Assignment 4
Gunnar Yonker

1.

a. To launch a man-in-the-middle attack against someone in the anonymous Diffe-Hellman exchange scheme, a couple steps need to take place. First the attacker will intercept the initial communication between the two different parties that are attempting the exchange using the anonymous DH protocol. The attack will then generate a separate key exchange with each party, so if A and B are communicating with each other and C is the attacker. C will generate a key with A and C will also generate a key with B. This way A will think they are communicating with B, but it's actually C and vice versa. The attacker will then relay the messages between the two parties as the man in the middle. This works because each party thinks that they are communicating with the other party. The attacker is able to then read all of the messages being exchanged and modify any of the messages if they so choose to. This is all possible because the attack was able to establish a shared secret between each of the parties.

b. The Elliptic Curve Diffe-Hellman (ECDH) key exchange would be a viable advanced version of the exchange scheme that could further defend against the man-in-the-middle attack. The ECDH key exchange scheme is an asymmetric cryptography scheme that uses the elliptic curves to perform the key exchange. This provides stronger security than the basic key exchange. In the ECDH key exchange the two parties agree on an elliptic curve and a base point on the agreed upon curve. Each of the parties will then generate a private key which is a random number between 1 and the order of the base point, and then use that private key to generate a public key. Each party will use their own private key and then use each other's public key to create a shared secret. The key sizes are relatively short, but still provide a high level of security. This scheme defends against a man-in-the-middle attack because it is able to include a key authentication step where the two parties authenticate the other's public keys using a certificate authority. This ensures that each party is exchanging their keys with their intended target.

2.

a. One of the most important advantages of ECC compared to RSA is that it has a smaller key size with the same level of security. This leads to advantages such as having faster computations and using less resources. Overall, ECC is more efficient than RSA by having a smaller key size that offers the same level of security.

b. ECC's security strength does not rely on the difficulty of factoring large number. It relies on the difficulty of solving the elliptic curve discrete logarithm problem. This process involves finding a random integer k such that $kP = Q$. In this equation P is a fixed point on the curve and Q is another point on the curve. ECC's security strength also relies on the size of the key.

c. ECC can be used in a situation where secure communication is needed between two parties such as sending secure emails. Since ECC has a smaller key size and is thus quicker so it could be used for secure email communications as a practical use.

ECC can also be used to generate digital signatures which can be used to verify the authenticity of digital documents. Again, this is a practical use due to the smaller key size and more efficient performance with less resources over a tool like RSA.

Assignment 4
Gunnar Yonker

3.

a. A should use B's public key to encrypt the message. Then B receives the encrypted message and uses their private key to decrypt and read the message.

b. A should use their private key to sign the message. Then B is able to use A's public key to verify the signature and authenticate that the message was actually sent by A and has not been altered/modified during the transmission.

4.

A cryptographic hash function can convert a large piece of information into a fixed length hash code by first taking the plaintext input message and breaking it up into smaller blocks of fixed size. On each one of these blocks there are mathematical operations that take place and then produce a unique output for each block. Each of these blocks are then reassembled and further processed which then results in a hash code representing the entire input message as a fixed message length. SHA-256 and MD5 are common cryptographic hash functions. By breaking the input message into smaller blocks, they can then be encrypted into unique fixed size outputs which is what makes this a secure process. Then each one of those fixed size outputs can be reassembled to have a fixed size output for the full input message.

5.

(1) The transaction output will have one output to Charlie and then one output for the leftover (1 bitcoin), the leftover will also be used as the transaction fee for the miner that confirms the transaction. Bob will need to create a new transaction to send the leftover (1 bitcoin) to himself or whatever recipient he chooses.

(2) Yes, this is doable for Alice. The first transaction will be to pay Bob 2 bitcoins and the second transaction will be to pay Charlie 3.98 bitcoins. The leftover amount will be used as the transaction fee. This is doable for Alice as long as she does not exceed her total of 6 bitcoins from her previous transaction and has available leftover bitcoin to use for the transaction fees.

(3) Alice is unable to void the transaction once it has been confirmed, it cannot be voided or canceled. The bitcoins are owned by the public address that Bob has given to Alice. They are owned by the address, but since Bob cannot access them, it is considered a "dead" key. However, there is no way to undo the transaction, that is why it is important to triple check that the intended recipient is correct for cryptocurrency transactions.

(4) The longer of the two branches should be accepted. The longer of the two chains represents the most computational work and miners are rewarded based on the amount of work they contribute to the network. The longer branch is then considered the valid branch and the shorter other branch is discarded.

(5) For a miner to be rewarded they must solve a cryptographic puzzle called the proof of work algorithm. They are rewarded if they are the first miner to solve the puzzle and add a new block to the blockchain. The reward is the newly minted bitcoin and transaction fees. Over the years the rewards have decreased, originally the reward was 50 bitcoins per block, every 210,000 blocks the reward is halved. The current reward is 6.25 bitcoins per block successfully mined.