Question 1.

Coin-flipping protocol for p=43, q=71, x=123.

(i) Alice chooses primes $p = 43, q = 71$, keeps them secret and sends Bob $n = p * q = 3053$.

(ii) Bob chooses random $x \in \{1, \ldots, \frac{n}{2}$; x=123. Now he computes $y = x^2 \mod n = 123^2 \equiv 2917 \mod 3053$ and sends y to Alice and tells her to guess x - if she guesses the correct x, she will win.

(iii) Alice now computes the square roots with the knowledge of p and q. We can use the property of the two primes, that actually are Blum primes (equal 3 modulo 4).

$$x = \pm y^{\frac{p+1}{4}} \mod p$$

$$x = \pm y^{\frac{q+1}{4}} \mod q$$

$$x = \pm 2917^{\frac{43+1}{4}} \mod 43 \equiv \pm 6 \mod 43$$

$$x = \pm 2917^{\frac{71+1}{4}} \mod 71 \equiv \pm 19 \mod 71$$

Now we can use Chinese remainder theorem to compute the four square roots modulo p. The inverse number modulo p can be computed using Extended Euclidean algorithm.

$$m_1 = 43, m_2 = 71, M = m_1 * m_2$$

$$M_1 = M/m_1 = 71, M_2 = M/m_2 = 43$$

$$N_1 = M_1^{-1} \mod m_1 = 71^{-1} \equiv 20 \mod 43$$

$$N_2 = M_2^{-1} \mod m_2 = 43^{-1} \equiv 38 \mod 71$$

$$x \equiv \pm 6 * 71 * 20 \pm 19 * 43 * 38 \mod 3053$$

So the four square roots modulo n are 2930, 1898, 123, 1155. From these, Alice chooses randomly one of the two smallest (as the two largest are just n minus one of the two lowest x) and tells Bob which one she chose, for example by saying the position and value of the leftmost bit, on which the two smallest x differ.

(iv) Bob tells Alice if she is right or wrong and therefore the result of the coin-flipping. If there are some doubts, Alice reveals p and q and Bob reveals x.

Question 2.

The protocol starts with Alice choosing a random input $x \in \{0,1\}^n \to \{0,1\}^n$. Alice then computes $f(x)$ and sends it to Bob. Bob now guesses the parity of Alice's input and tells Alice. If he guesses correctly, Bob wins, otherwise Alice wins. Bob can verify the result by making Alice send him the input x.

This protocol is secure. Since the function is bijective, there's no other $y \neq x$ such that $f(x) = f(y)$ and thus Alice commits to her x by sending $f(x)$ and cannot change her choice later to cheat. On the other hand, since no information can be gained about the input of function f from its input, Bob has no way of computing the parity of x from $f(x)$.

Question 3.

(a) Alice can easily reveals r and x. Bob checks if $g^r h^x \mod p$ is equal to the message, which he received in the commitment phase.

(b) **Binding is computational**. Suppose it is computationally feasible to compute $r, r' \in \mathbb{Z}_p^*$, such that commit(r,x) = commit(r', x'). That means that

$$g^r h^x = g^{r'} h^{x'} \mod p$$

$$g^r g^{kx} = g^{r'} g^{kx'} \mod p$$

$$g^{r+kx} = g^{r'+kx'} \mod p$$

$$r + kx = r' + kx' \mod q$$

$$kx - kx' = r' - r \mod q$$

$$k(x - x') = r' - r \mod q$$

$$k = \frac{r' - r}{x - x'} \mod q$$

So to be able to open the commitment in both ways is as hard as calculating the discrete logarithm problem for h with basis $g \in \mathbb{Z}_p^*$.

Hiding is information theoretic. It can be simply seen by the fact that the distribution $g^r h^x$ is independent of x, so g^r and $g^r h$ are statistically indistinguishable, because the value r is random value.

(c) It doesn't help Bob. Knowledge of k doesn't help him. For every x' there exists a unique value r' such that

$$r' = k(x - x') + r \mod q$$

Without further knowledge of r or x, every pair (r', x') that satisfies the commitment is equally likely. So if Bob only knows k he cannot deduce any information from the commitment.

(d) She can cheat. Let's assume that she commits with $g^r h^x \mod p$. Then she can cheat by calculating r' for any x' and revealing (r', x') instead of (r, x).

Question 4.

Alice calculates all $g(x, y_1), g(x, y_2 2), \ldots, g(x, y_{|y|})$, expresses them in binary and inputs $g(x, i)$ as the i-th input into the *1-out-of-k* OST protocol. Bob upon inputing y learns $g(x, y)$ and communicates it to Alice. Because OST protocol does not reveal x to Bob, all he can learn about x is can be deduced from $g(x, y)$. Reversely, since OST protocol does not reveal anything about Bob's choice, all Alice learns about y can be deduced from $g(x, y)$. This is therefore an instance of a secure function evaluation for arbitrery function g.

Question 5.

We will provide a physical (non-cryptographic) zero-knowledge protocol for killer sudoku, which combines elements of sudoku and kakuro. Both of them have rather simple zero-knowledge protocols, so we will just combine them. We need a rather large amount of dichromatic cards (e.g. red and black) and envelopes.
If envelope represents a number k, then it has inside k red cards and $9 - k$ black cards. Black card are there so the envelopes appear indistinguishable.

Setup:
9×9 grid: Each cell has an envelope corresponding to the solution of the cell.
Cages: Each cage needs to have assigned a set of envelopes representing the missing (not in the solution) numbers.

Protocol:

(i) To verify row, column or nonet (3×3 grid), Peggy takes the 9 envelopes from the structure based on Victor's choice, shuffles them in a way they cannot be tampered with (this may require a trusted 3rd party or other mechanisms ensuring honesty or we'll just assume an almighty abstract shuffle functionality exists). Shuffled envelopes are given to Victor.

(ii) Victor opens each envelope and verifies that all 9 envelopes contain numbers from 1 to 9.

(iii) To verify a cage (unique numbers) of Victor's choice, Peggy takes the envelopes from the given cage and also envelopes assigned to the cage with missing numbers. Envelopes are shuffled and given to Victor.

(iv) Victor opens each envelope and verifies that all 9 envelopes contain numbers from 1 to 9.

(v) To verify a cage (sum) of Victor's choice, Peggy takes the envelopes from the given cage. Envelopes are opened face down and card are shuffled and given to Victor.

(vi) Victor then verifies that the number of red cards corresponds to the sum of the cage.

After n rounds Victor should have enough statistical evidence, that Peggy indeed knows the solution.

Question 6

Under the assumption that there exists a statistically binding and computationally hiding bit commitment scheme, there exists a zero-knowledge proof for any NP language (Goldreich, Micali, Wigderson, 1991).

Hamiltonian path is also known to be an NP-complete problem, therefore it has a zero-knowledge protocol to verify the solution.

Question 7.

Let's assume that we have identical container for each grade. We arrange them in a line, and write labels with grades in front of each container, one for each container. I put a folded slip of paper saying Yes in the container of the grade, which I received. I put also folded slip of paper saying No in the other containers, that represent the other grades. My colleague does the same. Then we remove the labels, and shuffle the containers at random. Then we look inside the containers to see if one of them contains two slips saying Yes. Inspiration is from Solution 10: click here.

Question 8.

There is a message hidden in a microdot in the colon following "Lewis Carroll" with a text `steganographia` in Greek letters $\sigma\tau\epsilon\gamma\alpha\nu o\gamma\rho\alpha\phi\iota\alpha$.