Question 1.

(a) The scheme is $(5, 3)$, so $n = 5$ and $t = 3$. The polynomial will be quadratic. $a_1 = 3^{394097} \mod 101021 = 12117$, $a_2 = 5^{394097} \mod 101021 = 30858$ and $S = 394097$. The polynomial is $a(x) = a_1x + a_2x^2 + S = 12117x + 30858x^2 + 394097 \mod 567997$.

Using the polynomial we can calculate shares for each of the five users: $(1, 437072)$, $(2, 541763)$, $(3, 140173)$, $(4, 368296)$ and $(5, 90138)$.

(b) The three shares create a system of three equations with three variables:

$$a_1 + a_2 + S = 438827, \tag{1}$$

$$2a_1 + 4a_2 + S = 273042, \tag{2}$$

$$3a_1 + 9a_2 + S = 133864. \tag{3}$$

After solving the system we get $S = 63222 \mod 567997$.

Question 2.

(a) $\alpha_1 = 113$
$\alpha_2 = 169$

v = 83 mod 311

Verification is done by: $\gamma = \alpha_1^{y1} * \alpha_2^{y2} * v^r$ mod p

1) (20, 27,(18, 29)):

$\gamma = 113^{18} * 169^{29} * 83^{27}$ mod 311 = 15 * 250 * 243 = 20 mod 311 -> correct transcript

2) (20, 4,(18, 26)):

$\gamma = 113^{18} * 169^{26} * 83^{4}$ mod 311 = 15 * 195 * 32 = 300 $\neq$ 20 -> not correct transcript

3) (24, 4,(15, 26)):

$\gamma = 113^{15} * 169^{26} * 83^{4}$ mod 311 = 250 * 195 * 32 = 24 -> correct transcript

4) (24, 27,(15, 29)):

$\gamma = 113^{15} * 169^{29} * 83^{27}$ mod 311 = 250 * 250 * 243 = 126 $\neq$ 24 -> not correct transcript

(b) $y_1 = k_1 + a_1 *$ r mod q

$y_2 = k_2 + a_2 *$ r mod q

I took two correct transcripts: (20, 27,(18, 29)) and (24, 4,(15, 26)) and decided to try both possibilities:

1) Transcript (20, 27,(18, 29)) was first and (24, 4,(15, 26)) was second:

I got these 4 equations by using $(k_1)_2 = 3 * (k_1)_1 + 4$ mod 31 and $(k_2)_2 = 5 * (k_2)_1 + 3$ mod 31:

18 = $k_1 + a_1 *$ 27 mod 31

15 = 3 * k_1 + 4 + a_1 * 4 mod 31

29 = $k_2 + a_2 *$ 27 mod 31

26 = 5 * k_2 + 3 + a_2 * 4 mod 31

From the first two:

k_1 = 18 - 27 * a_1 mod 31 -> 15 = 3 * (18 - 27*a_1) + 4 + 4 * a_1 mod 31

11 = -81 * a_1 + 4 * a_1 + 54 mod 31

11 = 16 * a_1 + 23 mod 31

19 = 16 * a_1 mod 31

a_1 = 19 * 16^{-1} mod 31 = 19 * 2 mod 31 = 7

From the second two:

k_2 = 29 - 27 * a_2 mod 31 -> 26 = 5 * (29 - 27 * a_2) + 3 + 4 * a_2 mod 31

2 = 24 * a_2 mod 31

a_2 = 2 * 24^{-1} mod 31 = 2 * 22 mod 31 = 13

2) Transcript (24, 4,(15, 26)) was first and (20, 27,(18, 29)) was second:

By similar computations I got:

15 = k_1 + 4 * a_1 mod 31

18 = 3 * k_1 + 4 + 27 * a_1 mod 31

18 = 3 * (15 - 4 * a_1) + 4 + 27 * a_1 mod 31 -> a_1 = 0

26 = k_2 + 4 * a_2 mod 31

29 = 5 * k_2 + 3 + 27 * a_2 mod 31

29 = 5 * (26 - 4 * a_2) + 3 + 27 * a_2 mod 31 -> a_2 = 25

But I didn't even need to control the second case, because I can verify that a_1 = 7 and a_2 = 13 is right solution from:

v = $\alpha_1^{-a1} * \alpha_2^{-a2}$ mod p = $113^{-7} * 169^{-13}$ mod 311 = $7^{-1} * 91^{-1}$ mod 311 = 89 * 270 = 83 -> so these recovered keys a_1, a_2 are correct (the inverses can be computed by ext.eucl.algorithm).

Question 3.

Lets denote treshold as T, F is field marshal, G is general, C is colonel and M is major.
From assignment we know, that:
$F \geq T$
$3G \geq T \rightarrow G \geq \frac{T}{3}$
$2G + 5C \geq T \rightarrow 2 * \frac{T}{3} + 5C \geq T \rightarrow C \geq \frac{T}{15}$
$G + 7C + 15M \geq T \rightarrow \frac{T}{3} + 7 * \frac{T}{15} + 15M \geq T \rightarrow M \geq \frac{T}{75}$

Now for condition that any number of Colonels or Majors cannot launch the missile without General it must holds:
$50 * C + 100 * M < T$
but we get that:
$50 * \frac{T}{15} + 100 * \frac{T}{75} < T$
Which is obviously not true. Thus there is no single instance of a threshold secret sharing scheme that would satisfy all conditions.

Question 4.

(a)

No. Because when we take second and third column combination (2,2) appears 3 times and repetition count is 1.

(b)

i.

OA(2,7,2)
This array exists and here is an example:

0	0	0	0	0	0	0
0	0	0	1	1	1	1
0	1	1	0	0	1	1
0	1	1	1	1	0	0
1	0	1	0	1	0	1
1	0	1	1	0	1	0
1	1	0	0	1	1	0
1	1	0	1	0	0	1

ii.
OA(2,8,2)
Lets assume that such orthogonal array exists. Then it must hold
$\lambda \geq \frac{k(n-1)+1}{n^2}$
But in our case
$2 \geq \frac{8(2-1)+1}{2^2}$
and
$2 < \frac{9}{4}$
Thus there is no such orthogonal array.

Question 5.

(a) We can see that the verification will succeed for any b[1]:

$$\text{Alice sends: } y = rs^b \mod n$$
$$\text{Bob verifies: } xv^b = r^2(s^2)^b = (rs^b)^2 = y^2 \mod n$$

In case Bob sends the challenge $b = 2$ to Alice, she calculates $y = rs^2 \mod n$ and sends it to Bob. Since $v = s^2 \mod n$, Alice opens her commitment by revealing r, as Bob can calculate $r = yv^{-1}$. However, because of the assumption that it's computationally infeasible for Bob to find $\sqrt{v} \mod n$, s remains secret.

(b) If Eve can guess the challenge, she can calculate her commitment for $b = 0, 1$ as described in the slides, either by sending $x = r^2$ for $b = 0$ or $x = r^2v^{-1}$ for $b = 1$, then she responds with $y = r$ to Bob's challenge.

[1]Of course Bob does not need to know r, he just needs to know $x = r^2$, which Alice sends first as her commitment.

In case the challenge is $b = 2$, she sends her commitment as $x = r^2$ and as a response she sends $y = rv$, since $s^b = s^2 = v \mod n$. Here is how Bob correctly verifies her response:

$$\text{Eve sends commitment: } x = r^2 \mod n$$
$$\text{Bob sends challenge: } b = 2$$
$$\text{Eve sends response: } y = rs^2 = rv \mod n$$
$$\text{Bob verifies: } xv^b = r^2v^2 = (rv)^2 = y^2 \mod n$$

As the part (a) suggests, in this case she can also fool Bob if he sends the challenge $b = 0$, as she can just send $y = r$ as a response, which Bob verifies as $y^2 = xv^0 = r^2$.

Actually we can generalize this method for all possible values of b. Eve just needs to correctly guess if the challenge will be odd or even. Then she calculates $x = r^2$ for even b or $x = r^2v^{-1}$. After Bob responds with his challenge, she calculates her response $y = rv^x$, x being the number of even/odd numbers between 0 and b. So in case of even numbers, $x = \frac{b}{2}$, in case of odd numbers $x = \frac{b-1}{2}$.

For example, this is how it works for $b = 3$:

$$x = \frac{3-1}{2} = 1$$
$$\text{Eve sends commitment: } x = r^2v^{-1} \mod n$$
$$\text{Bob sends challenge: } b = 3$$
$$\text{Eve sends response: } y = rv^x = rv^1 \mod n$$
$$\text{Bob verifies: } xv^b = r^2v^2 = (rv)^2 = y^2 \mod n$$

For $b = 5$, her response would be $y = rv^2$ and the verification would be $xv^5 = r^2v^{-1}v^5 = r^2v^4 = y^2$.

This implies that the probability of fooling Bob is still 2^{-t} for t rounds, therefore Alice and Bob did not improve the security of this protocol.

Question 6.

Let A be an arbitrarily chosen $t-(q,n,1)$ orthogonal array. Using q^t rows of A as codewords of our new code, we construct code C. We prove that code C is a q-ary maximum distance separable [n,k]-code as follows. Suppose that $d(C) \leq n-t$ (and therefore that C is not a maximum distance separable code with aforementioned properties). Then there exist two codewords $x, y \in C$ such that they match on at least t columns. Within these columns the rows of x, y are the same which is a contradiction since we have constructed the code from an orthogonal array with $\lambda = 1$.

Now we show that the other side of the equivalence holds. Let C be a q-ary maximum distance separable [n,k]-code. $M = q^{n-d+1}$. We construct a $M \times n$ array A by taking the codewords of C to be the rows of A. Consider the restriction of A to any subset of $n-d+1$ columns. The q^{n-d+1} $(n-d+1)$-tuples obtained from the rows of A must all be different (otherwise two codewords would be less than d bits apart). Since there are q^{n-d+1} different $(n-d+1)$-tuples, every possible $(n-d+1)$-tuple occurs in exactly one row of A in this restriction. Since this holds for all the possible subsets of $n-d+1$ columns of A, we have shown that A is a $(n-d+1)-(q,n,1)$ orthogonal array.