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 korrekt?

A Identische Nachrichten können im CBC-Modus durch Veränderung des Anfangsvektors unterschiedlich verschlüsselt werden.

B Sender und Empfänger können im CBC-Modus nahezu gleichzeitig ver- bzw. entschlüsseln.

C Im CBC-Modus hängt die Verschlüsselung von Blöcken von den nachfolgenden Blöcken ab.

D Übertragungsfehler richten im CFB-Modus weniger Schaden als im OFB-Modus an.

Frage 2

Welche der folgenden Aussagen ist korrekt? Der One-time Pad von Vernam . . .

A . . . ist sicher gegen Known-Plaintext-Angriffe.

B . . . leistet perfekte Geheimhaltung, falls keiner der gleichverteilten Schlüssel mehrfach verwendet wird.

C . . . hat keinerlei Nachteile in der praktischen Anwendung.

D . . . ist noch nie in der Praxis verwendet worden.

Frage 3

Die Entropie des Ausgangs eines Pferderennens mit vier “gleich schnellen” Pferden ist . . .

A . . . größer als die Entropie des Ausgangs eines Pferderennens mit fünf “gleich schnellen” Pferden.

B . . . gleich der Entropie des Ausgangs eines Pferderennens mit fünf “gleich schnellen” Pferden.

C . . . gleich 3.

D . . . größer als die Entropie des Ausgangs eines Pferderennens mit drei “gleich schnellen” Pferden und einem langsameren Gaul.

Frage 4

Welche der folgenden Aussagen ist/sind korrekt?

A Unter “Schlüsselmehrdeutigkeit” (*“key equivocation”*) versteht man die Anzahl der verschiedenen Schlüsseltexte, die man aus ein und demselben Klartext mit ein und demselben Schlüssel erhält.

B Mit der Entropie einer natürlichen Sprache wächst ihre Redundanz.

C Die Redundanz einer vollständig “zufälligen” Sprache ist null.

D Je kleiner die Redundanz einer natürlichen Sprache ist, umso stärker lässt sie sich ohne Informationsverlust komprimieren.

Frage 5

Angenommen, Sie sollen

$$43^{1025} \bmod 51$$

berechnen. Welche der folgenden Möglichkeiten würden Sie benutzen?

A Den Chinesischen Restesatz.

B Den Kleinen Fermat.

C Den Satz von Euler.

D Den erweiterten Algorithmus von Euklid.

Frage 6

Wenn Sie Ihre gewählte Methode benutzen, um

$$43^{1025} \bmod 51$$

zu berechnen. In welcher Restklasse modulo 51 landen Sie?

A 0.

B 43.

C 41.

D Gar keiner.

Frage 7

Die Anzahl der Primzahlen ist . . .

A . . . nach oben beschränkt durch 1 925 320 391 606 803 968 923.

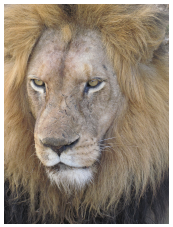
B . . . endlich.

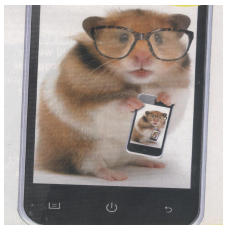
C . . . abzählbar unendlich.

D . . . überabzählbar unendlich.

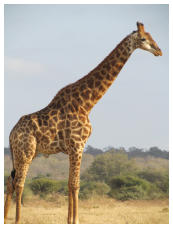
Frage 8

Welche Arten mögen Primzahlen?

A  Löwe

B  Hamster

C  Zikade

D  Giraffe