Institut für Theoretische Informatik
Prof. Dr. Dennis Hofheinz
Übungsleiter: Thomas Agrikola

Stammvorlesung Sicherheit im Sommersemester 2017

Übungsblatt 2

Hinweis. Für die Vorlesung und Übung wurde eine Mailingliste eingerichtet. Wir werden diese Liste benutzen, um aktuelle Informationen zur Vorlesung/Übung zu verschicken, außerdem kann die Liste verwendet werden, um Fragen zu diskutieren. Alle weiteren Informationen zur Anmeldung etc. können hier nachgelesen werden:

`https://lists.ira.uni-karlsruhe.de/mailman/listinfo/sicherheit2017`

(Die Anmeldung ist freiwillig, erleichtert aber die Kommunikation)

Aufgabe 1. Aus der Vorlesung ist bekannt, dass eine Blockchiffre im CBC-Modus IND-CPA-sicher ist, wenn $\mathsf{E} : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$, für $k, \ell \in \mathbb{N}$, ununterscheidbar von einer echt zufälligen Funktion ist und der Initialisierungsvektor IV für jeden Verschlüsselungsvorgang neu gleichverteilt zufällig gezogen wird. Wir betrachten nun die folgenden zwei Fälle:

Fall 1: IV wird fest und für jeden Verschlüsselungsvorgang gleich gewählt,

Fall 2: IV wird, ausgehend von einer fixen Wahl, bei jedem Verschlüsselungvorgang um 1 hochgezählt (dabei wird nicht zwischen Verschlüsselungsvorgängen des Orakels und des Experiments unterschieden).

Geben Sie für diese beiden Fälle jeweils einen Angreifer an, der das IND-CPA-Spiel immer gewinnt.

Aufgabe 2. Es sei SKE ein IND-CPA-sicheres, symmetrisches Verschlüsselungsverfahren mit einem Verschlüsselungsalgorithmus Enc und einem Entschlüsselungsalgorithmus Dec. Wir verwenden die Algorithmen von SKE um zwei weitere Verschlüsselungsverfahren zu konstruieren:

(1.) Betrachten Sie das symmetrische Verschlüsselungsverfahren SKE' mit den folgenden Algorithmen:

- $\mathsf{Enc}'(K, M) := \mathsf{Enc}(K, \mathsf{Enc}(K, M))$,
- $\mathsf{Dec}'(K, C) := \mathsf{Dec}(K, \mathsf{Dec}(K, C))$.

(a) Zeigen Sie die Korrektheit von SKE', d.h. zeigen Sie, dass Dec' Chiffrate die mit Enc' erstellt wurden, korrekt entschlüsselt.

(b) Zeigen Sie, dass SKE' ebenfalls IND-CPA-sicher ist (Hinweis: Reduzieren Sie die Sicherheit von SKE' auf die Sicherheit von SKE. Nehmen Sie dazu zum Widerspruch an, dass ein Angreifer auf SKE' existiert und konstruieren Sie daraus einen Angreifer auf SKE).

(2.) Betrachten Sie das symmetrische Verschlüsselungsverfahren SKE^* mit den folgenden Algorithmen:

- $\mathsf{Enc}^*(K, M) := (M_{(0)}, \mathsf{Enc}(K, M))$ $(= (C_1, C_2))$,
- $\mathsf{Dec}^*(K, C) = \mathsf{Dec}^*(K, (C_1, C_2)) := \mathsf{Dec}(K, C_2)$.

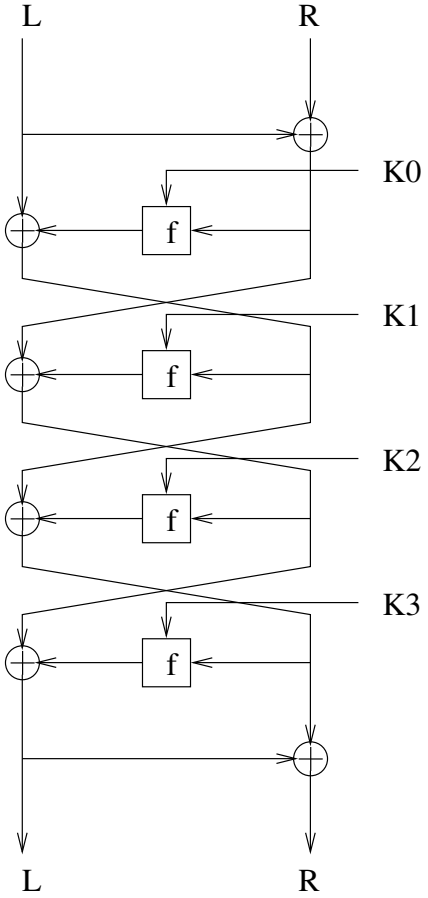
Dabei bezeichne $M_{(0)}$ das niederwertigste Bit des Klartextes M.

(a) Zeigen Sie die Korrektheit von SKE^*.

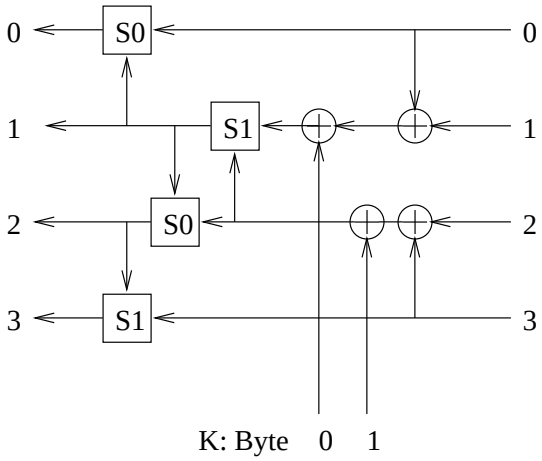
(b) Zeigen Sie, dass SKE^* nicht IND-CPA-sicher ist.

Aufgabe 3. Der ebenso brilliante wie einflussreiche Wissenschaftler und Superbösewicht Doktor Meta hat nach Jahren der Planung endlich **den** idiotensicheren Plan zur Übernahme der Weltherrschaft ausgearbeitet. Da er von der Ausarbeitung des Plans sehr erschöpft ist, macht er erstmal Urlaub und überlässt in der Zwischenzeit seinem mittelmäßig intelligenten Handlanger die Aufgabe seinen Plan verschlüsselt an seine Anhänger zu übermitteln. Da die Geheimhaltung des Plans essentiell für dessen Gelingen ist, hat Doktor Meta selbstverständlich bereits dafür gesorgt, dass er, sein Handlanger und alle seine Anhänger in Besitz eines gemeinsamen geheimen Schlüssels sind. Der Handlanger verwendet zur Verschlüsselung des Plans eine leichte Vereinfachung des symmetrischen Verfahrens FEAL-4 (siehe auch `http://de.wikipedia.org/wiki/FEAL`).

Helfen Sie uns die fiesen Weltherrschaftspläne Doktor Metas ans Licht zu bringen indem Sie das verwendete Verschlüsselungsverfahren durch lineare Kryptoanalyse brechen (und damit unseren Geheimdiensten ermöglichen, den Plan zu entschlüsseln und die Welt zu retten)!



Die f-Funktion und die S-Boxen ($S_i(a,b) := rot2((a+b+i) \mod 256)$ sind gegenüber dem Original nicht verändert:



Der Ausgangspunkt für eine lineare Approximationen der f-Funktion ist das jeweils letzte Bit der Addition der 4 S-Boxen, bei dem gegenüber allen anderen Bits kein Übertrag auftreten kann. Die ersten beiden S-Boxen liefern die Gleichungen:

- $F[2] = B[0] + F[8]$ und
- $F[10] = 1 + B[0] + B[8] + K[0] + B[16] + B[24] + K[8]$ (hier geht auch der Schlüssel mit ein!),

wobei $F[i]$ das i-te Ausgabebit von f ist; $B[i]$ und $K[i]$ entsprechend das i-te Eingabe- bzw. Schlüsselbit.

(a) Geben Sie die Gleichungen an, die die beiden anderen S-Boxen liefern.

(b) Geben Sie die 3-Runden Charakteristiken an, die sich durch die Gleichung zur ersten und dritten S-Box ergeben.

(c) Beschreiben Sie das Vorgehen der linearen Kryptoanalyse, das die vier Charakteristiken verwendet.

(d) Bei wievielen Klartext/Chiffrat-Paaren erwarten Sie einen Erfolg der Analyse?
Empirisch funktioniert der Angriff bei etwa 15 Paaren problemlos. Wie erklärt sich der Unterschied zu dem geschätzten Wert (falls er abweicht)?

Aufgabe 4. Symmetrische Verschlüsselungsverfahren in der Praxis: Wählen Sie drei (verbreitete) kryptographische Protokolle bzw. drei Programme aus, in denen symmetrische Verschlüsselungsverfahren zum Einsatz kommen. Welche Chiffren werden jeweils verwendet? (Bei Blockchiffren: Welche Modi werden benutzt? Wie wird ggf. der Initialisierungsvektor gewählt?) Woher kommt der verwendete Schlüssel?