Question 1.

$(n, t) = (5, 3), p = 567997$

(a) $x = \{1, 2, 3, 4, 5\}$

$$a_1 = 3^{469517} \mod 101021 = 71631$$
$$a_2 = 5^{469517} \mod 101021 = 78075$$
$$S = a_0 = 469517$$

Next, we can construct the polynomial:

$$f(x) = a_0x^0 + a_1x^1 + a_2x^2$$
$$f(x) = 469517 + 71631x + 78075x^2$$

Now, we can compute the shares:

$$s_1 = f(1) = 619223 \mod 567997 = 51226$$
$$s_2 = f(2) = 925079 \mod 567997 = 357082$$
$$s_3 = f(3) = 1387085 \mod 567997 = 251091$$
$$s_4 = f(4) = 2005241 \mod 567997 = 301250$$
$$s_5 = f(5) = 2779547 \mod 567997 = 507559$$

The shares are:

$$(1, 51226),\ (2, 357082),\ (3, 251091),\ (4, 301250),\ (5, 507559)$$

(b) The shares create a system of equations:

$$S + a_1 + a_2 = 438605$$
$$S + 2a_1 + 4a_2 = 273820$$
$$S + 3a_1 + 9a_2 = 133642$$
$$S = 627997 \mod 567997 = 60000$$

The secret from the shares is 60000.

Question 2.

(a) Yes, such orthogonal array exists. Following the condition that any pair of symbols n^2 occurs in exactly λ rows, we can find the following array

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

(b) The upper bound is computed as

$$k = \frac{\lambda n^2 - 1}{n - 1}$$

(c) Number of rows is computed as

$$r = \lambda n^s$$

where r is the number of rows

(d) We need to find an orthogonal array, where each subset of length 3 occurs only once. There are $1 \cdot 2^3 = 8$ rows in the OA.

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

(e) We take the $t - (n, k, \lambda)$ array and choose an element e in it. We then select rows that have this element on the first position and delete the first position to get a subarray. This subarray is the $(t-1) - (n, k-1, \lambda)$ orthogonal array.

Question 3.

(a) $\sigma = \alpha^y * v^r \mod p$

$v = 47$

$\alpha = 169$

(13, 23, 11)

$169^{11} * 47^{23} \mod 311 = 13 = \sigma$ **correct**

(113, 17, 3)

$169^3 * 47^{17} \mod 311 = 113 = \sigma$ **correct**

(113, 19, 15)

$169^{15} * 47^{19} \mod 311 = 105 \neq \sigma$ **incorrect**

(13, 27, 15)

$169^{15} * 47^{27} \mod 311 = 260 \neq \sigma$ **incorrect**

(b) If random k was used in $(113, 17, 3)$ and pseudo-random in $(13, 23, 11)$ it must hold that:

$\sigma_1 = \alpha^k \mod p$

$\sigma_2 = \alpha^{3*k+4} \mod p$

$\sigma_2 = \sigma^3 * 169^4 \mod p$

$\sigma_1 = 113$

$13 = \sigma_2 = 113^3 * 169^4 \mod 311$

Therefore:

$y_1 = k_1 + \alpha * r_1 \mod q$

$y_2 = 3 * k_1 + 4 + \alpha * r_2 \mod q$

$3 = k_1 + 17 * a \mod 31$

$11 = 3 * k_1 + 4 + 23 * a \mod 31$

$9 - 7 = 3 * k_1 - 3 * k_1 + 51 * a - 23 * a \mod 31$

$2 = 28 * a \mod 31 = 20$

Secret key is 20.

Question 4.

Peggy will take every row and every column as a lists, together there will be 2n such lists. Every list will contains n numbers. Every number will be twice in all the lists. Sum of every list will be m, which will be a prove that she knows the solution. However she will mix the numbers in every list, so he doesn't know the exact combination. She wouldn't tell him which list is a row and which is a column.
Victor will see 2n lists, where sum of every list is m. He can see that every number is twice in all the lists and that every list is different, which means that she knows the solution. However it wouldn't help him to find the solution.

Question 5.

(a) z_i can be expressed as $z_i = h(i)$, where $h(i) = f(i) + g(i)$.
$f(x) = x + \sum_{j=1}^{t-1} a_j x^j (mod\ p)$
$g(x) = y + \sum_{j=1}^{t-1} b_j x^j (mod\ p)$
$h(x) = z + \sum_{j=1}^{t-1} (a_j + b_j) x^j (mod\ p)$, where $z = x + y$
h(x) is not polynomial of degree $t-1$ if $a_{t-1} + b_{t-1} \equiv 0\ mod\ p$ and therefore $t' < t$.

(b) $t' = t$ only when $a_{t-1} + b_{t-1} \not\equiv 0\ mod\ p$.

Question 6.

(a) Victor would have at the end of every round u, c, z.

Victor accepts with:

$b^z = u * a^c \mod p$

$b^{r+c*x} = b^r * b^{x*c} \mod p$

$r + c * x = r + c * x \mod p$

(b) Victor can only change r in this protocol.

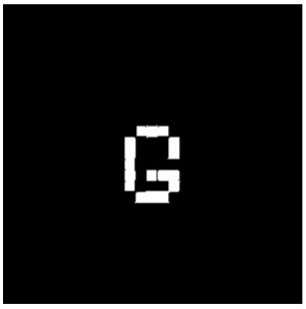
He can e.g. precompute a large number of results for $k = b^y \mod p$, where $y < p$.

Then he sets $c = 1$ every time. Because there is $p/2$ rounds, it is probable, that in some point, he find $u = k$. Therefore, he found r for that specific round.

Now, he can compute $z = r + c * x$, because he know z, r, c.

Question 7.

Using script to xor pixels in given qr codes I have found:



Question 8.

Inside the dot at the end of the text there is text: microdot

Figure 2: Zoomed at the dot