



Übungen zur Vorlesung „Netzicherheit“ Übungsblatt 2, WS08/09

Abgabe: 12. Nov. 2008
Besprechungstermin: 19. Nov. 2008

Aufgabe 1: Meet-In-The-Middle Angriff auf Double-DES

Der Verschlüsselungsalgorithmus Double-DES wird wie folgt definiert: Es wird ein symmetrischer Schlüssel K der Länge 112 (2×56) verwendet. Dieser Schlüssel wird in 2 Schlüssel eingeteilt: K_1 und K_2 . Ein Plaintext P wird wie folgt verschlüsselt:

$$C = E(K_2, E(K_1, P))$$

Dabei ist E die Verschlüsselungsfunktion mit dem DES-Algorithmus. Recherchieren Sie und beschreiben Sie (am besten mit einer Abbildung) den Meet-In-The-Middle Angriff auf Double-DES.

Begründen Sie, warum Double-DES kaum mehr Sicherheit bietet als der einfacher DES-Algorithmus.

Aufgabe 2: Symmetrische Verschlüsselung im Counter Modus (CTR)

In Abbildung 1 wird die Funktionalität des CTR Modes beschrieben.

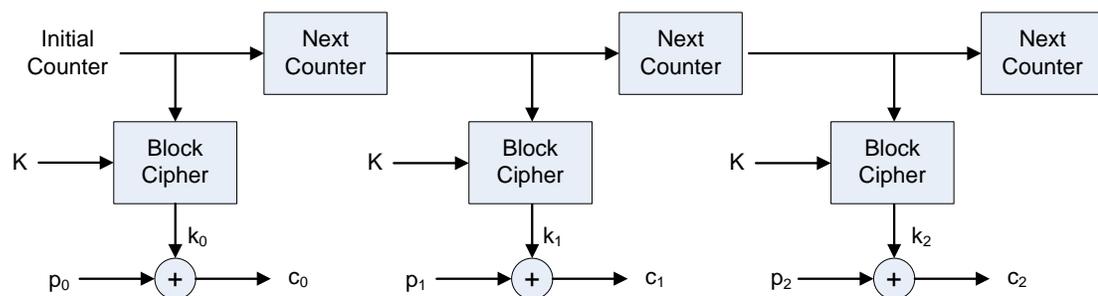


Abbildung 1: Symmetrische Verschlüsselung im CTR Modus

- Beschreiben Sie wie ein Angreifer gezielt Bits einer im CTR Modus verschlüsselten Nachricht umkippen kann. Wie kann man sich gegen einen solchen Angriff schützen?
- Angenommen es soll für jede neue Nachricht ein neuer Schlüsselstrom ($k_0 || k_1 || k_2 \dots$) mit einem neu generierten "Initial Counter" berechnet. Begründen Sie, warum beim gleichen Schlüssel K eine Wiederverwendung des gleichen „Initial Counters“ zu einem so genannten „Known-Plain-Text Angriff“ führt¹.

¹ Ein "Known-Plain-Text Angriff" ergibt sich, wenn ein Angreifer über ein oder mehrere Nachrichten-Paare

Aufgabe 3: RSA-Algorithmus

- Sei $n = 11 \times 17 = 187$. Berechnen Sie die Anzahl der Zahlen $m \in \mathbb{N}$, so dass $1 \leq m < n$ und $\text{ggT}(n, m) = 1$.
- Sei $M = 13$. M soll mit dem RSA-Algorithmus verschlüsselt werden. Der öffentliche Schlüssel besteht aus $n = 187$ und dem Exponenten $e = 3$. Berechnen Sie den passenden Cipher Text C zu M .
- Die Anwendung des erweiterten euklidischen Algorithmus ergibt

$$3 \times 107 - 2 \times \Phi(n) = 1$$

Geben Sie den privaten Schlüssel bei der Anwendung des RSA-Algorithmus an, wenn der öffentlicher Schlüssel aus $n = 187$ und dem Exponenten $e = 3$ besteht.
Verifizieren Sie am Beispiel $M = 13$, dass sich bei der Entschlüsselung von $C = E(M)$ wieder M ergibt.

Aufgabe 4: Man-In-The-Middle Angriffe auf RSA und Diffie-Hellmann

- Angenommen Bob möchte mit Alice kommunizieren. Die Kommunikation soll über einen sicheren Kanal gegen Abhör-Angriffe geschützt werden. Hierfür ist in jede Richtung jeweils eine Verschlüsselung mit dem RSA-Algorithmus vorgesehen. K_{A-pub} und K_{B-pub} sind jeweils die öffentlichen Schlüssel von Alice und Bob. K_{A-priv} und K_{B-priv} sind die privaten Schlüssel. Dabei kennen weder Bob noch Alice den öffentlichen Schlüssel des jeweiligen Kommunikationspartners.

Beschreiben Sie die Nachrichten, die bei einem Man-In-The-Middle-Angriff (MITM) zwischen Alice, Bob und dem Angreifer Mallory jeweils ausgetauscht werden.

- Angenommen Alice und Bob möchten einen gemeinsamen geheimen Schlüssel mit dem Diffie-Hellman-Verfahren austauschen. Beschreiben Sie die Nachrichten, die bei einem Man-In-The-Middle Angriff zwischen Alice, Bob und dem Angreifer Mallory jeweils ausgetauscht werden. Welchen gemeinsamen Schlüssel haben schließlich Alice bzw. Bob mit wem ausgetauscht?

Aufgabe 5: RSA – Performance Optimierung (Freiwillige Aufgabe)

Der folgende Algorithmus berechnet zu einer Zahl C den passenden Plain Text M mit Hilfe des privaten Schlüssels d .

```
//Input: C, d, n
//Output: M

M := 1;
i := 0;

while (i < d)
{
    M := M*C;
    M := M mod n;
    i++;
}
return M;
```

(P_i, C_i) verfügt und dadurch eine verschlüsselte Nachricht C_j entschlüsseln kann. Dabei könnten die Nachrichten P_i eventuell auch nur geraten werden oder nur Teile von ihnen bekannt werden.

- a) Sei k die Bit-Länge bei der Binärdarstellung von n : $k = \lfloor \ln_2(n) \rfloor + 1$. Da d durch n beschränkt ist, schätzen Sie den Aufwand dieses Algorithmus als Funktion von k ab.
- b) Geben Sie einen besseren Algorithmus an, bei dem der Aufwand der Berechnung von M linear von k abhängt.