

Cryptocomplexity I

Kryptokomplexität I

BBBingo

Wintersemester 2020/2021

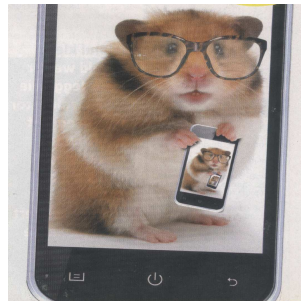
Dozent: Prof. Dr. J. Rothe



Website

~~<https://pingo.upb.de/>~~

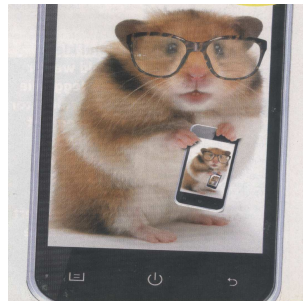
~~Code: 1869~~



Website

~~<https://pingo.upb.de/>~~

~~Code: 1869~~



Wir stimmen im BBB-Raum **WiSe 20/21 - Kryptokomplexität 1** ab.

Frage 1

Wann soll die Vorlesung beginnen?

A 8:40 Uhr

B 8:30 Uhr

Frage 2

Ich bin heute hier, weil ich ...

- A ... meine Geheimnisse gern sicher hüte.
- B ... die Geheimnisse der anderen gern auskundschaftete.
- C ... mal wissen wollte, wie HS 6C von innen aussieht.
- D ... wissen möchte, warum manche Probleme so verdammt schwer zu lösen sind.

Frage 3

Ich kenne mich ein wenig aus in ...

- A ... Zahlentheorie und linearer Algebra.
- B ... Wahrscheinlichkeitstheorie.
- C ... Algorithmik.
- D ... Komplexitätstheorie.

Frage 4

Welche der folgenden Aussagen ist/sind korrekt?

- A Eine Blockchiffre verschlüsselt im ECB-Modus gleiche Blöcke von Klartext durch stets dieselben Blöcke von Schlüsseltext.
- B Die Vigenère-Chiffre ist monoalphabetisch.
- C Die Substitutionschiffre ist eine spezielle Blockchiffre.
- D Die Permutationschiffre ist linear.

Frage 5

Die Determinante der Matrix $\begin{pmatrix} 3 & 4 \\ 5 & 2 \end{pmatrix}$ mod 7 ist gleich ...

A ... 0.

B ... 1.

C ... 2.

D ... 3.

Frage 6

Die Matrix $\begin{pmatrix} 3 & 4 \\ 5 & 2 \end{pmatrix}$ ist ...

- A ... mod 7 invertierbar.
- B ... mod 7 nicht invertierbar.
- C ... mod 9 invertierbar.
- D ... mod 9 nicht invertierbar.

Frage 7

Welche der folgenden Aussagen ist/sind korrekt?

- A Der erweiterte Euklidische Algorithmus findet Inverse modulo k .
- B Die Verschiebungschiffre ist monoalphabetisch.
- C Monoalphabetisch kann man oft mittels Häufigkeitsanalyse brechen.
- D Der Buchstabe A kommt in typischen deutschen Texten am häufigsten vor.

Frage 8

Welche der folgenden Aussagen ist/sind korrekt?

- A Kasiskis Methode bestimmt die Periode der Vigenère-Chiffre.
- B Bei der *Triple Encryption* verwendet man denselben Schlüssel dreimal hintereinander.
- C Stromchiffren verallgemeinern das Prinzip des CBC-Modus.
- D Die Hill-Chiffre ist sicher gegen *Known-Plaintext*-Angriffe.