned} L(x) &= \sum_{i=0}^{2} y_i \ell_i(x) \\ &= \frac{1045116192326}{5}(x-3)(x-7) - \frac{154400023692}{4}(x-2)(x-7) + \frac{973441680328}{20}(x-2)(x-3) \\ &= \frac{1095476582793}{5}x^2 - 1986192751427x + \frac{20705602144728}{5} \end{aligned}$$

Using the Extended Euclidean algorithm, we can easily find the inverse of 5 modulo p as 740740734080. Then we can determine that:

$$r_2 \equiv \frac{1095476582793}{5} \equiv 1095476582793 \cdot 740740734080 \equiv 1206749628665 \; mod \; p$$

$$r_1 \equiv -1986192751427 \equiv 482943028839 \; mod \; p$$

$$m \equiv \frac{20705602144728}{5} \equiv 20705602144728 \cdot 740740734080 \equiv 190503180520 \; mod \; p$$

In this way, we can recover the secret message.

Ex4 — Simple questions

1. From the two plains from Alice and Bob, we know that:

$$z = 2x + 3y + 13 = 5x + 3y + 1 \quad \Rightarrow \quad x = 4, \; z = 3y + 21$$

where $x = 4$ is the secret. Therefore, Alice and Bob don't need the help of Charly.

2. We know the fact that if one adds to a column of a matrix the product by a scalar of another column, then the determinant remains unchanged. So we can subtract each column with the previous column multiplied by x_1, starting from the rightmost colum, except for the first column, then it gives us the following matrix:

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & x_2 - x_1 & x_2(x_2 - x_1) & \cdots & x_2^{t-2}(x_2 - x_1) \\ 1 & x_3 - x_1 & x_3(x_3 - x_1) & \cdots & x_3^{t-2}(x_3 - x_1) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_t - x_1 & x_t(x_t - x_1) & \cdots & x_t^{t-2}(x_t - x_1) \end{bmatrix}$$

Denote the Vandermonde matrix as V, the above matrix as W, we know that $\det(V) = \det(W)$. According to the Laplace expansion formula along the first row, we can transform matrix W into:

$$L = \begin{bmatrix} x_2 - x_1 & x_2(x_2 - x_1) & \cdots & x_2^{t-2}(x_2 - x_1) \\ x_3 - x_1 & x_3(x_3 - x_1) & \cdots & x_3^{t-2}(x_3 - x_1) \\ \vdots & \vdots & \ddots & \vdots \\ x_t - x_1 & x_t(x_t - x_1) & \cdots & x_t^{t-2}(x_t - x_1) \end{bmatrix}$$

And we can obviously find out that $\det(L) = \det(W) = \det(V)$. Then we notice that each row has a factor $x_k - x_1,\ k \in \{2, 3, \cdots, t\}$. So we can express $\det(L)$ as follows:

$$\det(L) = \prod_{1<k\leq n} (x_k - x_1) \begin{vmatrix} 1 & x_2 & x_2^2 & \cdots & x_2^{t-2} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{t-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_t & x_t^2 & \cdots & x_t^{t-2} \end{vmatrix} = \det(V')$$

where V' is a Vandermonde matrix from x_2 to x_t. So we iterate the process until

$$\det(V') = \begin{vmatrix} 1 & x_{t-1} \\ 1 & x_t \end{vmatrix} = x_t - x_{t-1}$$

Therefore, we can conclude that:

$$\begin{aligned} \det(V) &= (x_t - x_1) \cdots (x_t - x_{t-1})(x_{t-1} - x_1) \cdots (x_{t-1} - x_{t-2}) \cdots\cdots (x_2 - x_1) \\ &= \prod_{1\leq j<k\leq t} (x_k - x_j) \end{aligned}$$

Therefore, the proof is done.

3. The evaluation website for VE475 has not opened so far.

Ex5 — Reed Solomon codes

1. The Reed–Solomon code is actually a family of codes, where every code is characterised by three parameters: an alphabet size q, a block length n, and a message length k, with $k < n \leq q$. The set of alphabet symbols is interpreted as the finite field of order q, thus q has to be a prime power. the block length is usually some constant multiple of the message length, that is, the rate $R = k/n$ is some constant, and the block length is equal to or one less than the alphabet size, that is, $n = q$ or $n = q - 1$.
   Every codeword of the Reed–Solomon code is a sequence of function values of a polynomial of degree less than k. The message symbols are treated as the coefficients a polynomial p of degree less than k, over the finite field $\mathbb{F}$ with q elements. In turn, the polynomial p is evaluated at $n \leq q$ distinct points $\{a_1, \ldots, a_n\}$ of the field $\mathbb{F}$, and the sequence of values is the corresponding codeword.
   Formally, the set $\mathcal{C}$ of codewords of the Reed–Solomon code is defined as follows:

   $$\mathcal{C} = \{(p(a_1), \ldots, p(a_n)) \,|\, p \text{ is a polynomial over } \mathbb{F} \text{ of degree} < k\}$$

2. Since any two distinct polynomials of degree less than k agree in at most $k - 1$ points, this means that any two codewords of the Reed – Solomon code disagree in at least $n - (k - 1) = n - k + 1$ positions. So the distance of the Reed–Solomon code is exactly $D = n - k + 1$.
   According to theorem 7.16, if $D > k(1 - 1/w^2)$, where w is the size of coalition, and k is the code length in Reed-Solomon code, then it is possible to identify a parent of descendant of $\mathcal{C}$. Therefore, for $w = 2$, we can obtain that

   $$\begin{aligned} D = n - k + 1 &> k(1 - \frac{1}{w^2}) \\ k &< \frac{4}{7}(n + 1) \end{aligned}$$

   So we can conclude that k should satisfy the condition $k < \frac{4}{7}(n + 1)$.