



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. Anwendungen und 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



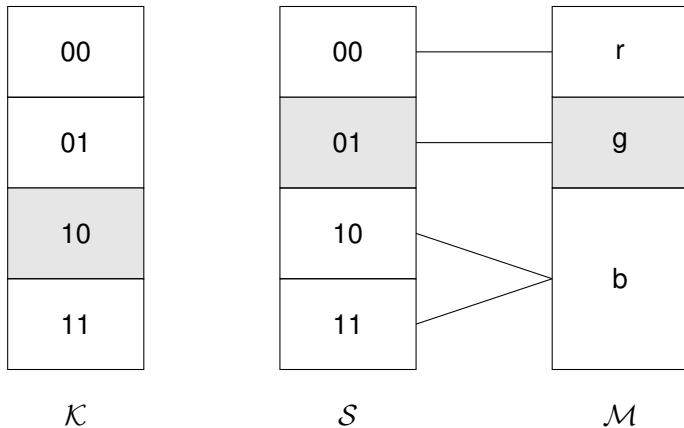
<https://xato.net/wp-content/xup/passwordscLOUD.png>

Honey Encryption

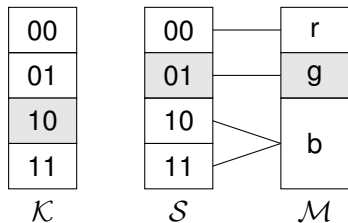
„Honey Encryption wurde entwickelt, um Ciphertexte zu generieren, die bei Entschlüsselung mit einem falschen Schlüssel zu einem plausibel wirkenden, aber unechten Klartext führen.“

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

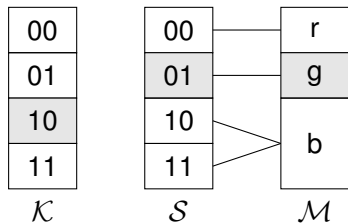
Honey Encryption - Ein Beispiel



Honey Encryption - Ein Beispiel



Honey Encryption - Ein Beispiel



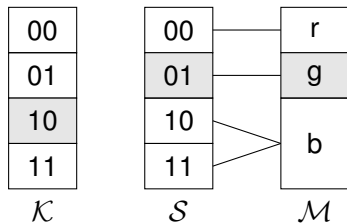
Verschlüsselung

01 \leftarrow Nachricht M (grün)

\oplus 10 \leftarrow Schlüssel K

11 \leftarrow Ciphertext C

Honey Encryption - Ein Beispiel



Entschlüsselung

11 \leftarrow Ciphertext C

$\oplus \underline{10} \leftarrow$ Schlüssel K

01 \leftarrow Nachricht M (*grün*)

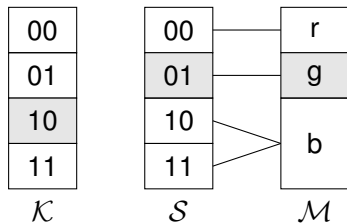
Verschlüsselung

01 \leftarrow Nachricht M (*grün*)

$\oplus \underline{10} \leftarrow$ Schlüssel K

11 \leftarrow Ciphertext C

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

Hashbasierte Verschlüsselung

Verschlüsselung

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

$$S \stackrel{\langle r \rangle}{\equiv} \text{DTE}_{\text{encode}}(M)$$

$$R \stackrel{\langle r \rangle}{\equiv} \{0, 1\}^k$$

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

$$C = H \oplus S$$

Return (C, R)

Hashbasierte Verschlüsselung

Verschlüsselung

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

$S \stackrel{\langle r \rangle}{\equiv} \text{DTE}_{\text{encode}}(M)$

$R \stackrel{\langle r \rangle}{\equiv} \{0, 1\}^k$

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

$C = H \oplus S$

Return (C, R)

Entschlüsselung

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

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

$S = H \oplus C$

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

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.

Anwendungen und Einschränkungen

Fazit

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