Template für Folien

Prof. Dr. Hannes Federrath

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Agenda

1. Einleitung
2. Beispiel
3. DTE
4. Hashbasierte Verschlüsselung
5. Einschränkungen
6. Fazit
7. Der Arbeitsbereich SVS
   - Mission
   - Themen
   - Kontakt
8. Beispiel für eine Abbildung
   - Zugangskontrolle
   - DRM-Systeme
9. Weiteres Beispiel für eine Abbildung
10. Ebenen
11. Spalten

Einleitung

??

Brute-Force-Angriff

Grafik mit Verschlüsselung, Entschlüsselung, Brute-Force-Angriff
//Durch Eigenschaften der Nachricht lässt sich ein Treffer erkennen
(natürlichsprachlich, Primzahl, festes Dokumentenformat)

Verwendete Passwörter

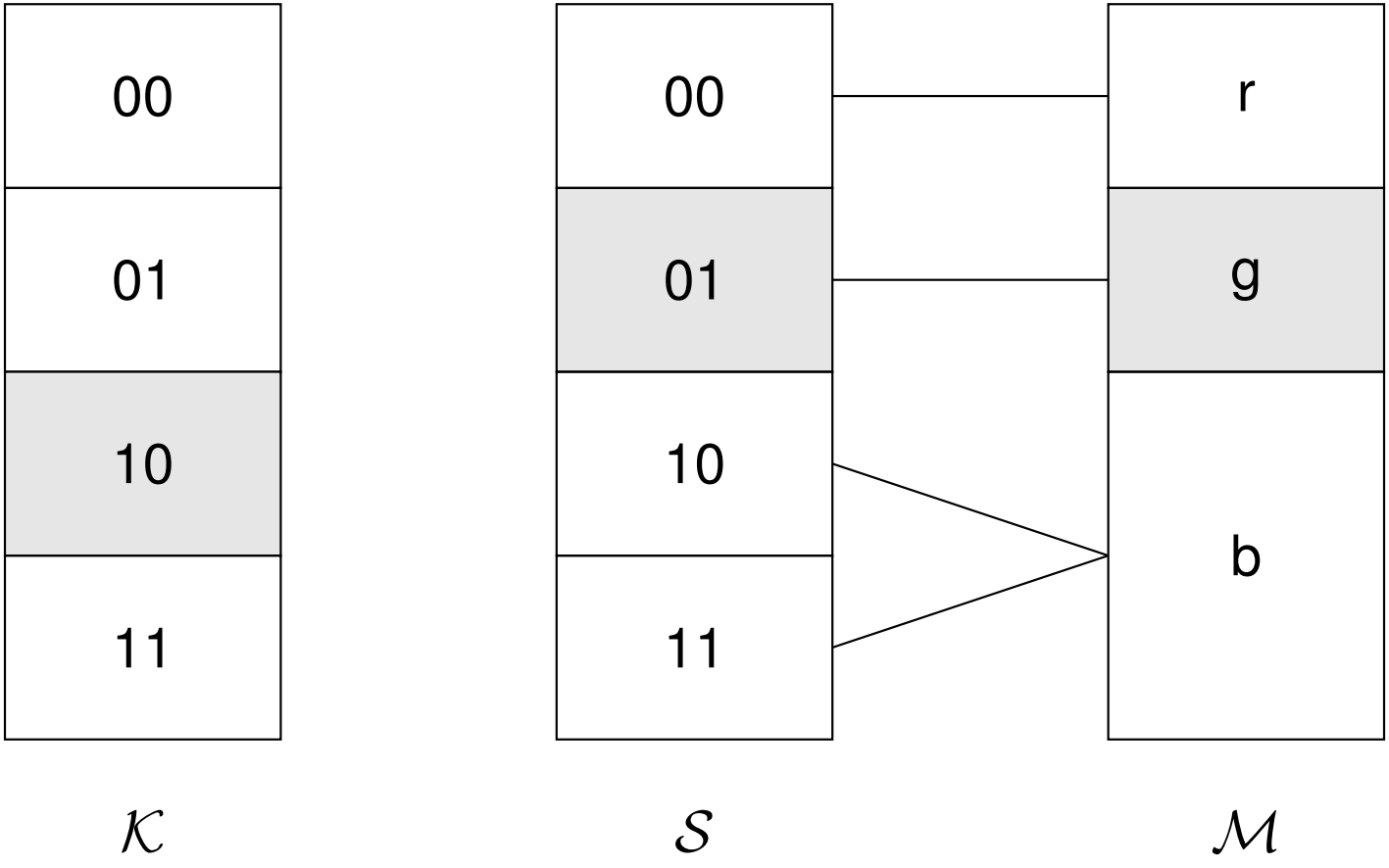
https://xato.net/wp-content/xup/passwordscloud.png

Honey Encryption

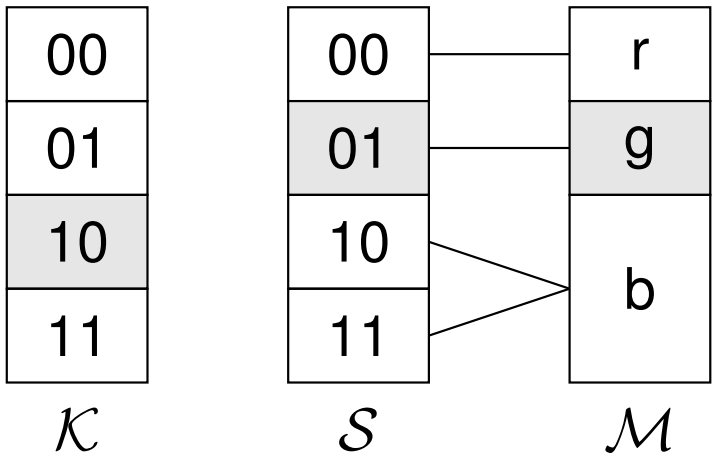
„Honey Encryption wurde entwickelt, um Ciphertexte zu generieren, die bei Entschlüsselung mit einem falschen Schlüssel zu einem plausibel wirkenden, aber unechten Klartext führen.“

[A. Juels, T. Ristenpart:
Honey Encryption - Security Beyond the Brute-Force Bound]

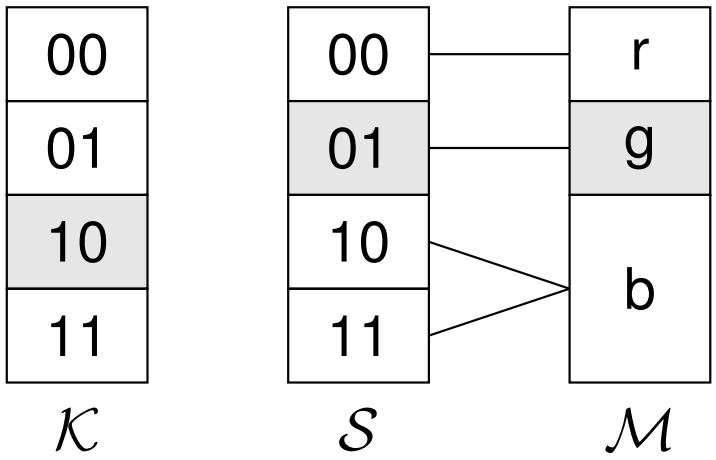
Honey Encryption - Ein Beispiel



Honey Encryption - Ein Beispiel



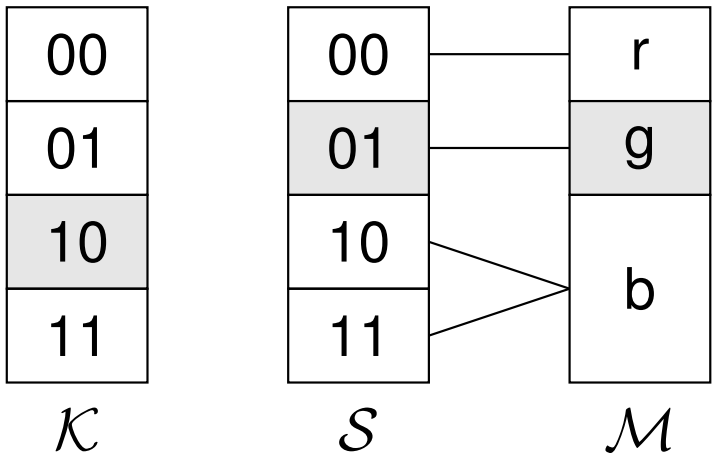
Honey Encryption - Ein Beispiel



Verschlüsselung

$$\begin{aligned} 01 &\leftarrow \text{Nachricht } M \textit{ (grün)} \\ \oplus\underline{10} &\leftarrow \text{Schlüssel } K \\ 11 &\leftarrow \text{Ciphertext } C \end{aligned}$$

Honey Encryption - Ein Beispiel



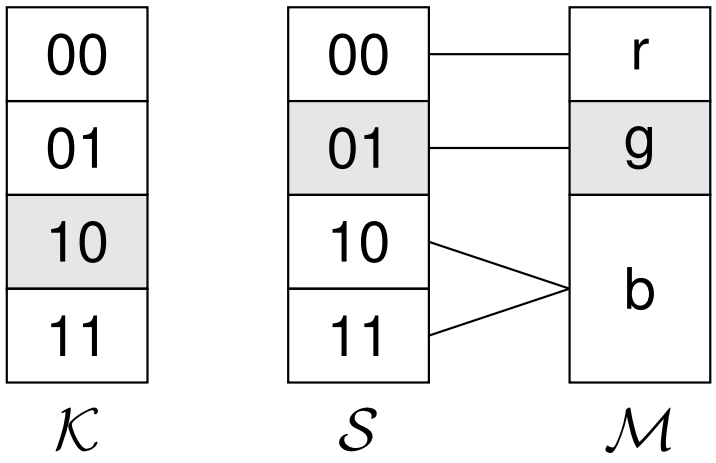
Entschlüsselung

$$\begin{aligned} 11 &\leftarrow \text{Ciphertext } C \\ \oplus\underline{10} &\leftarrow \text{Schlüssel } K \\ 01 &\leftarrow \text{Nachricht } M \textit{ (grün)} \end{aligned}$$

Verschlüsselung

$$\begin{aligned} 01 &\leftarrow \text{Nachricht } M \textit{ (grün)} \\ \oplus\underline{10} &\leftarrow \text{Schlüssel } K \\ 11 &\leftarrow \text{Ciphertext } C \end{aligned}$$

Honey Encryption - Ein Beispiel



Verschlüsselung

$$01 \leftarrow \text{Nachricht } M \text{ (grün)}$$
$$\oplus\underline{10} \leftarrow \text{Schlüssel } K$$
$$11 \leftarrow \text{Ciphertext } C$$

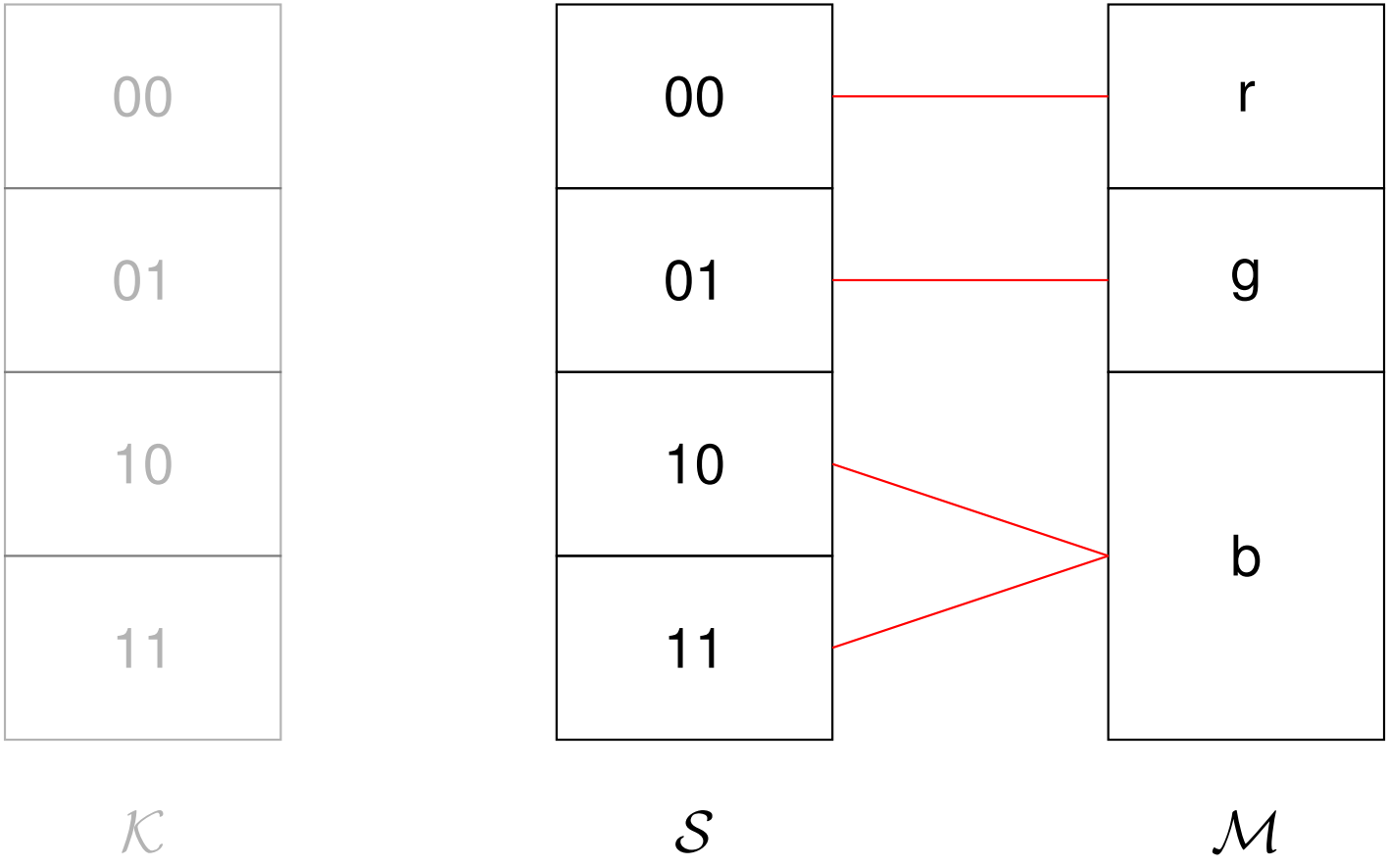
Entschlüsselung

$$11 \leftarrow \text{Ciphertext } C$$
$$\oplus\underline{10} \leftarrow \text{Schlüssel } K$$
$$01 \leftarrow \text{Nachricht } M \text{ (grün)}$$

Brute-Force-Angriff

$$11 \leftarrow \text{Ciphertext } C$$
$$\oplus\underline{11} \leftarrow \text{Schlüssel } K'$$
$$00 \leftarrow \text{Nachricht } M' \text{ (rot)}$$

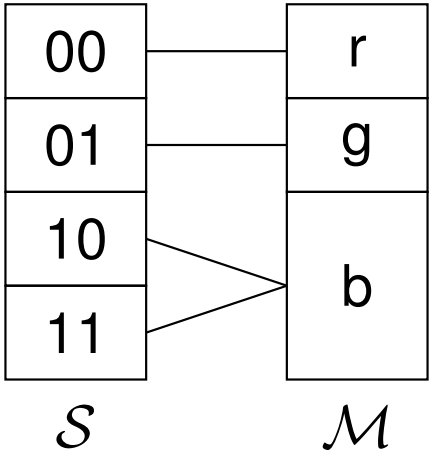
DTE



DTE

$$DTE = (encode, decode)$$

- *encode* meist randomisiert
- *decode* deterministisch



DTE

Mögliche DTE-Formen:

- Tabelle/Datenstruktur zum Nachschauen
- Funktion zur Berechnung

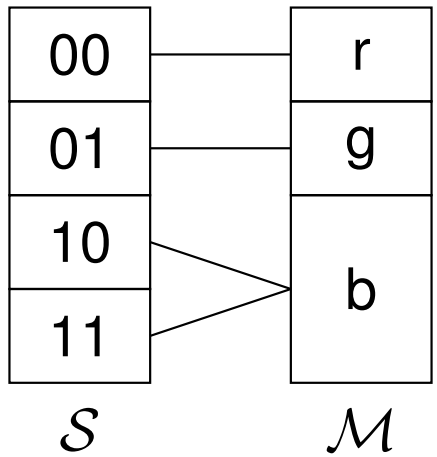
Seed	**Nachricht**
00	rot
01	grün
10, 11	blau

DTE

Seed	Nachricht
000000000000000	0000
000000000000001	0001
000000000000010	0002
...	...
10011100010000	9999

Bekannt sein muss:

- Menge/Struktur der Nachrichten
  - endlich speicherbar/berechenbar
  - unendlich berechenbar
- Verteilung der Nachrichten
  - Nachricht wahrscheinlicher $\Rightarrow$ mehr Seeds



Hashbasierte Verschlüsselung

Verschlüsselung

$\mathrm{HEnc}_{\mathrm{Hash}}(M, K)$

$S \xleftarrow{<r>} \mathrm{DTE}_{\mathrm{encode}}(M)$

$R \xleftarrow{<r>} \{0,1\}^k$

$H = \mathrm{HF}(K, R)$

$C = H \oplus S$

Return (C, R)

Hashbasierte Verschlüsselung

Verschlüsselung

$\mathrm{HEnc}_{\mathrm{Hash}}(M, K)$

$S \xleftarrow{<r>} \mathrm{DTE}_{\mathrm{encode}}(M)$

$R \xleftarrow{<r>} \{0,1\}^k$

$H = \mathrm{HF}(K, R)$

$C = H \oplus S$

Return (C, R)

Entschlüsselung

$\mathrm{HDec}_{\mathrm{Hash}}((C, R), K)$

$H = \mathrm{HF}(K, R)$

$S = H \oplus C$

$M = \mathrm{DTE}_{\mathrm{decode}}(S)$

Return M

Verschlüsselung mit Blockchiffren

Blockchiffren

Blockchiffren sind *symmetrische* Verschlüsselungsverfahren, die Klartexte und Ciphertexte in Bitgruppen fester Länge (*Blöcken*) bearbeiten.

Verschlüsselung mit Blockchiffren

Blockchiffren

Blockchiffren sind *symmetrische* Verschlüsselungsverfahren, die Klartexte und Ciphertexte in Bitgruppen fester Länge (*Blöcken*) bearbeiten.

- Können unter bestimmten Voraussetzungen ebenfalls für *HE* genutzt werden.
- Nur bestimmte Betriebsmodi (CTR, CBC) sind geeignet.
- Es darf kein Padding benötigt werden.

Einschränkungen

- Freitext (noch) nicht möglich
  - *Message Space* unendlich groß
  - Verteilung nicht bekannt
- *Typo-Safety*
  - Tippfehler führt zu falschen Daten
  - große Stärke $\Rightarrow$ große Schwäche
- Vorab bekannte Informationen
  - Angreifer kennt z.B. Teil des Klartextes $\Rightarrow$ Verifizierung eines Passwortes
  - Sicherheit der Verschlüsselung

Fazit

- Sehr sicher
- Nicht universal anwendbar
- Forschungsgebiete:
  - Natural Language Processing
  - Stochastik
  - User Experience
- Nächstes Ziel: Passwort-Manager

Der Arbeitsbereich Sicherheit in Verteilten Systemen (SVS)

Lorem ipsum dolor

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

- Themen
  1. Privacy Enhancing Technologies (PET)
  2. Security Management & Risk Management
  3. Security of Mobile Systems
- Weitere Informationen
  - http://www.informatik.uni-hamburg.de/svs

Beispiel für eine Abbildung

- Zweck
  - Nur mit berechtigten Partnern weiter kommunizieren
  - Verhindert unbefugte Inanspruchnahme von Betriebsmitteln

Beispiel für eine Abbildung

- Zweck
  - Nur mit berechtigten Partnern weiter kommunizieren
  - Verhindert unbefugte Inanspruchnahme von Betriebsmitteln

Beispiel für eine Abbildung

- Zweck
  - Einem Kunden *K* einen Inhalt *I* in einer bestimmten Weise zugänglich machen, ihn aber daran hindern, *alles* damit tun zu können.

Weiteres Beispiel für eine Abbildung

[John Doe, 1966]

- Voraussetzung: Angreifer
  - betreibt täuschend echte Webseite der Bank
  - bewegt den Kunden zum Besuch dieser Seite

Ebenen

- Erste Ebene
  - Zweite Ebene
    - Dritte Ebene
  - Zweite Ebene
- Erste Ebene

1. Erste Ebene
   1.1 Zweite Ebene
      1.1.1 Dritte Ebene
   1.2 Zweite Ebene
2. Erste Ebene

Spalten

- Linke Spalte
  - Lorem ipsum dolor sit amet,
  - consectetur adipisicing elit,
  - sed do eiusmod tempor incididunt ut
  - labore et dolore magna aliqua.
- Erste Ebene
  - Zweite Ebene
  - Zweite Ebene
- Erste Ebene
  - Zweite Ebene
  - Zweite Ebene

Das SVS-Logo