IV054 Coding, Cryptography and Cryptographic Protocols
2019 - Exercises IX. - Solutions

Exercise 1

(a) Given:

$$(n, t) = (5, 3)$$
$$p = 567997$$
$$x = \{1, 2, 3, 4, 5\}$$
$$a_1 = 3^{456195} \mod 101021 = 41352$$
$$a_2 = 5^{456195} \mod 101021 = 18679$$
$$S = a_0 = 456195$$

From that we construct the polynomial:

$$f(x) = a_0 x^0 + a_1 x^1 + a_2 x^2$$
$$f(x) = 456195 + 41352x + 18679x^2$$

And compute the shares:

$$s_1 = f(1) = 516226 \mod 567997 = 516226$$
$$s_2 = f(2) = 613615 \mod 567997 = 45618$$
$$s_3 = f(3) = 748362 \mod 567997 = 180365$$
$$s_4 = f(4) = 920467 \mod 567997 = 352470$$
$$s_5 = f(5) = 1129930 \mod 567997 = 561933$$

The shares are pairs (i, s_i) for $i = 1..5$.

(b) We can compute it with usage of Lagrange formula from slides.
$(x_1, y_1) = (1, 64104), (x_2, y_2) = (2, 156586), (x_3, y_3) = (3, 291500)$
$l_1 = \frac{x-x_2}{x_1-x_2} * \frac{x-x_3}{x_1-x_3} = \frac{x-2}{1-2} * \frac{x-3}{1-3} = \frac{x^2}{2} - \frac{5x}{2} + 3$
$l_2 = \frac{x-x_1}{x_2-x_1} * \frac{x-x_3}{x_2-x_3} = \frac{x-1}{2-1} * \frac{x-3}{2-3} = -x^2 + 4x - 3$
$l_3 = \frac{x-x_1}{x_3-x_1} * \frac{x-x_2}{x_3-x_2} = \frac{x-1}{3-1} * \frac{x-2}{3-2} = \frac{x^2}{2} - \frac{3x}{2} + 1$

a(x) = $\sum_{j=1}^{t-1} y_j l_j$
a(x) = $y_1 * l_1 + y_2 + l_2 + y_3 + l_3 \mod p$
a(x) = $y_1 * l_1 + y_2 + l_2 + y_3 + l_3 \mod p$
a(x) = 14054 + 26x(816x + 1109) mod p
S = 14054
We can also compute it as

$$S = \sum_{i \in J} f(i) \prod_{j \in J, j \neq i} \frac{j}{j-i} = 64104 * 2 * \frac{3}{2} + 156586 * \frac{-1}{1} * 3 + 291500 * \frac{-1}{2} * \frac{-2}{1} = 14054$$

So the secret for shares (1, 64104), (2, 156586), (3, 291500) is 14054.

Exercise 2

This example is similiar to 9.14 from exersice book. Let's assume that the super-secret research project is protected by secret, let's assume a password used for encryption. We'll be protecting the password. As each professor should have full access on his own, let's give them password directly.

Let's use (38, 19)-threshold scheme to protect the password and let's distribute the shares this way: each post-doc gets 7, each Ph.D. students gets 3, each external consultant gets 1.

Now let's confirm, that they do indeed have access as required:

- one professor - yes, they has the password directly
- three post-docs - yes, they have in $3 * 7 = 21$ shares which is enough $(21 >= 19)$
- two post-docs and two Ph.D. students - $2 * 7 + 2 * 3 = 20$ shares which is enough $(20 >= 19)$
- two post-docs, one Ph.D. student and two external consultants - $2 * 7 + 1 * 3 + 2 * 1 = 19$ which is enough $(19 >= 19)$
- one post-doc and four Ph.D. students - $1 * 7 + 4 * 3 = 19$ which is enough $(19 >= 19)$

So everyone that needs to have access does have it. Even though the assignment doesn't explicitly specify that for example one post doc shouldn't have access on his own, I would argue it's presumed. So let's confirm that there is no combination that shouldn't have access and has it.

Let's ignore any combination involving professor, they have access on their own. Let's split the combinations based on the number of postdocs:

- If you have three post-docs you should have access.
- If you have only two post-docs you have 14 shares and can't get the 7 shares of the another post-doc. So you need to get at least $19 - 2 * 7 = 5$ shares out of the remaining $38 - 3 * 7 = 17$. You can't use more than one Ph.D. student otherwise you would have access, so you can get only 3 shares from the Ph.D. students and need to get another $5 - 3 = 2$ shares. Those you can only get by using both consultants and in that case you should have access.
- If you have only one post-doc, you can get only 7 shares out of the 21 that post-docs hold. So you need to get $19 - 7 = 12$ out of the remaining $38 - 3 * 7 = 17$ remaining shares. You can use at most 3 Ph.D. students otherwise you should have access, so you can get 9 out of the 15 shares the postdocs hold. That means you need to get another $12 - 9 = 3$ shares, but only $17 - 15 = 2$ are remaining, so it's impossible.
- If you have no post-docs, they you can only use $38 - 3 * 7 = 17$ shares but you need to get 19 to unlock the secret. So it's not possible.

Exercise 3

From the slides we know that a secret sharing scheme is based on the fact: Three nonparallel planes in space intersect in exactly one point. Each share is a plane, and the secret is the point at which three shares intersect. If we want to find the intersection of 3 planes, we need to convert their parameterized form to general. So let's convert it.

Parametrized form (s + 1, -s - t + 2, t + 3) we can convert to:

x = s + 1
y = -s - t + 2
z = t + 3
x + y + z = 6

Parametrized form (s + 1, 5s + 3t + 2, 2t + 3) we can convert to:

x = s + 1
y = 5s + 3t + 2
z = 2t + 3
10x - 2y + 3z = 15

Parametrized form (3s + 1, 2s - t + 2, 3t + 3) we can convert to:

x = 3s + 1
y = 2s - t + 2
z = 3t + 3
-2x + 3y + z = 7

So we have 3 equations of 3 variables:

x + y + z = 6
10x - 2y + 3z = 15
-2x + 3y + z = 7

So x = 1, y = 2, z = 3. The shared secret is (1, 2, 3).

Just straight by looking at these parametric equations (considered that (x, y, z) stand for points) we can see that we have an intersection if $s = 0$ and $t = 0$

Therefore, $x = 1$, $y = 2$ and $z = 3$

Exercise 4

(a) Such OA cannot exist: inequality $\lambda \geq \frac{k(n-1)+1}{n^2}$ must hold. But in this case, $1 < \frac{5}{4}$

(b)

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

Exercise 5

Using the same threshold and p, we know that the two secrets are both split into polynomials of power $t-1$, and each user has the shares (i, y_i), (i, y'_i), then

$$y_i = S + a_1 \cdot i + ... + a_{t-1} \cdot i^{t-1}$$

$$y'_i = S' + a'_1 \cdot i + ... + a'_{t-1} \cdot i^{t-1}$$

and the new scheme for secret $S + S'$ can be as follows:

$$\hat{y_i} = y_i + y'_i = S + S' + (a_1 + a'_1) \cdot i + ... + (a_{t-1} + a'_{t-1}) \cdot i^{t-1} = S + S' + \sum_{j=1}^{t-1} \hat{a_i} \cdot i^j$$

This is exactly how shares are made with $x_i = i$ and $\hat{a_i} = a_i + a'_i$. Now we also need t shares for reconstruction of the secret. The users can compute their shares as $(i, y_i + y'_i)$.

Exercise 6

(a) If we have a transcript of a correctly performed execution of the Schnorr identification scheme then the following must hold:
$\gamma = \alpha^y v^r \mod p$
Verification for all the (γ, r, y) transcripts, having $v = 47 \mod p$ and $\alpha = 169$:

$(83, 21, 7) \rightarrow 169^7 * 47^{21} \mod 311 = 83 = \gamma$
The transcript (83, 21, 7) is a correct one.

$(83, 17, 21) \rightarrow 169^{21} * 47^{17} \mod 311 = 32 \neq \gamma$
The transcript (83, 17, 21) is not a correct one.

$(126, 19, 15) \rightarrow 169^{15} * 47^{19} \mod 311 = 105 \neq \gamma$
The transcript (126, 19, 15) is not a correct one.

$(126, 11, 8) \rightarrow 169^8 * 47^{11} \mod 311 = 126 = \gamma$
The transcript (126, 11, 8) is a correct one.

(b) Two of the valid transcripts: (83, 21, 7), (126, 11, 8). We know that Alice uses a pseudorandom update function $k_{i+1} = 3k_i + 4 \bmod 31$. If random k was used in transcript (83, 21, 7) and pseudorandom was used in (126, 11, 8) it must holds that

$$\gamma_2 = \alpha^{3\gamma_1} * \alpha^4 \mod p$$

$$126 = 169^{3*83} * 169^4 \mod 311$$

It holds. So now we obtain two equations:

$$y_1 \equiv k_1 + ar_1 \mod q$$

$$y_2 \equiv 3k_1 + 4 + ar_2 \mod q$$

$$7 \equiv k_1 + 21a \mod 31$$

$$8 \equiv 3k_1 + 4 + 11a \mod 31$$

$$21 \equiv 3k_1 + 63a \mod 31$$

$$4 \equiv 3k_1 + 11a \mod 31$$

Now, the equations can be combined to obtain:

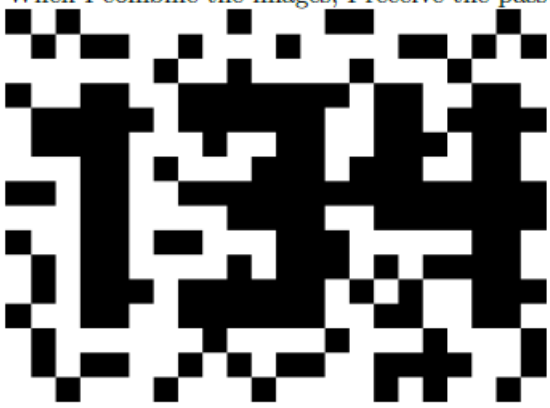
$$y_1 - y_2 \equiv 3k_1 - 3k_1 + ar_1 - ar_2 \mod q$$

$$17 \equiv 63a - 11a \mod 31$$

From this we obtain a = 20.

Exercise 7

When I combine the images, I receive the password 134.



Exercise 8

(a) We can see that a $t-(n,t,1)$ orthogonal array exists because the array consists of all the n^t t-tuples. Now consider creating (t+1)-tuples where the sum of the tuple is 0 mod n. These tuples create a $t-(n,t+1,1)$ orthogonal array, also called a Zero sum array. To prove this we can see that if we choose the first t columns, the the condition for each tuple to appear once is satisfied. Let's choose a different column, so in a sense let's erase on of the first t columns. If the array should not be an orthogonal array then some two rows of n-1 elements would be the same and there would be a choice of a column to be erased. But because the sum of elements in each row is 0 mod n and the elements are numbers from 0 to n-1, the elements in the erased column must be the same too. Therefore these two rows were same in the t-(n,t,1) array which creates a contradiction as that is an orthogonal array.

(b) Suppose there is an $t-(n,k,\gamma)$ orthogonal array A. Let x be any symbol in the array. We can then rearrange the rows of A so that the rows containing symbol x in the first column are grouped up. Then if we remove all the rows that do not contain the symbol x in the first column and then the first column, we have effectively lowered t and k by 1 and created the subarray A' that is a $(t-1)-(n,k-1,\gamma)$ orthogonal array. Following is a visualisation of A' within A.

$$\begin{pmatrix} x & \\ x & \\ x & A' \\ x & \\ x & \\ \vdots & \\ \vdots & \cdots \\ \vdots & \end{pmatrix}$$