evaexam		evasys

Bitte so markieren: ☐ ☒ ☐ ☐ ☐ Bitte verwenden Sie einen Kugelschreiber oder nicht zu starken Filzstift. Dieser Fragebogen wird maschinell erfasst.

Korrektur: ☐ ■ ☐ ☒ ☐ Bitte beachten Sie im Interesse einer optimalen Datenerfassung die links gegebenen Hinweise beim Ausfüllen.

Bitte ausfüllen (Die Angabe des Namens ist freiwillig.):

Vorname: _____

Nachname: _____

Für die eindeutige Zuordnung der Prüfung übertragen Sie bitte Ihre Prüfungsteilnehmer-ID gewissenhaft in die dafür vorgesehenen Felder. Alle Seiten sind vollständig individualisiert und nicht mit anderen Prüfungen tauschbar.

Matrikelnummer

0	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐

1. Mathematik

1.1 Welche Aussage über die sogenannte "Mitternachtsformel" ist korrekt? (1 Punkt)

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

☐ Nur wenn die Werte a, b und c vorliegen, kann die MItternachtsformel eingesetzt werden.
☐ Mit der Mitternachtsformel erhält man drei Lösungen.
☐ Die Mitternachtsformel ist eine Lösungsformel für quadratische Gleichungen.

1.2 Was ist richtig? (1 Punkt)

☐ 35 mod 4 = 32
☐ 35 mod 4 = 3
☐ 35 mod 4 = 8

2. Diffie-Hellmann-Verfahren

Anton und Berta wählen p=7 und g=4.

Anton wählt a=2 und berchnet A:=g^a mod p und sendet dies an Berta.

Berta wählt b=4 und berechnet B:=g^b mod p und sendet dies an Anton.

2.1 Anton errechnet: (1 Punkt)

☐ A = 6
☐ A = 4
☐ A = 2

2.2 Berta berechnet nun: (1 Punkt)

☐ A^B mod p
☐ B^a mod p
☐ A^a mod p

2.3 Was stimmt? (1 Punkt)

☐ Das D-H-Verfahren liefert einen veschlüsselten Text.
☐ Das D-H-Verfahren liefert Anton und Berta verschiedene aber passende Schlüssel.
☐ Das D-H-Verfahren ermöglicht den Einsatz des sicheren One-Time-Pad-Verfahrens.
☐ Diffie und Hellmann waren die ersten, die für Kryptografie Primzahlen und Modulo-Rechnungen einsetzen.