H1 A uppgifter

A2 Describe an attack that the CVV1 code on a credit card prevents. Why is it not effective against skimming?

Svar: CVV1 koden förhindrar att man noterar de synliga kortnumren och tillverkar ett eget eller kopierar karbonkopior av kortet.CVV1 koden lagra på en magnetremsa i "klartext" och kan därför lätt kopieras med rätt utrustning.

A5 How does the Merchant verify the dual signature in SET?

Svar: Handlaren har tillgång till Order information(OI), hashen av payment information(PIMD) dual signature(DS) samt kundens publika nyckel. DS tas fram genom att sammanfoga hasharna PIMD och OIMD, hasha resultatet och signera med kundens privata nyckel. Med den tillgängliga informationen kan handlaren återskapa hashen: $H((\text{PIMD}||H(OI))$ Till sist kontrollera med hjälp av kundens publika nyckel att resultatet stämmer med DS

A8 How does the SET protocol provide non-repudiation?

Svar: Transaktionen signeras med en privat nyckel som genom en publik nyckel kan kopplas till användaren.

A14 The multiplicative property of RSA provides for blind signatures. What is meant by ”the multiplicative property of RSA”?

Svar: Med den multiplikativa egenskapen hos RSA menas egenskapen att $(x_1x_2)^d = (x_1^d \bmod n)(x_2^d \bmod n)$ dvs produkten av två krypterade meddelande är lika med det krypterade resultatet av produkten av de två klartexterna.

A22 Briefly explain the differences between session-level aggregation, aggregation by intermediation and universal aggregation.

Svar: Session-level aggregation samlar transaktioner kopplade till en specifik handlare gjorda av en användare. Aggregation by intermediation är en lösning där en central instans agerar mellanhand och samlar betalningar gjorda av en användare. Debiteringen sker när användaren nått upp till en viss summa. Samma sak gäller fast omvänt för handlaren. Universal aggregation "samlar" universellt små transaktioner till större genom att använda mattemagi(sannolikhetslära). En viss andel betalningar debiteras aldrig och de som debiteras tar en större summa. övertid motsvarar den totala summan som debiterar de man faktiskt ska ha betalat.

A25 In step 2 of the PayWord protocol in Section 5.1 of the lecture notes, can

$$A \;=\; \{M, w_0, C\}PRI_U$$

be replaced by

$$A \;=\; \{\{M, w_0, \}PRI_U\}C \;?$$

Svar: Nej. C är ett certifikat och används för att koppla ihop den privata nyckeln med den publika nyckeln och verifera att den är godkänd av betalningstjänsten. En signatur genererad av den är helt meningslös då den inte kan användas till att verifierar någonting annat än att sändaren besitter det publika certifikatet.

A27 In the PayWord protocol, give the Bank’s algorithm for verifying how much money should be taken from the user’s account.

Svar:

1. handlaren skickar in användarens initial utfästelse(som innehåller w_0, payword kedjans rot och användarens signatur m.m) och det senast mottagna paywordet w_l Commitment
2. verifiera användarens initial utfästelse (signatur osv).
3. utför hashfunktionen h enligt nedan:
   (a) $\mathrm{h}(w_0) = w_1$
   (b) $\mathrm{h}(w_1) = w_2$
   (c) osv

   tills resultatet blir w_l
4. dra l enheter pengar från användarens konto och betala ut till handlaren.

A33 In Bitcoin, one transaction can list several outputs. The hash of the transaction must be well-defined, so the outputs must be ordered. Give another reason why these must be ordered.

Svar: input i en transaktion refererar till en output från en tidigare transaktion med outputens index.