Home Assignment 1

Victor Englund, 8911212010

Complete the eight A-assignments below and solve them individually.

A-1 In EMV, SDA cards are cards that only support SDA data authentication. List some advantages and drawbacks of these cards compared to cards that support DDA. Can you find an attack that would work on SDA cards but not on DDA compatible cards?

A-2 Describe an attack that the *CVV1* code on a credit card prevents. Why is it not effective against skimming?

A-4 What is the difference between a three-party scheme and a four-party scheme for credit card payments?

A-6 In SET, why is the Payment Information first symmetrically encrypted and not immediately encrypted with the Gateway's public key?

A-13 What is the difference between *authorization* and *authentication* in VbV (3D Secure)?

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

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

A-22 Briefly explain the differences between session-level aggregation, aggregation by intermediation and universal aggregation.

Complete the four B-assignments below and solve them in groups of two students.

B-1 Implement the Luhn algorithm in your favorite language and use your implementation to verify the validity of a few actual credit card numbers. Can you build your own credit card number generator? What is the design rationale behind the Luhn algorithm? Would it be better or worse to use a hash function, i.e., to hash the 15 digits, take the result modulo 10 and use that as control digit? Motivate your answer! How is the CVV2/CVC2 checksum on the back of your credit card calculated? Can you build your own CVV2/CVC2 checksum generator?

B-2 MicroMint has the property that it is much cheaper (per coin) to generate many coins rather than just one or a few. How is this property achieved? Write a program that simulates the difficulty of producing MicroMint coins and present your findings appropriately. (See reference list in lecture notes for the MicroMint specification.) Hint: Don't make this more difficult than you have to.

B-3 Compare the security between SET and 3D Secure in terms of authentication, encryption, cardholder verification etc.

B-4 When the number of transactions in a Bitcoin block is very large, the Merkle tree can be used to prove that a specific transaction is in that block without the need of revealing the entire transaction set, thereby minimizing data transfer. Illustrate this and explain how the Merkle tree of a transaction set can be used to this end. How many hashes must be downloaded to prove that a specific transaction is in a given block with 2^{10} transactions?

Complete one out of the two C-assignments below and solve them in groups of two students.

C-1 Implement the coin withdrawal (the version with 2k quadruples) in the untraceable e-cash scheme given in the lecture notes.

- You may use a variant of RSA with easily manageable numbers.
- The data transfer can be simulated locally.
- The extended euclidean algorithm can be used to find the inverse of 3 mod n.
- The square-and-multiply technique can be used to efficiently compute the signature.
- Choose sensible functions f and h.

Summarize your implementation in a report. The exact layout of the report is up to you. Make sure that you pick all blinding values r_i such that $\gcd(r_i, n)=1$. Otherwise you will not be able to extract the real signature. You do not need to implement the connection between the bank and the user. Passing values inside your program is sufficient. Pick k appropriately.

C-2 There is a large number of mobile payment solutions that have been proposed. Give a broad overview of mobile payment solutions. Describe and compare a few of them in more detail, highlighting advantages and drawbacks. Use 2-4 pages. The number of points will be based on the amount of effort that you seem to have put into the report. More specifically, the originality of the text, the accuracy of the text, and your ability to make relevant comparisons and conclusions.