Home Assignment 1

Part A

1p A-5 How does the Merchant verify the dual signature in SET?

This is correct according to the lecture notes about SET.

- The merchant verifies the dual signature using the order information (OI) and digested and signed payment information (PIMD). The OI is hashed and is sent as an authorization request to the Payment Gateway by the merchant. The sent message consists of an encrypted payment information, digested and signed payment and order information i.e. PIMD and OIMD, transaction ID and the Merchant's and Cardholder's certificate. The message is signed by the Merchant using a symmetric key, and encrypted using the Payment Gateway's public key.

  The Payment Gateway sends a request to the issuer for payment authorization, if the payment request goes through, payment authorization response is returned to the merchant, which in turn is encrypted using the merchants public key.

1p A-9 In 3D Secure, describe briefly what happens after the Merchant/MPI receives the PARes from the issuer.

This is correct according to the lecture notes about 3D Secure, 3.2.2 step 3 in the second main phase.

- The merchant verifies the signed Payment Authentication Response PARes sent from the issuer.

1p A-11 The acronyms ACS and ADS are both related to VbV (3D Secure). Explain them briefly.

This is correct according to the lecture notes about 3D Secure.

Prior using a card, the card has to be activated, Activation During Shopping (ADS) is a mechanism which is done as a first purchase using a program, in this case called Verified by Visa (VbV), to activate the card by answering a series of questions and then choosing a password for the card.

Access Controller Server (ACS) is an authenticating party on the issuer's side that authenticates the cardholder and provides digitally signed messages. The cardholder must be enrolled to VbV program in order to be authenticated.

1p A-14 The multiplicative property of RSA provides for blind signatures. What is meant by "the

multi- plicative property of RSA"?

This is correct according to the lecture notes about RSA's functionality in blind signatures.

By the multiplicative property of RSA is meant that the product of two ciphertexts is equal to the encrypted product of respective plaintexts.

$$(m_1 m_2)^e = (m_1^e)\,(m_2^e) \pmod{n}$$

1p A-16 In the DigiCash scheme, explain how Alice could trick the bank into signing something completely different than a coin, e.g., the message "The Bank should give 1000 SEK to Alice". How could such user misbehaviour be avoided?

This is correct according to the lecture notes about blind signatures for E-Cash. Worth mentioning is that the cut-and-choose technique requires that Alice has to reveal information about half of the computed values.

In the DigiCash scheme consists of three parties a bank, a payer and a merchant. The bank issues electronic cash to the payer and debits her account. Alice then transfers the money to the merchant, Bob and in turn deposits the money back in to the bank. The bank cannot trace that the coins belonged to Alice.

Alice could trick the bank using a blind signature, she lets the bank sign the electronic coin, but doesn't want to be traced back to her once Bob deposits the same coin. The misbehaviour can be avoided by cut-and-choose technique.

1p A-17 How can the cut–and–choose technique be used to make sure that identifying information is properly added into an untraceable coin?

This is correct according to the lecture notes about blind signatures with E-Cash using cut-and-choose technique. As mentioned, some information will be revealed using this technique.

When the users spends coins from the bank, each coin is represented by $2k$ quadruplets of random number (mod n) a_i, c_i, d_i, r_i . Each coin has an identifier ID and can be linked to its user during withdrawal.

The user then computes $B_i = r^3_i f(x_i, y_i) \bmod n$, which are then sent to the bank. The bank then chooses randomly picked k indices out of the $2k$, i.e.cuts-and chooses that a random half of the B_i correctly identifies the user.

1p A-20 How is Alice's identity revealed if she double spends a coin in the untraceable E-cash scheme?

This is correct according to the lecture notes about untraceable E-Cash.

When Alice purchases something from Bob she sends a signature S of the coins to be spent, which are computed using k quadruplets $a_i, a_i \oplus ID, c_i, d_i$. Bob then generates a random binary vector of length k , $z = (z_1,...,z_k)$ and sends it back to Alice, in order to verify the coin.

Alice then uses the indices that were used to generate the signature S, the indices are

numbered from 1 to k. For every indices *i*, in the given interval, Alice uses a set of rules to respond to Bob.

- If $z_i = 0$, Alice sends x_i , $a_i \oplus ID$, d_i
- If $z_i = 1$, Alice sends y_i , a_i,c_i, d_i

Bob then computes $f(x_i, y_i)$ for all given indices *i* in order to verify the signature. Bob cannot figure out the ID since he does not have the a_i and $a_i \oplus ID$ at the same time. Bob then sends the signature *S* and the random binary vector *z* and Alice's response to the bank. The bank verifies the signature and then credits Bob's account.

If Alice tries to double spend the coin with another merchant, the merchant will create another random binary vector z, which in turn will be sent to the bank. The bank will notice that the S has been used before and can therefore extract the ID by computing $a_i \oplus a_i \oplus ID$, since the bank has both a_i and $a_i \oplus ID$.

1p A-25 In step 2 of the PayWord protocol in Section 5.1 of the lecture notes, can

This is correct according to lecture notes about PayWord protocol. If C isn't part of the hash chain it will be vurneble to man-in-the-middle attacks.

$$A = \{M, w_0, C\}_{PRIU}$$

Be replaced by,

$$A = \{\{M, w_0\}_{PRIU}, C\}?$$

- No, the certificate C contains the name B and is signed using the user's public key. The certificate is vulnerable to replay attacks because it signed using the user's public key.

8p/8p