SbD_Blatt3_Loesung

November 21, 2019

In [ ]:

1 1 Welche der folgenden Aussagen bezüglich Elliptischer-Kurven-Kryptographie stimmen?

Wählen Sie eine oder mehrere Antworten:

b. ElGamal, DSA und Diffie-Hellman sind Algorithmen, die sich auf elliptische Kurven übertragen lassen

d. Elliptische-Kurven-Kryptographie benötigt kürzere Schlüssel als andere asymmetrische Kryptoverfahren um ein vergleichbares Sicherheitsniveau zu erreichen.

e. Verfahren auf der Basis diskreter Logarithmen lassen sich auf elliptische Kurven übertragen.

2 2 In der Vorlesung wurden verschiedene Blockmodi behandelt. Ordnen Sie diese den Beschreibungen zu.

Cipher Block Chaining: Jeder Block wird vor der Verschlüsselung mit dem vorherigen Block verknüpft

cipher feedback: Als Einagbe für die Verschlüsselungsfunktion wird in jedem Block der vorherige Cipher-Block text genutzt

output Feedback: Als Einagbe für die Verschlüsselungsfunktion wird in jedem Block die vorherige ausgabe der verschlüsselungsfunktion benutz.

Electronic Code Book: Jeder Block wird einzelnd verschlüsselt

Counter Mode: Jeder Block wird vor der verschlüsselung mit steigendem Zähler verknüpft

3 3 Elliptic Curve Cryptography (ECC) bezeichnet asymmetrische Kryptosysteme, die auf Operationen auf elliptischen Kurven über endlichen Körpern aufbauen. Zur Erinnerung:

Elliptische Kurven in der Kryptographie beinhalten alle Punkte, die die folgende Gleichung erfüllen: y^2 = x^3 + ax + b mod P .

Mit der Lösung welches mathematischen Problems lassen sich elliptische Kurven brechen?

Auf der Schwierigkeit der Berechnung des Diskreten Logarithmus

Gegeben sei folgende elliptische Kurve: E(GF(P)) mit a=1, b=6, P=11. Bestimmen Sie die Punkte, die diese Kurve besitzt in der Form (A,B) (C,D) ...

(A, B, C, ...entsprechen den Zahlen. Aufsteigend sortiert. Primär nach der ersten Zahl sekundär nach der zweiten Zahl. Andere Fälle am Ende. In der Klammer kein Leerzeichen.)

Einzige Aufgabe die nicht gelöst wurde

```
In [ ]:
```

Der 'ECB'-Modus erlaubt, Strukturen der Klartext-Blöcke auch im Ciphertext wiederzuerkennen. Mehrere gleiche Klartext-Blöcke 'sind im Ciphertext identisch'.

Fehlerhaft übertragene Ciphertext-Bits wirken sich dabei 'Nur auf den Betroffenen Block' im Klartext aus.

Im Gegensatz dazu wird im 'CBC'-Modus für die Verschlüsselungs jedes Blocks die Ausgabe der Verschlüsselungsfunktion des vorherigen Blocks eingesetzt, sodass 'True: gleiche Klartextblöcke nicht mehr die gleichen Ciphertext-Blöcke verursachen.'

Im ersten Block wird stattdessen ein 'zufälliger' 'IV' verwendet.

Fehlerhaft übertragene Ciphertext-Bits wirken sich dabei 'False:auf alle folgenden Blöcke' im Klartext aus.

4 4 r-Bit MAC

Nehmen Sie an, dass pro Nachrichtenbit 11 Schlüsselbits benötigt werden. Wie hoch ist die Wahrscheinlichkeit, dass ein*e Angreifer*in den richtigen MAC für das Bit wählt? (Bitte geben Sie das Ergebnis auf 4 Nachkommastellen genau an. Darstellung mit Kommata)

```
In [6]: #Antwort 2^{-r} : 0,0004
        2**(-11)

Out[6]: 0.00048828125
```

5 5 Alice möchte Bob die Nachricht 'CYBER!' schicken. Um ein Abhören durch Eve zu vermeiden, verschlüsselt sie die Nachricht mit dem Verschlüsselungsverfahren nach ElGamal. Hierzu ersetzt sie zunächst mit Hilfe der untenstehenden Tabelle jedes Zeichen durch eine Zahl, um diese dann einzeln zu verschlüsseln. Alice und Bob einigen sich auf die Primzahl p = 29 und den Generator (primitive Wurzel von p) a = 2. Bobs öffentlicher Schlüssel lautet y_B = 4.

erschlüsseln Sie jedes einzelne ersetzte Zeichen mit Bobs öffentlichem Schlüssel. Die Zufallszahl sei z = 5. Geben Sie die Schlüsselzahlen an

Antwort: 27, 25, 18, 16, 17, 11

```
In [26]: #                  C  Y   B  E   R   !
         char_to_number = [3, 25, 2, 5, 18, 27]

         def elgamal_crypt(m):
```

```
        return (4**5) * m % 29
    [elgamal_crypt(char) for char in char_to_number]
```

```
Out[26]: [27, 22, 18, 16, 17, 11]
```

Durch die Lösung welches Problem lässt sich die Verschlüsselung mit ElGamal brechen?
Das diskrete Logarithmus Problem

6 Alice und Bob wollen sich gegenseitig symmetrisch verschlüsselte Nachrichten schicken. Um sich auf einen zu nutzenden Schlüssel zu einigen nutzen sie den Diffie-Hellman-Schlüsselaustausch. Die öffentlichen Werte sind p_B = 97 und a = 29.

Alices geheimer Wert x_A ist 4; Bobs geheimer Wert x_B ist 7. Wie lautet das gemeinsame Geheimnis k_AB?

Antwort: 24

$Y_B = a^{x_B} \mod P_B \; Y_B = 29^7 \mod 97 \; Y_B = 37$

Key Agreement $k_{AB} = Y_B^{x_A} \mod P_B \; k_{AB} = 37^4 \mod 97 \; k_{AB} = 24$

7 Bob möchte Alice über das Internet das Ergebnis eines Würfelwurfs senden. Bob verschlüsselt das Ergebnis vor der Übertragung mit dem deterministischen RSA-Verfahren. Alice hat bereits ein RSA-Schlüsselpaar erzeugt und dabei die folgenden Parameter verwendet: p_A=5, q_A=11, e_A=3, d_A=27. Bob hat ebenfalls ein RSA-Schlüsselpaar erzeugt und dabei folgende Parameter verwendet: p_B=17, q_B=5, e_B=3, d_B=43.

Die öffentlichen Schlüssel haben die beiden bereits über einen authentifizierten Kanal ausgetauscht.

Bob hat gewürfelt und möchte das Ergebnis nun an Alice senden. Er überträgt dazu c_B=9.

Eine passive Angreiferin (Eve), die lediglich die öffentlichen Schlüssel und c_B kennt, kann mittels einer Chosen-Plaintext-Attack Bobs Wurfergebnis m_B ermitteln. Welche Zahl hat Bob gewürfelt?

Antwort: 4

```
In [ ]:
```