Übungen zur Kryptologie

Blatt 1 SoS 2024 — H. Kiechle

Präsenzaufgaben

1. Wiederholen Sie die Begriffe „Abbildung“, „injektiv“ und „surjektiv“, und geben Sie jeweils Beispiele und Gegenbeispiele an.

Hausaufgaben

2. Es sei (P, K, C, f) ein Kryptosystem und $k \in K$ ein Schlüssel. Zeigen Sie:

(a) die Chiffrier-Funktionen f_k ist stets injektiv;

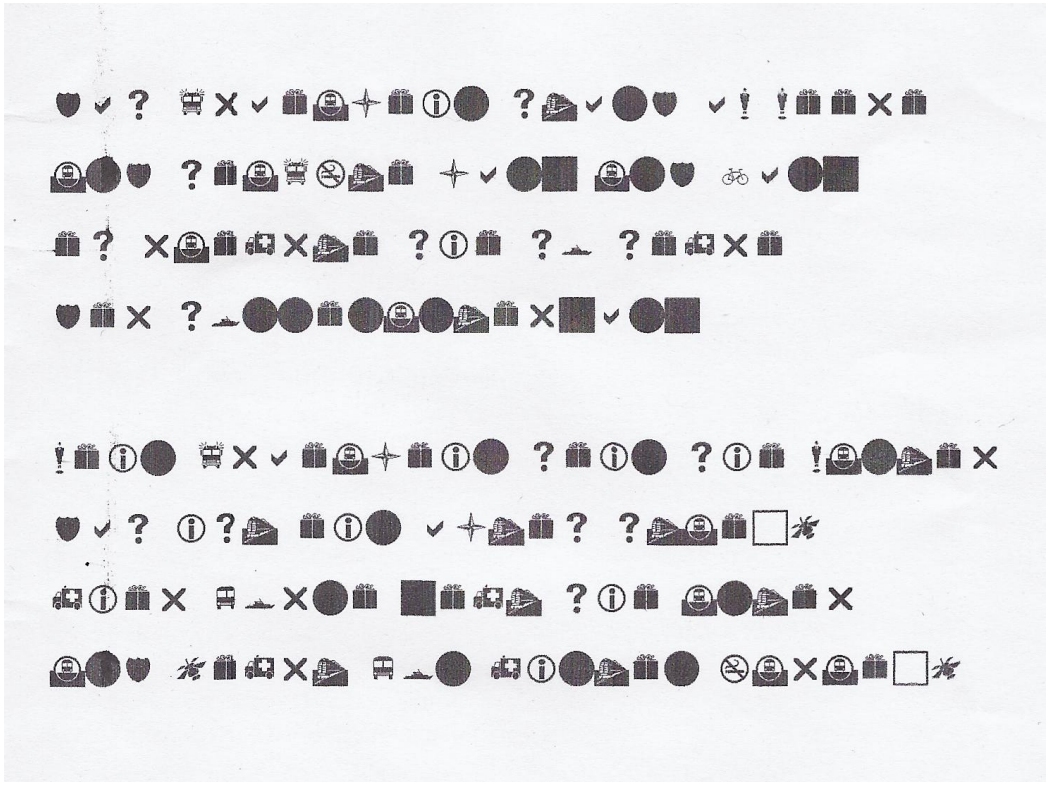
(b) die Dechiffrier-Funktionen $g_{k'}$ ist stets surjektiv.

(c) Welche praktische Bedeutung hat das?

(d) Folgere $|P| \leq |C|$.

3. Beim folgenden Geheimtext wurden Buchstaben (keine Umlaute; keine Sonderzeichen; nur Kleinbuchstaben) eins-zu-eins durch andere Zeichen ersetzt. Leerzeichen und Zeilenumbrüche wurde belassen.

Entschlüsseln Sie den Text und ermitteln Sie den Autor.



Literatur

- Beutelspacher: Kryptologie, 10. Aufl., Springer 2015
- Beutelspacher, Schwenk, Wolfenstetter: Moderne Verfahren der Kryptographie, 8. Aufl., Springer 2015
- Buchmann: Einführung in die Kryptographie, 6. Aufl., Springer-Verlag 2016
- Diffie, Hellman: New directions in cryptography, IEEE Trans. Inform. Theory **22** (1976), 644–654
- Kahn: The Codebreakers — the story of secret writing, MacMillan 1967
- Karpfinger, Kiechle: Kryptologie — Algebraische Methoden und Algorithmen, Vieweg+Teubner Verlag 2010
- Menezes, et al.: Handbook of Applied Cryptography, CRC Press 1996
- Rivest, Shamir, Adleman: A method for obtaining digital signatures and public key cryptosystems, Comm. ACM **21** (1978), 120–126
- Salooma: Public-Key Cryptography, Springer-Verlag 1996
- Stinson: Cryptography—Theory and Practice, 3. Aufl., CRC Press 2006