Aufgabenblatt der Lernkontrolle: InfSi1_V07

Name der Lernkontrolle:	InfSi1_V07
Beschreibung:	Asymmetische Verschlüsselung
Startzeitpunkt:	12. April 2016 16:53:00
Endzeitpunkt:	26. April 2016 16:53:00
Maximale Punktezahl:	50
Anzahl Fragen:	21
Anzahl eigene Teilnahmen:	1
Teilnehmer:	Rico Akermann (rakerman@hsr.ch)
Startzeitpunkt Teilnahme:	28. July 2016 23:51:12
Endzeitpunkt Teilnahme:	29. July 2016 00:05:20
Benötigte Zeit:	00:14:08
Punkte:	14/50 (28%)

Frage 1: Welchen Teil des Schlüssels muss der Empfänger einer mit einem Public Key Verfahren verschlüsselten Nachricht für die Entschlüsselung verwenden?

Richtige Antwort	Deine Antwort	Fragetext
O	O	den Public Key des Empfängers
⊙	⊙	den Private Key des Empfängers
O	O	den Public und den Private Key des Empfängers
O	O	den Public Key des Senders
O	O	den Private Key des Senders

Frage 2: 33 mod (13) ist gleich

Richtige Antwort	Deine Antwort	Fragetext
⊙	⊙	7
O	O	6
O	O	20
O	O	5

Frage 3: Die heute bekannten Erfinder des ersten Public Key Verschlüsselungsverfahrens heissen ?

Richtige Antwort	Deine Antwort	Fragetext
O	O	Diffie, Hellman
O	⊙	Rivest, Shamir, Adleman
⊙	O	Ellis, Cocks, Williamson

Frage 4: Welche Aussagen treffen auf Hybride Verschlüsselungssysteme zu?

Richtige Antwort	Deine Antwort	Fragetext
✗	✓	sind sicherer als symmetrische Verschlüsselungssysteme
✓	✓	werden bei TLS/SSL eingesetzt
✓	✓	arbeiten mit Public Key und Symmetric Key Verfahren
✓	✗	werden bei der SMIME E-Mail-Verschlüsselung eingesetzt

Frage 5: Warum ist bei RSA die Verschlüsselung schneller als die Entschlüsselung?

Richtige Antwort	Deine Antwort	Fragetext
O	◉	Weil die Verschlüsselungsoperation (Verschlüsselungsformel) einfacher aufgebaut ist
◉	O	Weil der Exponent bei der Verschlüsselung typischerweise besonders günstig gewählt wird
O	O	Weil die Chiffrate typischerweise länger als die Meldungen sind
O	O	Weil Logarithmieren einfacher ist als Exponentieren

Frage 6: Welche sind Abkürzungen von Public Key Verfahren?

Richtige Antwort	Deine Antwort	Fragetext
✗	✗	AES
✗	✗	RC4
✗	✗	DES
✓	✓	RSA
✓	✓	ECC
✓	✗	DH

Frage 7: Welche Schlüssellänge ergibt beim RSA Public Key Verfahren etwa die selbe Sicherheit wie 128 Bit Schlüssellänge bei einem symmetrischen Verfahren?

Richtige Antwort	Deine Antwort	Fragetext
O	O	64
O	O	128
O	◉	256
◉	O	3072
O	O	15360

Frage 8: 33 mod (7) ist gleich

Richtige Antwort	Deine Antwort	Fragetext
◉	◉	5
O	O	2
O	O	3
O	O	1

Frage 9: Falls die Schlüssellänge von 56 auf 64 Bit erhöht wird, so gibt es ?

Richtige Antwort	Deine Antwort	Fragetext
O	O	8 mal mehr mögliche Schlüssel
O	O	64 mal mehr mögliche Schlüssel
◉	◉	256 mal mehr mögliche Schlüssel

Frage 10: In einem hybriden Cryptosystem mit n Teilnehmenden benötigt man ?

Richtige Antwort	Deine Antwort	Fragetext
◉	◉	n geheime Schlüssel
O	O	n(n-1)/2 gemeime Schlüssel
O	O	n^2 geheime Schlüssel
O	O	n(n-1) geheime Schlüssel

Frage 11: Welche Eigenschaften zeichnen symmetrische Verschlüsselungsverfahren gegenüber

asymmetrischen Verfahren aus?

Richtige Antwort	Deine Antwort	Fragetext
✓	✓	kürzere Schlüssel
✓	✓	einfachere Ver- und Entschlüsselung
✗	✗	kleinere Anzahl geheime Schlüssel bei mehr als 2 Teilnehmern
✗	✗	sind generell sicherer

Frage 12: Alice schickt Bob eine mittels Public-Key-Verfahren verschlüsselte Nachricht. Welchen Schlüssel muss Bob für die Entschlüsselung verwenden?

Richtige Antwort	Deine Antwort	Fragetext
O	O	seinen Public Key
◉	◉	seinen Private Key
O	O	den Public Key von Alice
O	O	den Private Key von Alice

Frage 13: Wie viele Primzahlen gibt es?

Richtige Antwort	Deine Antwort	Fragetext
O	O	endlich viele
◉	◉	unendlich viele

Frage 14: Welchen Teil des Schlüssels muss der Sender einer Nachricht zur Verschlüsselung mit einem Public Key Verfahren verwenden?

Richtige Antwort	Deine Antwort	Fragetext
◉	◉	den public Key des Empfängers
O	O	den Private Key des Empfängers
O	O	den Private Key des Senders
O	O	den Public Key des Senders

Frage 15: Um einer Person eine verschlüsselte Meldung schicken zu können, braucht man ...

Richtige Antwort	Deine Antwort	Fragetext
◉	◉	den Public Key dieser Person
O	O	den Private Key dieser Person
O	O	den Public und den Private Key dieser Person
O	O	den Public Key des Absenders der Meldung

Frage 16: Ein Schlüssel habe 512 Bit. Wie vielen möglichen Schlüsseln bzw. Binärkombinationen (Angabe als Dezimalzahl) entspricht das?

Richtige Antwort	Deine Antwort	Fragetext
O	O	10^512
◉	O	10^154
O	O	10^50
O	◉	10^1536

Frage 17: Welche Schlüssellänge ergibt beim Elliptic Curve Public Key Verfahren etwa die selbe Sicherheit wie 128 Bit Schlüssellänge bei einem symmetrischen Verfahren?

Richtige Antwort	Deine Antwort	Fragetext
O	O	64

O	O	128
◉	O	256
O	◉	3072
O	O	15360

Frage 18: Bei welcher Schlüssellänge erzielt RSA eine vergleichbare Sicherheit wie 3DES?

Richtige Antwort	Deine Antwort	Fragetext
O	O	112 Bit
O	◉	256 Bit
◉	O	2048 Bit
O	O	15360 Bit

Frage 19: Bei welcher Schlüssellänge erzielt RSA eine vergleichbare Sicherheit wie AES-256?

Richtige Antwort	Deine Antwort	Fragetext
O	O	256 Bit
O	O	512 Bit
O	O	2048 Bit
◉	O	15360 Bit

Frage 20: Welches ist die beste Art zur Gewinnung "echter Zufallszahlen"?

Richtige Antwort	Deine Antwort	Fragetext
O	O	Aufruf einer Pseudo-Random Generator Funktion
O	◉	Verwendung des Resulate von zufälligen Mausbewegungen
◉	O	Nutzung elektrischer Rauschsignale
O	O	Verschlüsselung eines Zeitstempels mit Verwendung eines geheimen Schlüssels

Frage 21: Die (multiplikativ) inverse Zahl von 5 mod(7) ist gleich ?

Richtige Antwort	Deine Antwort	Fragetext
O	O	1
O	O	2
◉	◉	3
O	O	4
O	O	4