ANSWERS TO THE EXAM QUANTUM INFORMATION, 4 NOVEMBER 2024

each item gives 2 points for a fully correct answer, grade = total $\times 9/24 + 1$

1. *a)* You need N single-qubit Hadamard gates, one acting on each qubit.
   b) If $f(x) = f(y)$ for some pair $x \neq y$, then the operation $|x\rangle \mapsto |f(x)\rangle$ is not invertible, hence it cannot be unitary.
   c) Bob is right. Alice is wrong because the operation $|x\rangle|0\rangle \mapsto |x\rangle|x\rangle$ does not copy the superposition $(|x\rangle+|y\rangle)|0\rangle \mapsto |x\rangle|x\rangle+|y\rangle|y\rangle$ [the copy would be $(|x\rangle + |y\rangle)(|x\rangle + |y\rangle)$].

2. *a)* $\rho_A = 2^{-1}|\uparrow\rangle\langle\uparrow| + 2^{-1}|\downarrow\rangle\langle\downarrow|$ and $S_{\rho_A} = 1$.
   b) same as in a)
   c) the pure state is entangled, it does not factor into a product state (concurrence = 1); the mixed state density matrix is the sum of two pure state density matrices which each represent a factored state, so it is not entangled; note that the von Neumann entropy cannot distinguish entangled or non-entangled states.

3. *a)* $\text{CNOT} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.
   b) the entanglement operation transforms $|\psi\rangle\,|\uparrow\rangle$ into $2^{-1/2}\,|\uparrow\rangle\,|\uparrow\rangle + 2^{-1/2}\,|\downarrow\rangle\,|\downarrow\rangle$; before the entanglement operation $\rho_A = |\psi\rangle\langle\psi|$; after the entanglement operation, $\rho_A = 2^{-1}\,|\uparrow\rangle\langle\uparrow| + 2^{-1}\,|\downarrow\rangle\langle\downarrow|$.
   c) the control qubit is only unchanged as a result of the CNOT gate if it is in one of the two basis states $|\uparrow\rangle$ and $|\downarrow\rangle$, not if it is in a superposition of these two states.

4. *a)* Alice tells Bob the results of her coin tosses, one by one; Bob then knows in which basis to measure the qubits, in order to obtain the same bit string as Alice.
   b) The random bit string can be added bitwise by Alice to the string that encodes the information. The resulting bit string can then be communicated to Bob in a nonsecure way, who will subtract the shared code to recover the information.
   c) Alice and Bob can disclose a part of their shared code and check if the bits are indeed the same. If the qubits were measured by an adversary before reaching Bob, there will be errors with high probability. It is essential for this to work that Eve can only find out the basis in which the qubits were prepared *after* they were received by Bob, otherwise she could measure the qubits in that basis before sending them on to Bob, and they would not be disturbed.