Klausur 1866 Sicherheit im Internet I
Klausur am 15. September 2007

Lösungsvorschläge

Prof. Dr. J. Keller
LG Parallelität & VLSI

Aufgabe 1: **(12 Punkte)**

Erklären Sie kurz (3–4 Sätze) und in eigenen Worten die wesentlichen Schutzziele, die ein sicheres System erreichen sollte.

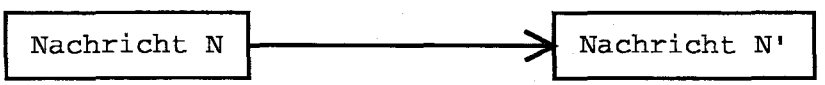
Lösung: *Das Schutzziel* (1) Vertraulichkeit *besagt, daß Daten/Informationen nur den befugten Personen/Systemen zugänglich sind, bzw. nur von diesen zur Kenntnis genommen werden können. Andere Personen, z.B. Angreifer können keine Kenntnis der vertraulichen Informationen erhalten.*
Das Schutzziel (2) Integrität *besagt, daß Daten oder Systeme nicht unbemerkt manipuliert werden können. Alle Veränderungen müssen entweder unmöglich sein oder zumindest erkannt werden können.*
Das Schutzziel (3) Authentizität *bedeutet, daß man die Herkunft von Daten bestimmten Personen oder Systemen eindeutig zuordnen kann. Das bedingt natürlich, daß man Personen und Systeme auch eindeutig unterscheiden können muß.*
Das Schutzziel (4) Verfügbarkeit *verlangt, daß Systeme ihren legitimen Benutzern immer dann zur Verfügung stehen müssen, wenn die Benutzer sie benutzen wollen. Immer bedeutet hier aber nicht jederzeit, sondern es sind auch sog. Wartungsfenster erlaubt. In dieser Zeit wird ein System vom Administrator gepflegt und steht den Benutzern möglicherweise nicht zur Verfügung.*

Aufgabe 2: **(18 Punkte)**

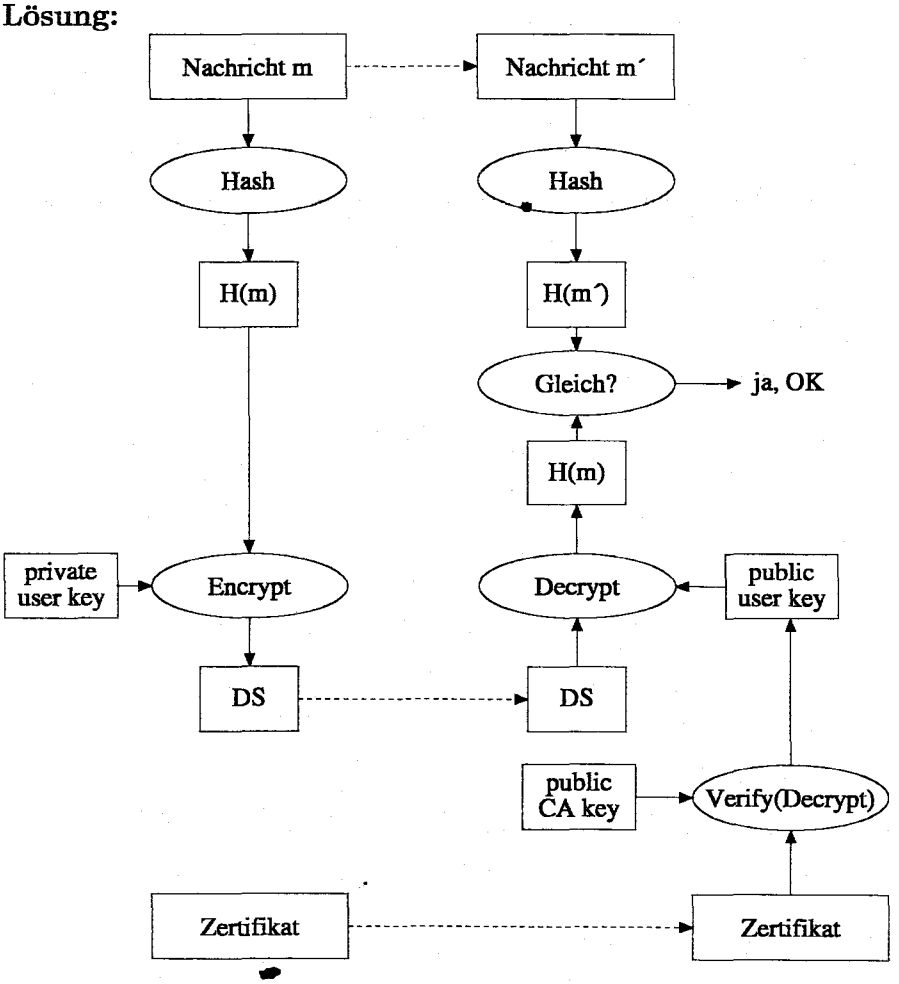
Skizzieren Sie den Ablauf bei der Überprüfung der Authentizität einer Nachricht. Dabei sendet der Absender die Nachricht N an den Empfänger, der eine Nachricht N' empfängt (siehe Bild unten). Zeichnen Sie dazu Pfeile und weitere Rechtecke und Ovale in das unten beginnende Bild ein: Dabei haben die Symbole die folgende Bedeutung:

Symbol	Bedeutung
Pfeil	Daten werden übertragen (von/zu Operationen/Daten)
Rechteck	Daten (im Rechteck Beschreibung der Daten)
Oval	Operation (im Oval Beschreibung der Operation)

Gehen Sie davon aus, daß der Empfänger den öffentlichen Schlüssel des Absenders noch *nicht* vorliegen hat.
Beginn des Bildes:



Lösung:



Aufgabe 3: **(5 + 15 = 20 Punkte)**

Gegeben sei ein „einfaches" Kerberos System (also ohne TGS). Ein Hacker kontrolliert das Netz, d.h. er kann Pakete abfangen, unterdrücken oder modifiziert weiter leiten. Außerdem hat der Hacker einen gefälschten Server (engl. fake server) installiert. Siehe hierzu Abbildung 1.

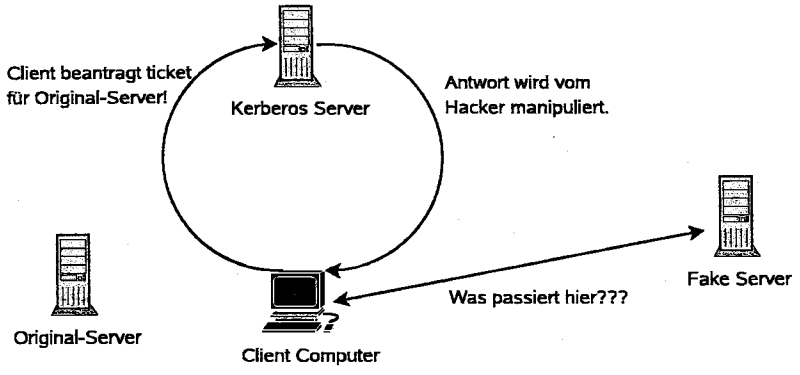


Abbildung 1: Kerberos in einem manipulierten Netz

Ein Benutzer kontaktiert nun den Kerberos Server und beantragt ein ticket für den Original-Server. Der Hacker fängt die Antwort des Kerberos-Servers ab, entfernt das Original-Ticket, fügt ein gefälschtes Ticket für seinen „fake server" ein und läßt den Rest der Antwort unverändert. Außerdem hat der Hacker den DNS-Server manipuliert, so daß alle Client Nachrichten an den Original-Server tatsächlich an den fake server gesendet werden.

a) Was steht alles in der gefälschten Antwort (des AS) die der Client empfängt?

Lösung: *In der Nachricht steht (1) das gefälschte Ticket, (2) der mit dem Client-Key verschlüsselte Session-Key (der auch im Original-Ticket steckte) und (3) ein time stamp t_1.*

b) Was passiert wenn der Client sich mit dem Original-Server verbinden will und tatsächlich beim fake server landet? Erklären Sie Ihre Antwort.

Lösung: *Der Client leitet das ticket einfach weiter. Außerdem verschlüsselt er mit dem Session Key einen Authenticator (t_2) in dem sein Name und ein weiterer time stamp stehen. Der fake server muß nun diesen Authenticator entschlüsseln und dem Client eine Antwort senden, die auf dem Inhalt des Authenticators basiert. Da der fake server aber den vom Client benutzten Session Key nicht kennen kann (der Stand für den Original-Server im Original-Ticket; verschlüsselt mit dem Schlüssel des Original-Servers), kann er den Authenticator nicht entschlüsseln und somit auch keine korrekte Antwort an den Client senden. Daran erkennt der Client, daß er nicht mit dem richten Server verbunden ist und bricht die Verbindung ab.*

Aufgabe 4: **(5 + 5 = 10 Punkte)**

a) Gegeben seien ein öffentlicher RSA-Schlüssel (e, n) und der zugehörige private RSA-Schlüssel (d, n).

Welche Berechnung findet bei der Verschlüsselung statt, welche bei der Entschlüsselung?

- Verschlüsselung:

Lösung: *Bei der Verschlüsselung einer Nachricht x wird $V(x, e) = x^e \bmod n$ berechnet.*

- Entschlüsselung:

Lösung: *Bei der Entschlüsselung einer verschlüsselten Nachricht y wird $E(y, d) = y^d \bmod n$ berechnet.*

b) Kann man bei RSA auch mit dem privaten Schlüssel verschlüsseln und anschließend mit dem öffentlichen Schlüssel wieder entschlüsseln? Begründen Sie Ihre Antwort.

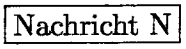
Lösung: *Ja man kann. Begründung: Wenn man x erst mit dem privaten Schlüssel (d, n) verschlüsselt, dann berechnet man: $x^d \bmod n$. Anschließendes entschlüsseln liefert $(x^d \bmod n)^e \bmod n$ und das ist $x^{(d \times e)} \bmod n$ und das ist gleich $x^{(e \times d)} \bmod n$ weil die Multiplikation kommutativ ist. Es kommt also dasselbe heraus wie beim Verschlüsseln mit dem öffentlichen Schlüssel und dem anschließenden Entschlüsseln mit dem privaten Schlüssel.*

Aufgabe 5: **(15 + 5 = 20 Punkte)**

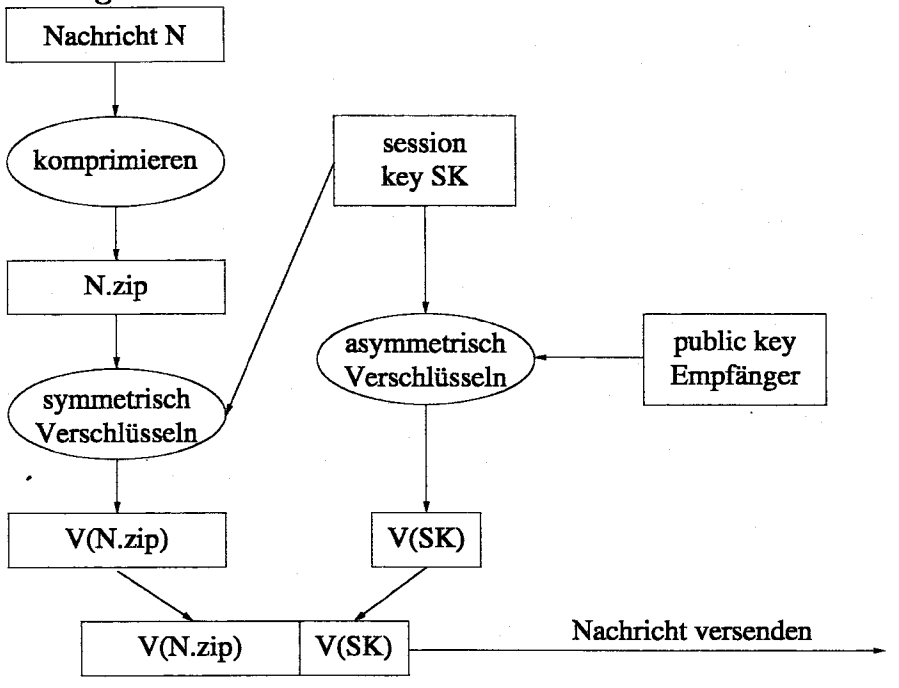
In dieser Aufgabe geht es um die Verschlüsselung mit PGP bzw. GnuPG.

a) Skizzieren Sie die Schritte die ausgeführt werden wenn PGP eine Nachricht N für einen Benutzer X verschlüsselt. Vervollständigen Sie die folgende Grafik mit Kästchen (für Daten), Pfeile (für den Transport von Daten) und Ovale (für Operationen).

Anfang der Abbildung:



Lösung:



b) Was macht PGP wenn die Nachricht M an Benutzer X und Benutzer Y geschickt werden soll?

Lösung: *Der erzeugte session key wird asymmetrisch für beide Benutzer verschlüsselt und in die Nachricht eingefügt. Die endgültige Nachricht besteht aus drei Teilen, (1) der mit dem session key symmetrisch verschlüsselten Nachricht ($V(N.zip)$), (2) dem mit dem public key von X asymmetrisch verschlüsselten session key ($V(SK)$) und (3) dem für Benutzer Y asymmetrisch verschlüsselten session key (nicht im Bild dargestellt).*

Aufgabe 6: **(5 + 5 + 10 = 20 Punkte)**

a) Was bedeutet es, wenn eine Zahl g primitiv modulo p (p sei eine Primzahl) ist?

Lösung: *Zu jeder Zahl $y \neq 0$ aus Z_p existiert eine Zahl x aus Z_p mit: $g^x \bmod p = y$.*

b) Zeigen oder widerlegen Sie, daß 3 primitiv modulo 5 ist.

Lösung: *Drei ist primitiv modulo fünf, denn:*
$3^0 \bmod 5 = 1$
$3^1 \bmod 5 = 3$
$3^2 \bmod 5 = 4$
$3^3 \bmod 5 = 2$
$3^4 \bmod 5 = 1$
Zu jeder Zahl y aus Z_p ohne 0 existiert ein Exponent x, so daß $3^x \bmod 5 = y$ gilt.

c) Schildern Sie den Diffie-Hellmann-Schlüsselaustausch zwischen zwei Parteien A und B.

Lösung: *Die Parteien A und B einigen sich zuerst auf eine große Primzahl p und eine Zahl g die primitiv modulo p ist. Diese Zahlen dürfen bekannt sein. A wählt zufällig eine Zahl a_x und schickt $a_y = g^{a_x} \bmod p$ an B. B wählt eine Zahl b_x und schickt $b_y = g^{b_x} \bmod p$ an A. A berechnet aus b_y und seinem geheimen Wert a_x : $b_y^{a_x} \bmod p$. B berechnet $a_y^{b_x} \bmod p$. A und B haben nun beide denselben Wert berechnet. Jemand der den Kommunikationskanal abhört, kennt nur g, p, a_y und b_y und kann den berechneten Wert nicht rekonstruieren.*