Aufgabenblatt der Lernkontrolle: InfSi1_V08

Name der Lernkontrolle:	InfSi1_V08
Beschreibung:	Hashes und digitale Signaturen
Startzeitpunkt:	20. April 2016 09:26:00
Endzeitpunkt:	27. April 2016 09:26:00
Maximale Punktezahl:	50
Anzahl Fragen:	18
Anzahl eigene Teilnahmen:	1
Teilnehmer:	Rico Akermann (rakerman@hsr.ch)
Startzeitpunkt Teilnahme:	30. July 2016 09:17:56
Endzeitpunkt Teilnahme:	30. July 2016 09:59:38
Benötigte Zeit:	00:41:42
Punkte:	21/50 (42%)

Frage 1: Welche Aussagen treffen auf Password-Hashing Verfahren zu?

Richtige Antwort	Deine Antwort	Fragetext
O	◉	Das Hashing Verfahren soll möglichst schnell sein.
◉	O	Das Hashing Verfahren soll möglichst langsam sein.
O	O	Das Hashing Verfahren soll nicht bekannt sein.

Frage 2: Mit welchem Blockverschlüsselungsmode ist die MD/SHA-Hashbildung am ehesten vergleichbar?

Richtige Antwort	Deine Antwort	Fragetext
O	◉	ECB
◉	O	CBC
O	O	RSA

Frage 3: Mit welchem Begriff beschreibt man die Hash-Eigenschaft, dass zu einer vorgegebenen Meldung m_i keine andere Meldung m_j mit gleichem Hash-Wert gefunden werden darf.

Richtige Antwort	Deine Antwort	Fragetext
◉	◉	Preimage-Resistenz
O	O	Kollisionsfreiheit
O	O	Nicht-Umkehrbarkeit

Frage 4: Um einer Person eine signierte Meldung schicken zu können, brauche ich ....

Richtige Antwort	Deine Antwort	Fragetext
O	◉	den Public Key dieser Person
O	O	den Private Key dieser Person
O	O	meinen Public Key
◉	O	meinen Private Key

Frage 5: Hashes sind nicht zurückrechenbar

Richtige Antwort	Deine Antwort	Fragetext
◉	O	Richtig

O	◉	Falsch

Frage 6: Welche Eigenschaften gehören zu den drei wichtigsten Anforderungen an Hash-Algorithmen?

Richtige Antwort	Deine Antwort	Fragetext
✓	✓	Angemessene Geschwindigkeit
✓	✓	Kollisionsfreiheit
✓	✓	Das Verändern von einem Bit im Text sollte so viele Bits wie möglich im Hash verändern
✗	✗	Der Hash-Algorithmus soll mit Hardware realisiert werden können.

Frage 7: Welche Aussagen treffen auf die Integritätsprüfung durch den Empfänger einer Meldung mittels "Digitaler Signatur" zu?

Richtige Antwort	Deine Antwort	Fragetext
✗	✗	Sender und/oder Empfänger können die Meldung verändern ohne den Hashwert zu verändern.
✓	✓	Nur der Sender kann die Meldung verändern ohne den Hashwert zu verändern.
✗	✗	Der Empfänger kann die Echtheit der Meldung nur überprüfen, wenn er einen geheimen Schlüssel kennt.
✓	✓	Der Empfänger kann die Echtheit der Meldung überprüfen, wenn er den Public Key des Signierers hat.

Frage 8: Was versteht man unter einer "Rainbow Table"?

Richtige Antwort	Deine Antwort	Fragetext
◉	◉	Vorberechnete Tabellen, in denen Passwörter und deren Hashes abgelegt sind,
O	O	Tabellen die alle aktuellen Hashverfahren beinhalten
O	O	Eine Tabelle von Hashes, die besonders leicht zurückrechenbar sind
O	O	Eine Tabelle mit Passwörtern, die genau die gleiche Zeichenfolge wie deren Hashes haben

Frage 9: Sie erhalten eine signierte Nachricht, welche an mehrere Personen gerichtet ist. Sie möchten allen antworten. Welche Aussage trifft zu?

Richtige Antwort	Deine Antwort	Fragetext
✓	✓	Ich kann problemlos allen mit einer ebenfalls signierten Mail antworten.
✗	✗	Ich kann problemlos allen mit einer verschlüsselten Mail antworten.
✓	✗	Ich kann problemlos dem Absender der Mail mit einer verschlüsselten Mail antworten.
✓	✗	Ich kann nur denjenigen Personen verschlüsselt antworten, deren Zertifikat ich bereits habe.

Frage 10: Wie gross ist die maximal mögliche Meldungslänge für einen SHA-1-Hash von 160 Bit?

Richtige Antwort	Deine Antwort	Fragetext
O	O	2^160
◉	◉	2^64 - 1
O	O	160*160
O	O	unendlich viele

Frage 11: Welche Aussagen treffen auf die Integritätsprüfung durch den Empfänger einer Meldung bei "Keyed Hash" Systemen zu?

Richtige Antwort	Deine Antwort	Fragetext
✓	✗	Sender und/oder Empfänger können die Meldung verändern ohne den Hashwert zu verändern.
✗	✓	Nur der Sender kann die Meldung verändern ohne den Hashwert zu verändern.
✓	✗	Der Empfänger kann die Echtheit der Meldung nur überprüfen, wenn er einen geheimen Schlüssel kennt.

Frage 12: Bei welcher Organisation wurden die Public Key Cryptography Standards (PKCS) entwickelt?

Richtige Antwort	Deine Antwort	Fragetext
⊙	⊙	RSA
O	O	Symantec
O	O	ISO
O	O	IEEE

Frage 13: Ist es möglich, dass unterschiedliche Nachrichten gleiche Hashes ergeben?

Richtige Antwort	Deine Antwort	Fragetext
⊙	⊙	Ja
O	O	Nein

Frage 14: Geben Sie an, welches Abkürzungen von Hashverfahren sind.

Richtige Antwort	Deine Antwort	Fragetext
✓	✓	MD5
✓	✓	SHA
✗	-	RSA
✗	✗	DH
✓	✓	RIPEMD

Frage 15: Mit welchem Begriff beschreibt man die Hash-Eigenschaft, dass es nicht effizient möglich sein darf, zwei Meldungen m_x und m_y mit demselben Hash-Wert h=H(m_x)=H(m_y) zu finden.

Richtige Antwort	Deine Antwort	Fragetext
O	O	Preimage-Resistenz
⊙	⊙	Kollisionsfreiheit
O	O	Nicht-Umkehrbarkeit

Frage 16: Welche Hashverfahren sollten gemäss US CERT seit Ende 2008 nicht mehr verwendet werden?

Richtige Antwort	Deine Antwort	Fragetext
✓	✓	MD5
✓	✓	SHA-1
✗	✗	MD6
✗	✗	RIPEMD-160

Frage 17: Susanne hat ein Dokument digital signiert. Die Signatur von Susanne kann man mit folgenden Schlüsseln überprüfen:

Richtige Antwort	Deine Antwort	Fragetext
✓	✓	mit dem Public Key von Susanne
✗	✗	mit dem Private Key von Susanne
✓	✗	mit dem Public Key der Organisation, welche Susannes Public Key signiert hat
✗	✗	mit dem Private Key der Organisation, welche Susannes Public Key signiert hat

Frage 18: Was versteht man unter einer Kollision bei Hashes?

Richtige Antwort	Deine Antwort	Fragetext
⊙	⊙	Dass es mehrere Meldungen hat, welche auf den selben Hash abgebildet werden.
O	O	Dass die Hash-Funktion Fehler aufweist.
O	O	Dass der Hash nicht immer mit dem selben Algorithmus berechnet wird.

O	O	Dass Umlaute nicht korrekt gehasht werden.