Hochschule RheinMain
Fachbereich DCSM - Informatik
Marc Stöttinger

Security
SoSe 23
LV 4120, 7240

Übungsblatt 6

Aufgabe 6.1 (Advanced Encryption Standard):

Der Advanced Encryption Standard (AES) ist eine Blockchiffre die von der NIST mit verschiedenen Parametern standardisiert wurde.

Blochchiffre: Blockgröße 128 Bits (standarisiert 2000)

a) Geben Sie an, mit welchen Schlüssellängen AES standardisiert wurde und wie sich die Auswahl der Schlüssellänge auf folgende Parameter auswirkt:

subByte, shiftRows, mixColumns, addRoundKey werden n,- 1 mal ausgeführt

- ~~Anzahl der Runden für die Verschlüsselung von einem~~ Block
- Sicherheitslevel
- Blockgröße

b) Berochenen Sie die Zwischenwerte der ersten *(*AddRoundKey)-Operation und die Operation *Sbox*, *ShiftRows* und *MixColumn* der ersten AES-Runde für die gegebenen Werte:

- Plaintext:
  0x09 0x00 0x08 0xFF 0x52 0x52 0x52 0x52 0x52 0x52 0x52 0x52 0x52 0x52 0x52 0x52
- Schlüssel:
  0x00 0x09 0x01 0xF6 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Aufgabe 6.2 (Modes of Operation):

a) Die verschiedenen Modes of Operation können auch mathematisch unabhängig vom Verschlüsselungsalgorithmus selber notiert werden. Zum Bespiel kann die Verarbeitungsvorschrift für den ECB-Mode folgendermaßen niedergeschrieben werden:
Verschlüsselung: $C_i = ENC_K(P_i)$ und
Entschlüsselung: $P_i = DEC_K(C_i)$,
wobei $ENC_K(\cdot)$ für die Verschlüsselungsoperation mit dem Schlüssel K steht, P_i für den i-ten Plaintext und C_i für den i-ten Ciphertext, $DEC(\cdot)$ steht für die Entschlüsselungsoperation. Schreiben Sie die Verarbeitungsvorschriften für die Ver- und Entschlüsselung der folgende Modes:

a1) CBC

a2) CFB

a3) CTR

a4) OFB

Mode		Formulas	Ciphertext
Electronic codebook	(ECB)	Y_i = F(PlainText$_i$, Key) F(Plaintext, Key) = Encrypt	Y_i = Ciphertext
Cipher block chaining	(CBC)	Y_i = PlainText$_i$ XOR Ciphertext$_{i-1}$	F(Y, Key); Ciphertext$_0$ = IV
Propagating CBC	(PCBC)	Y_i = PlainText$_i$ XOR (Ciphertext$_{i-1}$ XOR PlainText$_{i-1}$)	F(Y, Key); Ciphertext$_0$ = IV
Cipher feedback	(CFB)	Y_i = Ciphertext$_{i-1}$	Plaintext XOR F(Y, Key); Ciphertext$_0$ = IV
Output feedback	(OFB)	Y_i = F(Y_{i-1}, Key); Y_0 = F(IV, Key)	Plaintext XOR Y_i
Counter	(CTR)	Y_i = F(IV + $g(i)$, Key); IV = token()	Plaintext XOR Y_i

b) Für welche Familie on Chiffren können die in der vorherigen Teilaufgabe gennanten Betriesbmodi angewendet werden? Blockchiffren

c) Nennen Sie drei verschiedene Konstruktionsarten für die Mitglieder dieser Chiffren-Familie und beschreiben Sie deren Kerneigenschaften und Unterschiede.

1) SPN (Substitutions-Permutations-Netzwerk):
Plaintext wird in mehrere gleich große Blöcke aufgeteilt.
Rundenfunktion wird immer mit einem individuellen Rundenschlüssel mehrfach aufgerufen

2) Feistel : Plaintext wird in zwei Blöcke aufgeteilt.
Verschlüsselung & Entschlüsselung verwenden die gleiche Rundenfunktion

3) ARX (Add-Rotate-Xor): kompakt, ressourcensparend

Aufgabe 6.3 (RSA):

In dieser Teilaufgabe berechnnen Sie eine RSA Schlüsselgenerierung, Ver- und Entschlüsselung per Hand. Gegeben sind folgende Werte $p = 17$, $q = 13$, $e = 11$, Plaintext $P_1 = 23$ und Ciphertext $C_2 = 42$.

a) Modulus N

b) Eulersche-Phi Funktion $\phi(N)$

c) Öffentlicher Schlüssel $K_E = (N, e)$

d) Privater Schlüssel $K_D = d$
Hinweis: Nutzen Sie hierfür den erweiterten Euklidschen Algorithmus

e) Ciphertext $C_1 = ENC_{K_E(P_1)}$

f) Ciphertext $C_1 = ENC_{K_E(P_1)}$

g) Auf welchem Problem beruht die Sicherheit des RSA-Verfahrens?

Aufgabe 6.4 (B2D Vertraulich Kommunizieren?):

Wie Sie in den vorherigen Übungen gesehen habe, benötigt die APP B2D eine sichere Kommunikation mit dem B2D-Server. Für eine einfache und verlässliche Kommunikation sind feste Statusnachrichten zwischen der App und dem Server von Herrn Spec definiert worden. Hierzu werden feste Nachrichtenformate definiert. Hier ist ein Auszug einiger Statusnachrichten:

Bedeutung	Sender	Empfänger	Nachrichentformat
Blutgruppe A wird benötigt	D2BS	App	0x00000101 0x00000000 0x00000000 0x0000000A
Blutgruppe B wird benötigt	D2BS	App	0x00000101 0x00000000 0x00000000 0x0000000B
Blutgruppe AB wird benötigt	D2BS	App	0x00000101 0x00000000 0x00000000 0x000000AB
Blutgruppe 0 wird benötigt	D2BS	App	0x00000101 0x00000000 0x00000000 0x00000100
Benutzer 3425 kann Blutgruppe A spenden	App	D2BS	0x00000110 0x00000000 0x00000D61 0x0001000A
Benutzer 3425 kann nicht Blutgruppe A spenden	App	D2BS	0x00000110 0x00000000 0x00000D61 0x0081000A
Benutzer 16 kann Blutgruppe B spenden	App	D2BS	0x00000110 0x00000000 0x00000010 0x0001000B
Benutzer 16 kann nicht Blutgruppe B spenden	App	D2BS	0x00000110 0x00000000 0x00000010 0x00000000
Die Spende findet im Krankenhaus Nummer 10 statt	D2BS	App	0x00800110 0x0000000A
Die Spende findet im Krankenhaus Nummer 1 statt	D2BS	App	0x00800110 0x00000001

Um die Vertraulichkeit der Nachrichten zu gewährleisten sollen diese Nachrichten verschlüsselt übertragen werden. Der neue Security-Engineer Herr Seky schlägt, vor die Nachrichten direkt mit AES zu verschlüsseln.

a) Sehen Sie ein Problem mit der Entscheidung die Nachrichten direkt als Plaintext zu nutzen und dann direkt den Ciphertext zu versenden? Begründen Sie ihre Aussage.

b) Welchen Betriebsmode würden Sie wählen und warum?

c) Weiterhin plant Herr Seky, das gesamte System ressourcenschonend zu gestalten und trotzdem hochsichere operative Sicherheitsfeatures mit konstantem Schlüsselaustausch zu nutzen, damit ein Angreifer nur maximalen einen Tag Zeit hat die Verschlüsselung zu brechen. Deswegen sollen alle APPs den gleichen Transportschlüssel nutzen der täglich über ein Schlüsselauslieferungsprotokoll geschützt werden soll. Das Schlüsselaustauschprotokoll sieht vor, den neuen Schlüssel mit dem alten Schlüssel zu verschlüsseln $ENC_{K_i}(K_{i+1})$ und dann einfach nach dem Erhalt um 23.59 Uhr zu ersetzen ($K_i \rightarrow K_{i+1}$). Was spricht gegen dieses Design oder Umsetzung?

d) Herr Sek sieht seinen Fehler ein und will nun lieber auf ein DHKE Protokoll setzen, bei dem jedes Mobiltlefon seinen eigenen $K_{App_{pr}}$ und $K_{App_{pub}}$ generiert und mit dem Server dann via DHKE einen Transportschlüssel alle 24 Stdunden individuell (pro Mobiltelefon) aushandelt. Ist diese Vorgehensweise besser? Was gibt es zu beachten.

Aufgabe 6.5 (Deffie-Hellman):

a) Auf welchem Problem basiert das Diffie-Hellmann Key Exchange (DHKE) Verfahren?

b) Schreiben Sie das DHKE Protokoll für einen Schlüsselaustausch zwischen Alice und Bob auf.

c) Zeigen Sie das $B^a \mod p \equiv A^b \mod p$ ist und somit Bob und Alice den gleichen Schlüssel K_{AB} haben.

d) Rechnen Sie ein Beispiel mit $a = 5$, $b = 12$, $g = 2$ und $p = 29$.

e) Zeigen Sie wie ein MiTM-Angriff auf DHKE ablaufen kann.

f) Was wird benötigt um einen MiTM bei einem DHKE-Protokoll zu verhindern?

Aufgabe 6.6 ((Vertiefende Aufgabe:) Elgamal-Verschlüsselung):

a) Wie könnte das DHKE erweitert werden, um direkt eine Nachricht m zu verschlüsseln anstatt einen Schlüssel auszutauschen? **Tipp:** Das Kapitel 8.5 *Das Verschlüsselungsverfahren nach Elgamal* in *Christoph Paar, Jan Pelz: Kryptografie verständlich, 2016, Springer* enthält hierfür wichtige Informationen.

b) Was für ein Problem oder Schwachstelle kann bei dieser Art der Nutzung des DHKE entstehen? Was müssen Sie für jede verschlüsselte Nachricht tun, damit die Verschlüsselung nicht gebrochen werden kann?

c) Schreiben Sie das Elgmal Verschlüsselungsprotokoll auf und rechnen Sie mit kleinen Zahlen ein Beispiel durch.