

Cryptocomplexity I

Kryptokomplexität I

Wintersemester 2023/2024

Pingo

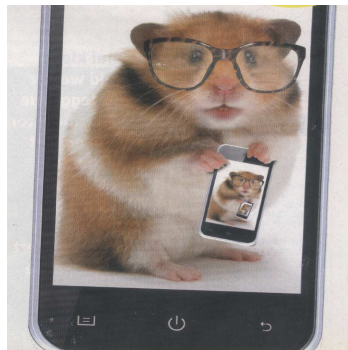
Dozent: Prof. Dr. J. Rothe



Website

<https://pingo.coactum.de/>

Access Number:
885317



© Titanic Verlag

Frage 1

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 2

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 3

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 4

Welche der folgenden Aussagen ist/sind korrekt?

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

Frage 5

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.

Frage 6

Mit welcher minimalen Anzahl von Schnitten können die Äpfel gerecht aufgeteilt werden?

- A Null Schnitte.
- B Ein Schnitt.
- C Zwei Schnitte.
- D Drei Schnitte.

