Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
PD Dr. Helmut Reiser, PD Dr. Wolfgang Hommel

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2012/2013
Übungsblatt 9

Abgabetermin: 23.01.2013 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per Email an die Adresse **uebung-itsec_AT_lrz.de** oder schriftlich vor der Übung). Während des Semesters werden vier Übungsblätter korrigiert. Bei vier richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei nur drei oder zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer drittel Notenstufe.

Aufgabe 21: (H) HMAC

Der HMAC mit 64 Bit Schlüssellänge wird wie in der Vorlesung definiert, berechnet. Gegeben sei eine Hashfunktion $H(x)$ und die 8 Byte langen hexadezimalen Konstanten $ipad = 3636363636363636$ und $opad = 5C5C5C5C5C5C5C5C$.
Es soll ein 128-bit langer Parameter P ausgetauscht werden, den es mit einem HMAC abzusichern gilt.

a. Gegeben sei der HMAC-Schlüssel $k = 9A45B7FE149BCE60$ und als Hashfunktion $H(x)$ der MD5 mit 128 Bit Ausgabelänge. Berechnen Sie den $HMAC_k(P)$ für den Parameter $P = 000102030405060708090A0B0C0D0E0F$. Benutzen Sie für die notwendigen MD5 Berechnungen die Tabelle auf dem Übungsblatt:

b. Nennen Sie jeweils einen Vorteil und Nachteil vom HMAC gegenüber einem asymmetrischen digitalen Signaturverfahren.

Aufgabe 22: (H) Authentisierung & Needham-Schröder

In der Vorlesung wurden verschiedene Varianten zur Authentisierung bei Verwendung symmetrischer, asymmetrischer Verschlüsselungsverfahren und Hash-Funktionen diskutiert. Außerdem wurde das Authentisierungsprotokoll Needham-Schröder unter Verwendung eines symmetrischen Verschlüsselungsverfahrens erläutert.

a. Skizzieren Sie den Ablauf, der auf Folie 43 in Kapitel 8 des Vorlesungsskriptes dargestellt ist unter Verwendung eines asymmetrischen Verschlüsselungsverfahrens. Dabei bezeichne Alice_S/Bob_S den privaten Schlüssel von Alice/Bob und Alice_P/Bob_P den dazu passenden öffentlichen Schlüssel.

Eingabe x (hex)	Ausgabe MD5(x) (hex)
0x1BAF81D154AD3D5600010203040506070809 0A0B0C0D0E0F	0xA339A0A2E397F5D59FFECED63B32B4FC
0x1B7381D122AD3D5600010203040506070809 0A0B0C0D0E0F	0x398A7DE773C25BE09AF3425D02EB216C
0x1B7381C822AD3D5601020304050607080 90A0B0C0D0E0F00	0xB9BFB2425097EE76B17C7AB7299F38D1
0x73DF81D154AD3D5600010203040506070809 0A0B0C0D0E0F	0xB239A0A2E397F5D59FFECED63B32755D
0x737381D122AD3D5600010203040506070809 0A0B0C0D0E0F	0x88D37DE773C25BE09AF3425D02EB218C
0x737399C822AD3D5601020304050607080 90A0B0C0D0E0F00	0xA23FB2425097EE76B17C7AB7299F3444
0xAC3881C822AD3D5601020304050607080 90A0B0C0D0E0F00	0xA95BBB4FF0A7511D07DC5CA6ACA6BE2E
0xAC7381C822ADF8560001020304050607080 90A0B0C0D0E0F	0x0898721134D8E73D7F0209244CFC733F
0xAC7393B143ADF8560001020304050607080 90A0B0C0D0E0F	0x58460D74328B15CC0E1B1FCF811E1621
0xC619EBA248C7923C0898721134D8E73D7F0209244CFC733F	0xA4167961D793AE17467720AB1C636951
0xC619EBF623542A340898721134D8E73D7F0209244CFC733F	0xDCB9C8C90936A7F26DC40C5403334AC8
0xC63AD4F623542A340898721134D8E73D7F0209244CFC733F	0x36165CCD748C4F0DA3CD51D83A5EA2BE
0xBB19EBA248C7923CB9BFB2425097EE76B17C7AB7299F38D1	0xB2167961D748AE17467720AB1C636425
0xBB59EBF623542A3458460D74328B15CC0E1B1FCF811E1621	0x14DFC8C90936A7F26DC40C54033388C3
0xBB3AD4F623542A340898721134D8E73D7F0209244CFC733F	0x54AB5CCD748C4F0DA3CD51D83A5ECC8B
0xFE19EBA248C7923CA339A0A2E397F5D59FFECED63B32B4FC	0x125388B1D748AE17467720AB1C9476D3
0xFE59EBF623542A3458460D74328B15CC0E1B1FCF811E1621	0xFF33236AF936A7F26DC40C540940ABE1
0xFE5D3AF623542A34B239A0A2E397F5D59FFECED63B32755D	0xCC325CCD748C4F0DA3CD51D83A19DA1F

b. Skizzieren Sie den Nachrichtenfluss der zum Verbindungsaufbau im Rahmen des Needham-Schröder-Verfahrens benötigten Pakete zwischen Alice und Bob bei Verwendung asymmetrischer Verschlüsselung. Den Kommunikationspartnern sei der öffentliche Schlüssel K_T von Trent T bekannt. Trent kennt andererseits die öffentlichen Schlüssel aller Beteiligten (K_A für Alice, K_B für Bob).

c. Die symmetrische Protokollvariante von Needham-Schröder besitzt eine bekannte Schwäche für Replay-Attacken bei bekanntem Session-Key. Erläutern Sie das Problem und beheben Sie dessen Ursache!

Aufgabe 23: (K) Kerberos

Ein weitverbreitetes Protokoll zur Benutzerauthentisierung ist Kerberos. Beschreiben Sie den Ablauf sowie den konkreten Aufbau der ausgetauschten Nachrichten anhand des folgenden Beispiel-Szenarios:

a. Sie kommen um 08:00 Uhr in die Arbeit und loggen sich mit Ihrem Nutzernamen *zdf26395* und zugehörigem Passwort *3z!fG7qiT* ein. An welche an Kerberos-beteiligte Komponente werden diese Informationen übermittelt? Wie sieht die zugehörige Nachricht aus?

b. Die Antwort, die Sie auf Ihre erste Nachricht in Teilaufgabe a) erhalten ist verschlüsselt. Welcher Schlüssel wurde hierzu verwendet? Welche Informationen werden in dieser Antwort-Nachricht übertragen?

c. Sie arbeiten gerade an einem Text-Dokument, welches Sie nun ausdrucken wollen. Die Steuerung des Druckers erfolgt über einen dedizierten Print-Server. An welche Kerberos-Komponente müssen Sie Ihre Druck-Anfrage übermitteln und welche Informationen enthält diese? Welchen Inhalt hat die entsprechende Antwortnachricht?

d. Welche Schritte sind abschließend zu durchlaufen, damit Ihr Dokument ausgedruckt wird?