Cryptocomplexity II

Kryptokomplexität II

Sommersemester 2024

Pingo

Dozent: Prof. Dr. J. Rothe

Website

https://pingo.coactum.de/

Access Number:
885317

© Titanic Verlag

Frage 1

Wie viele primitive Elemente hat $\mathbb{Z}_p^*$ für eine Primzahl p?

A $p-1$

B $\varphi(p-1)$

C $\varphi(\varphi(p-1))$

D $\varphi(\varphi(p))-1$

Frage 2

Welche der folgenden Aussagen ist wahr?

A Kann ein Angreifer in Polynomialzeit die Primfaktoren des RSA-Moduls $n = pq$ bestimmen, so kann er effizient $\varphi(n)$ berechnen.

B Es ist nicht bekannt, ob ein Angreifer, der in Polynomialzeit $\varphi(n)$ berechnen (und somit RSA brechen) kann, auch die Primfaktoren des RSA-Moduls $n = pq$ effizient bestimmen kann.

C Damit Wieners Angriff auf RSA funktioniert, muss für den geheimen Exponenten d gelten: $d > 3\sqrt[4]{n}$.

D Das Diffie–Hellman-Problem lässt sich nicht in Polynomialzeit auf das Problem des diskreten Logarithmus (Turing)-reduzieren.

Frage 3

Welche der folgenden Aussagen ist beweisbar wahr?

A Das Problem des diskreten Logarithmus lässt sich in Polynomialzeit auf das Diffie–Hellman-Problem (Turing-)reduzieren.

B Für jede Zahl $a \in \mathbb{Z}_n^*$ gilt $a^{\varphi(n)} \equiv 1 \bmod n$.

C Der “Man-in-the-Middle”-Angriff ist ein passiver Angriff.

D Inverse modulo einer Primzahl p werden mit dem Square-and-Multiply-Algorithmus bestimmt.

Frage 4

Was war Ihr Vorsatz von Silvester 2022? Wenn Corona vorbei ist, will ich endlich mal wieder ...

A ... in einem Hörsaal dösen.

B ... Party feiern.

C ... in Urlaub fahren.

D ... aufgetaut werden.

Frage 5

Does humor belong in cryptology and complexity theory?

A Ja.

B Vielleicht.

C Nein.