SMS1 für MC, FHS Hagenberg
10. Übungsblatt für den 22. Dezember 2005

Authentifizierung:

1. Lamport's OWF-based one-time passwords (siehe [1, 10.2.5]): Im folgenden übernehmen Sie die Rolle des Users A, der sich gegenüber einem System B identifizieren will. Sie einigen sich mit B auf die RSA-One-Way-Funktion $H(x) := x^9 \mod 135508573$ und auf eine Zahl von $t = 50$ Passwörtern. Als Ihr Geheimnis wählen Sie $w = 22122005$.

   Welchen Anfangswert w_0 übertragen Sie an B? Geben Sie das erste, zweite und 17te Passwort an, das Sie an B schicken.

2. Lamport's OWF-based one-time passwords (siehe [1, 10.2.5]): Im folgenden übernehmen Sie die Rolle des Systems B, dem gegenüber sich ein User A identifizieren will. Sie wissen, dass A die RSA-One-Way-Funktion $H(x) := x^3 \mod 3494122503799$ verwendet. Weiters haben Sie von A den Anfangswert $w_0 = 2648837217437$ für $t = 100$ erhalten.

   Bei aufeinanderfolgenden Übertragungen erhalten Sie von A jetzt die Nachrichten $w_1 = 1056628111157, w_2 = 49773944684, w_3 = 3083928538078, w_4 = 1162266204874$.

   Welche dieser Passwörter akzeptieren Sie?

3. Erklären Sie die wesentlichen Elemente des DES-Algorithmus zur symmetrischen Verschlüsselung [1, 7.4.2].

4. Verschlüsseln Sie die Nachricht "Heute ist der 22.12.2005." mit DES (ECB) und dem Schlüssel $k = 0123456789ABCDEF$ (in Hexadezimaldarstellung). Entschlüsseln Sie das Ergebnis dann wieder.

   Sie können dazu etwa das freie Paket "CrypTool" (`www.cryptool.de`) verwenden. Dort finden Sie DES unter dem Menüpunkt "Ver-/Entschlüsseln (Symmetrisch)". Schreiben Sie die Nachricht in eine Datei, die Sie verschlüsseln, und speichern Sie die verschlüsselte Datei.

5. Challenge-response based on symmetric key encryption; ISO/IEC 9798-2 mechanism, mutual authentication using random numbers (siehe [1, 10.16 (3)]): Im folgenden übernehmen Sie die Rolle von Alice, die sich gegenüber Bob identifizieren will. Sie haben sich mit Bob auf die Verwendung von DES (ECB) und den DES-Schlüssel ABCDEF0123456789 (in Hexadezimaldarstellung) geeinigt.

   Sie erhalten von Bob die Challenge $r_B = 1F5D6781E538BB92$, und wählen selbst eine Zufallszahl $r_A = 379BC3259873CDE1$. Was antworten Sie Bob?

Akzeptieren Sie Bobs Antwort E3 B4 B0 7A 48 6C 1B EC 9C 6A 90 7E 6E 98 98 1D 0B F7 39 5B 53 D3 44 76 3B 1C 7B 50 82 BA 42 AD (in Hex)?

Literatur

[1] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.