AES – Eine Einführung in Cryptography

Andreas Hofmeier

28/11/2005

Outline

Einführung: Was ist Cryptography? Warum brauchen wir das?

- Ein Verfahren um Daten vor unbefugtem Zugriff zu schützen.

Einführung: Was ist Cryptography? Warum brauchen wir das?

- Ein Verfahren um Daten vor unbefugtem Zugriff zu schützen.
- Öffentliches Netzwerk kann mit Postkarten vergleichen werden

Einführung: Was ist Cryptography? Warum brauchen wir das?

- Ein Verfahren um Daten vor unbefugtem Zugriff zu schützen.
- Öffentliches Netzwerk kann mit Postkarten vergleichen werden
- Einfaches Kopieren

Einführung: Was ist Cryptography? Warum brauchen wir das?

- Ein Verfahren um Daten vor unbefugtem Zugriff zu schützen.
- Öffentliches Netzwerk kann mit Postkarten vergleichen werden
- Einfaches Kopieren
- Kopieren/Lesen hinterlässt keine Spuren

Einführung: Was ist Cryptography? Warum brauchen wir das?

- Ein Verfahren um Daten vor unbefugtem Zugriff zu schützen.
- Öffentliches Netzwerk kann mit Postkarten vergleichen werden
- Einfaches Kopieren
- Kopieren/Lesen hinterlässt keine Spuren
- mathematische Algorithmus, abhängig von Schlüssel

Einführung: Was ist Cryptography? Warum brauchen wir das?

- Ein Verfahren um Daten vor unbefugtem Zugriff zu schützen.
- Öffentliches Netzwerk kann mit Postkarten vergleichen werden
- Einfaches Kopieren
- Kopieren/Lesen hinterlässt keine Spuren
- mathematische Algorithmus, abhängig von Schlüssel
- symetrische Verschlüsselung

Summenverfahren

Beispiel 1:

- Verschlüsselung
  Klartext (`6124627`) + Schlüssel (`4531773`)

$$\begin{array}{r} 6124627 \\ +4531773 \\ \hline 10656400 \end{array}$$

  Ergebnis: Chiffre (`10656400`)

Summenverfahren

Beispiel 1:

- Verschlüsselung
  Klartext (`6124627`) + Schlüssel (`4531773`)

$$\begin{array}{r} 6124627 \\ +4531773 \\ \hline 10656400 \end{array}$$

  Ergebnis: Chiffre (`10656400`)

- Entschlüsseln
  Chiffre (`10656400`) minus Schlüssel (`4531773`)

$$\begin{array}{r} 10656400 \\ -4531773 \\ \hline 6124627 \end{array}$$

  Ergebnis: Klartext (`6124627`)

Summenverfahren

Beispiel 2:

- Verschlüsselung
  Klartext (“TREFFEN UM SIEBEN”) + Schlüssel (“ZEBRA”)

```
   TREFFEN UM SIEBEN
 +             ZEBRA
---------------------
         ???????????
```

Summenverfahren

Beispiel 2:

- Verschlüsselung
  Klartext (“TREFFEN UM SIEBEN”) + Schlüssel (“ZEBRA”)

```
   TREFFEN UM SIEBEN
 +             ZEBRA
---------------------
         ??????????
```

- Jeder Buchstabe der Nachricht wird einzeln verschlüsselt.

Summenverfahren

Beispiel 2:

- Verschlüsselung
  Klartext (“TREFFEN UM SIEBEN”) + Schlüssel (“ZEBRA”)

```
   TREFFEN UM SIEBEN
 +             ZEBRA
--------------------
         ???????????
```

- Jeder Buchstabe der Nachricht wird einzeln verschlüsselt.
- Jedem Buchstabe wird aufgrund seine Position im Alphabet eine Zahl zugeordnet: `A = 0, B = 1, ... Z = 25, Freiraum = 26.`

Summenverfahren

Beispiel 2:

- Verschlüsselung
  Klartext (“TREFFEN UM SIEBEN”) + Schlüssel (“ZEBRA”)

```
   TREFFEN UM SIEBEN
 +             ZEBRA
---------------------
         ???????????
```

- Jeder Buchstabe der Nachricht wird einzeln verschlüsselt.
- Jedem Buchstabe wird aufgrund seine Position im Alphabet eine Zahl zugeordnet: `A = 0, B = 1, ... Z = 25, Freiraum = 26.`
- Ist die Nachricht länger als der Schlüssel, wird dieser wiederholt angewendet.

Summenverfahren

Beispiel 2:

- Verschlüsselung
  Klartext (“TREFFEN UM SIEBEN”) + Schlüssel (“ZEBRA”)

```
   TREFFEN UM SIEBEN
 +             ZEBRA
---------------------
          ??????????
```

- Jeder Buchstabe der Nachricht wird einzeln verschlüsselt.
- Jedem Buchstabe wird aufgrund seine Position im Alphabet eine Zahl zugeordnet: `A = 0, B = 1, ... Z = 25, Freiraum = 26.`
- Ist die Nachricht länger als der Schlüssel, wird dieser wiederholt angewendet.
-