

FTK KLAUSUR WS22/23 1. TERMIN

Prüfer: Jürgen Fuß

Benutze für deine Antworten ausschließlich den Fragebogen. Vorder- und Rückseiten können benutzt werden. Dauer: 90 Minuten.
Mache bei Rechnungen deinen Rechenweg nachvollziehbar, gib bei Lösungen mit Computerunterstützung die eingegebenen Rechenschritte an.

1. (Restklassengleichungssysteme)

(a) (2 Punkte) Bestimme eine natürliche Zahl z , die das Restklassengleichungssystem

$$z = 164 \pmod{267}$$

$$z = 205 \pmod{287}$$

$$z = 163 \pmod{391}$$

erfüllt.

(b) (1 Punkt) Wie viele natürliche Zahlen mit höchstens 8 Dezimalstellen sind Lösungen des Restklassengleichungssystems

$$z = 1 \pmod{2}$$

$$z = 1 \pmod{3}$$

$$z = 1 \pmod{5}$$

$$z = 1 \pmod{7}$$

$$z = 1 \pmod{11}$$

$$z = 1 \pmod{13}$$

$$z = 1 \pmod{17}$$

$$z = 1 \pmod{19}$$

(Du brauchst die Lösungen nicht zu berechnen, du musst sie nur zählen.)

2. (RSA) Du verwendest RSA-Signaturen mit einer Schlüssellänge von 2048 Bit. Aus Sicherheitsgründen soll die Schlüssellänge auf 8192 Bit erhöht werden. Welche Auswirkungen auf die Performance erwartest du?
- (1 Punkt) Die Schlüsselerzeugung wird etwa um den Faktor _____ länger dauern.
 - (1 Punkt) Das Signieren wird etwa um den Faktor _____ länger dauern.
 - (1 Punkt) Das Verifizieren einer Signatur wird etwa um den Faktor _____ länger dauern.
3. (Elliptische Kurven – Domainparameter) Du erzeugst für ECDH Key Agreement eigene Domain-Parameter, um dich nicht auf die vom NIST zur Verfügung gestellten Kurven verlassen zu müssen. Du möchtest ein Sicherheitsniveau von zumindest 128 Bit erreichen.
- (1 Punkt) Welche der folgenden Angriffe musst du bei der Wahl der Domain-Parameter berücksichtigen?
 - Pohlig-Hellman
 - Baby-Step-Giant-Step
 - Index-Calculus
 - Wiener-Attacke
 - (2 Punkte) Besonders relevant sind bei den Domain-Parametern die Primzahl p (über welchem Körper \mathbb{Z}_p wird die elliptische Kurve definiert) und die Primzahl ω (die Ordnung des Punkts auf der Kurve, mit dem gerechnet werden soll). Wie groß müssen diese beiden Zahlen sein, um das gewünschte Sicherheitsniveau von 128 Bit zu erreichen?
 - p muss mindestens _____ Bit lang sein.
 - ω muss mindestens _____ Bit lang sein.

4. (3 Punkte) (Diffie-Hellman) Alice und Bob führen einen DH-Schlüsselaustausch (gemäß Algorithmus 2.7 im Begleitheft) durch, um einen gemeinsamen Schlüssel zu erzeugen. Sie wählen die Gruppe $(\mathbb{Z}_n, +, [0]_n, -)$ mit $n = 76543$ und $g = 34567$ als Domain-Parameter. Leider haben die beiden eine Gruppe gewählt, in der das DLP nicht schwierig genug ist. Du fängst die DH-Nachrichten $A = 2390$ von Alice an Bob und $B = 37674$ von Bob an Alice ab. Berechne damit den Schlüssel, den die beiden vereinbaren.

5. (3 Punkte) (Diskrete Logarithmen) Die elliptische Kurve $\varepsilon : y^2 = x^3 + x + 4 \pmod{32771}$ hat die Ordnung 32492. Du kennst drei Punkte

- $P = (20624, 19557)$
- $Q = (11794, 3282)$ und
- $R = (0, 2)$

auf der elliptischen Kurve. In dieser Aufgabe zeigst du, dass man diskrete Logarithmen zu einer beliebigen Basis berechnen kann, wenn man diskrete Logarithmen wenigstens zu einer Basis berechnen kann.

Der diskrete Logarithmus von P zur Basis $G = (0, 2)$ auf der elliptischen Kurve ist 13421.
Der diskrete Logarithmus von Q zur Basis $G = (0, 2)$ auf der elliptischen Kurve ist 599.

Berechne den diskreten Logarithmus von P zur Basis Q auf der elliptischen Kurve.

(*Hinweis: Für diese Aufgabe ist keine Punktaddition und keine Punktmultiplikation auf der elliptischen Kurve erforderlich.*)

6. (Merkle Trees) Du erzeugst einen Merkle Tree für 65536 Datensätze. Als Hashfunktion verwendest du SHA-256.

- (1 Punkt) Wie lang ist die Merkle Root für deine Datensätze (in Bit) in diesem Fall.
- (1 Punkt) Du möchtest die Integrität eines Datensatzes überprüfbar machen. Aus wie vielen Hashwerten besteht der Authentication Path in diesem Fall?
- (1 Punkt) Die Integrität des von dir gesendeten Datensatzes (samt Authentication Path) soll überprüft werden. Wie viele SHA-256-Hashwerte müssen dafür berechnet werden?

7. (Endliche Körper) Berechne im endlichen Körper $\mathbb{Z}_2(\alpha) = \mathbb{Z}_2[x]/(x^3 + x^2 + 1)$.

- (1 Punkt) $(\alpha^2 + 1)(\alpha + 1)$
- (2 Punkte) $\frac{\alpha^2 + 1}{\alpha + 1}$
- (Bonuspunkt) Berechne α^{1001} .