This is correct according to lecture notes about SET. Other sources on the internet does also confirm this. Also Mastercard, Visa, Microsoft, Netscape, and others seem to use SET with Netscape's Secure Sockets Layer (SSL), Microsoft's Secure dealings Technology (STT), and Terisa System's Secure machine-readable text Transfer Protocol (S-HTTP).

1p **A-7** Is SSL required in SET? Motivate your answer.

Since SET is a protocol that ensures that the payment information is protected on an application level, SSL is not needed to protect the payment information. On the other hand, the order information is not encrypted. If you want anonymity and protecting the payment information is a thing you might want, you should use SSL.

I assume you mean order information and misplaced it with payment information here, since the payment information is encrypted, and your previous sentence mentions order information

1p **A-8** How does the SET protocol provide non-repudiation?

By demanding that everyone involved in the purchase, the cardholder, the merchant and the payment gateway, has a certificate and a corresponding public and private key pair that they can use to sign messages.

This is correct according to lecture notes about SET. All parties involved uses certificates and key pairs in order to authenticate the transaction.

1p **A-10** What two general ways are there to enroll in VbV (3D Secure) and which would you say is better?

This is correct according to the lecture notes about VbV. You can either enroll through the banks own services, or through a first purchase that gives rise to a security vurnability.

You can do it during a purchase, known as Activation During Shopping (ADS). Or you do it beforehand using the banks own service, either on the web or in person.
ADS have a couple of weaknesses compared to doing it in a separate process. First you have to enter a password and a Personal Assurance Message in the midst of a payment, you may not be focused on choosing a good password and a message that you will remember. Another drawback is that a spoofing attack that imitates the fairly simple web page, as the 3D secure page where you sign up, might be easier than to spoof an entire bank web page. You could theoretically spoof the sign up page and then send a message that something went wrong and redirect to the real page. You will probably enter the same information again and then the attacker knows your password.

1p **A-15** When requesting a blind signature, why must Alice keep r secret?

This is correct according to the lecture notes about blind signatures. The purpose is to keep the anonymity of Alice, the random number keeps Alice's coin a secret from the bank, but can still validate it.

Because it is the random number that ensures that bank can't see the coin x, but still give h(x) a valid signature, if alice would not keep it a secret, the bank could trace the coin x back to alice and she would no longer be anonymous.

1p **A-25** In step 2 of the PayWord protocol in Section 5.1 of the lecture notes, can A = {M, w0, C}P RIU be replaced by A = {M, w0}P RIU , C ?

This is correct according to the lecture notes about PayWord, without including C in the hash chain it will be vulnerable to man-in-the-middle attacks.

I would argue that this system could be vulnerable to man in the middle attacks where you can change the information in certificate C as long as the PUBu in C stays the same, since the merchant can't verify the validity of C if it is not signed. The bank on the other hand can validate certificate C by knowing, what certificates it has signed and handed out, but then this would not be discovered until the merchant contacts the bank and make the macro transaction. This defeats the purpose by accumulating micro transaction in to a macro transaction, since the merchant would need to validate the certificate C with bank with every micro transaction.

This is correct according to lecture notes about Electronic Lottery Tickets, Universal Aggregation and Peppercoin. Further could have developed argument for psychological effects for the user and merchant, such as the user with ELT may feel tricked into paying for more eventhough in the end payments would even out. This doubt is avoided in Peppercoin.

1p **A-29** What is meant by a probabilistic payment? How does the Electronic Lottery Tickets scheme differ from Peppercoin from the user's perspective? How do they differ from the Merchant's perspective?

A probabilistic payment means that a macropayment will be made on a microtransacion based on a probability. This probability used in ELT defined by $s = \mu/y$ where μ is the payment amount in the microtransaktion and y is the value for a microtransaktion.
In ELT the user takes the risk of paying a fixed cost macro transaction every time they make a micro transaction which may result in the user paying for more than what they bought. In pepper coin the user can never pay more than they actually paid for since the bank will only transfer as much money as they have spent when a micropayments is made.
From a merchants perspective, the ELT will result in a more or less correct payment as long as you have a lot of purchases. When using peppercoin the payment to the merchant will always be correct when a macropayment is made and the bank takes the risk of having less money then what is actually correct.

1p **A-30** Compare the anonymity given by the untraceable E-cash scheme and Bitcoin.

This is correct according to the lecture notes about BitCoin and E-cash. Since there still is a middle-man in E-cash handling all transactions from an account it is almost impossible for complete anonymity. Compared to BitCoin where there is no middle-man and all transactions are public.

In the E-cash scheme you are completely anonymous when you do a payment since nowone can know that you withdrew that particular E-cash. When you do a withdrawal you are not anonymous since you have to tell the bank who you are because you actually withdraw money from a bank. In Bitcoin you are completely anonymous since the only identifier is your public key, and no entity knows that the key is connected to you (unless someone handles your bitcoin for you). But if your relation to the public key would be revealed all your transaction history will be revealed since every transaction is public. But for that information to be relevant, the identity of the public keyes you have made your payment to, would also have to be revealed, otherwise you could only see that you've made a payment to some arbitrary entity. But since the ability to make a payment is only connected to, owning a connected private key, you can argue that you have not always owned that private key.

1p **A-34** How is the difficulty in Bitcoin block hashing adapted so that it (almost) always takes about 10 minutes for the system to produce a new block, regardless of the computational power that enters the system?

This is correct according to lecture notes about BitCoin and other sources on the internet. Roughly every two weeks (corresponding to 2016 blocks) the difficulty level is evaluated. The demand is that the hash must be smaller than a set requirement.

They do it by choosing a number that the hash must be smaller than. Doing this instead of just demanding a specified amount of zeros at the start of the hash gives them more control since they can have a higher accuracy. They also check the past 14 days average time to see if they need to change the number.

8p/8p