COSC412 Assignment 2:

Question 1:

Using the given values and attached java file difhel.java, the shared secret (g^{ab}) is: 3505815610982601623.

This is calculated by Alice picking a random number labelled a(1 < a < p-1) then performing g^a mod p (mod is modulus).

The same occurs for bob but he uses b as an exponent (g^b mod p).

Alice and Bob send each of their results to each other (A will represent Alice's results and B will represent Bob's result).

Alice will then compute B^a mod p and Bob will compute A^b mod p (since they received each others result). Due to the rules of exponentiation each of these computations work out to be g^{ab} giving both Bob and Alice the same result (a shared secret).

By hashing this value, a key can be gained.

This is very secure because neither Bob or Alice share their random values so even if A or B is intercepted, it is hard to compute the other random value using A and B to get the shared secret result.

Question 2:

A:

The message is: 21036236540192578. This was found using the attached java file rsa_solver.java.

The key to finding this is too figure out the two primes p and q. Once these primes are known, finding the secret key d is trivial since d * e = 1 (mod (p-1)(q-1). Since e is known and if p and q is known, d can be calculated and then c^d can be done to get the message (c = cipher text).

Since N is a product of p*q and both p and q are primes, we know that there is only one possible (p, q) set that will form N as a product and form the correct message from the cipher text. Therefore, taking N and forming every possible prime number that N is divisible by will allow one to form all the possible prime sets used. Then for each prime set we assume it is correct and calculate the secret key d as long as for each prime key set attempted, the greatest common denominator between e and (p-1)(q-1) is 1. If 1 is not the greatest common denominator then this prime key set cannot be the primes we are after due to the fact that e shares no common factors with (p-1)(q-1).

Now taking the d value calculated from the assumed prime key set we can calculate a possible correct message. To check if this message is correct, we only need to encrypt the possible correct message to form a cipher text and compare this to the known cipher text. If the known cipher text and calculated cipher text match, then the possible correct message is correct, and we found the correct prime numbers. This process gets repeated for every possible prime key set until the correct message is found.

B:

Overall the Lenstra paper showed the given flaw in the RSA algorithm but the root of that flaw was that there was not enough entropy (uncertainty) in the prime keys being generated for the RSA algorithm. Lenstra at the time found the RSA algorithm to be secure and good if it was implemented correctly where the unsecure RSA implementation cases where they found repeated prime keys was due to a lack of entropy in key generation.

The given solution in the Lenstra paper is true and is a solution because it acts to ensure enough prime key entropy for each key in relation to each other. Given one prime key, use the given equation and you will gain another prime key to form the prime keys to use for RSA. The prime key set ensures enough entropy to make brute force attacks difficult (hopefully futile and practically impossible) and therefore ensures the security of RSA (RSA will be implemented correctly) and therefore lower the risk of sharing prime keys with another RSA implementation since the idea of this equation is to avoid multiple secrets (sharing prime keys).

Question 3:

Quantum computing is the future for specific purposes but not for every computing application. This is due to two key properties of quantum computing; the ability for data to be in multiple states at once and the possibility of entanglement.

The first key component is very beneficial and decides a lot of what quantum computing will be good for, in a simple explanation it allows multiple ideas to be explored at once rather than the serial nature of current computers. Imagine two computers trying to explore a maze with one computer being your standard everyday computer and one being a quantum computer. The standard computer as you expect will explore a single path at a time and eventually find the exit while a quantum computer can explore multiple paths at once.

This is due to the way quantum computers handle data at the lowest level where in a standard computer a piece of data (a bit) can only be in one state at once and can hold only two different states. In quantum computers a single piece of data can hold multiple states due to super positioning, this allows data in quantum computers to be used in different ways at once like exploring multiple paths in a maze in parallel. By pairing qubits (how a quantum computer represents data) with more qubits, you increase the amount of possible states in an exponential manner, therefore significantly increasing the computing power of a quantum computer with ever qubit.

The second key component is the possibility of harnessing entanglement where entanglement is when two or a group of particles become entangled. When two particles become entangled they then have direct effects on each other regardless of the distance between them. This means that if given an entangled particle pair, you could change one particle and directly affect the other giving a form of data transfer over possibly large distances. This component itself if harnessed would be a revolution in the way data is moved since data transfer is needed in every computing device.

Overall quantum computing is going to a big part of the future but not for every part of computing. In a sense it will be another tool to be used by the technology industry, a tool with specific uses where this tool has significant advantage over the current tools we have today. When this tool is developed enough it is going to advance specific sectors of the industry significantly faster than how they are advancing now or at least keep advancement going as the improvement in standard computing continues to slow. Therefore, quantum computers will not replace the everyday computer but instead will be used as specialised tools for significant benefit meaning that investing into this growing section will ensure access and involvement in the future of the technology industry.

Reference articles read to give further knowledge:

Commercialize quantum technologies in five years

Here’s What a World Powered by Quantum Computers Will Look Like

Early quantum computing investors see benefits

The Commercial Prospects for Quantum Computing