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 7

Abgabetermin: 09.01.2013 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 16: (H) Asymmetrische Verschlüsselung

a. Welche Probleme der symmetrischen Verschlüsselung löst die asymmetrische Verschlüsselung?

b. Welche Probleme der asymmetrischen Verschlüsselung löst hingegen die symmetrische Verschlüsselung?

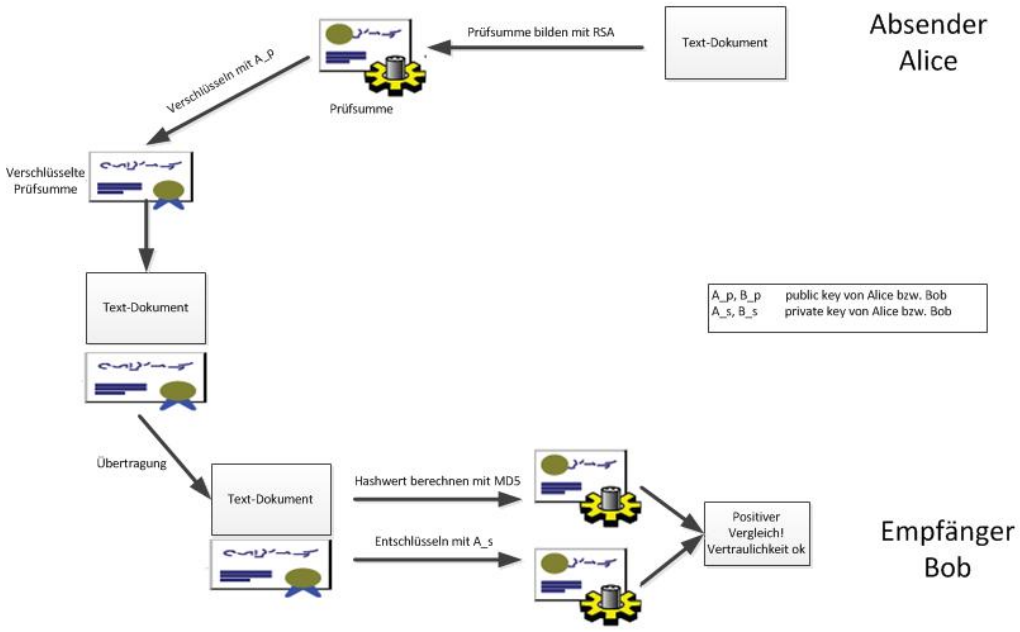
c. Welche Probleme der symmetrischen und asymmetrischen Verschlüsselung löst eine hybride Verschlüsselung?

d. Gegeben sei folgender Ablauf (s. Abbildung unten) für eine digitale Signatur, in dem mehrere Fehler enthalten sind. Finden und korrigieren Sie diese, damit die Signatur und deren Verifikation korrekt durchgeführt wird. Geben Sie auch an, welche(s) Sicherheitsziel(e) erreicht werden können.

e. Auf der Vorlesungswebseite finden Sie im Abschnitt *Übung* ein Text-Dokument. Sie wollen dieses digital mit dem RSA-Verfahren signieren. Verwenden Sie dazu als Hash-Algorithmus MD5 (Befehl *md5sum*), nehmen Sie vom MD5-Hash die ersten 2 Bytes und verwenden sie diese als Klartext-Nachricht m. Parametrisieren Sie im Hashwert enthaltene Buchstaben analog zu Aufgabe 14d, d.h. der Buchstabe *A* wird bspw. auf den Wert *01* abgebildet. Führende Nullen werden ignoriert. Achten Sie darauf, dass ihr selbstgewählter RSA-Modul groß genug ist und verwenden Sie den Verschlüsselungsexponenten $e = 257$. Berechnen Sie den dazu passenden Wert von d und verifizieren Sie die Signatur.

Aufgabe 17: (H) Hash-Funktionen

Zum Erreichen der Sicherheitsziele Vertraulichkeit, Integrität und Authentizität werden unterschiedliche Mechanismen verwendet.



a. Erläutern Sie das Merkle-Damgard-Prinzip zur Konstruktion sicherer Hashfunktionen.

b. Nachdem die Funktionsweise des Conficker-Virus Version A bekannt war, waren die Autoren des Virus gezwungen das auf einem mit dem Virus infizierten System installierte Binary, das für die Verbindung zum Command&Control-Server verantwortlich war, auszutauschen.

   (i) Angenommen wird, dass in einem ersten Schritt das neue 166 Byte lange Binary mit dem Algorithmus MD5 gehasht wird. Skizzieren Sie welche Schritte des Algorithmus zu durchlaufen waren. Der MD5-Hash wird mit M bezeichnet.

   (ii) Das Windows-Binary wurde mit der Stromchiffre RC4 und Schlüssel M verschlüsselt. Das Ergebnis lautete *enc.bin*. Um zusätzlich die Authentiztät zu gewährleisten, wurde ein asymmetrisches Verschlüsselungsverfahren mit privatem Schlüssel e^{priv} und öffentlichem Schlüssel e^{pub} angewendet. Wie lautet die Berechnungsvorschrift für eine digitale Signatur, wenn der eingebettete Modulus N lautet?

   (iii) Nach Übertragung über das Internet musste die Korrektheit verifiziert werden. Mit welcher Vorschrift kann der Hash-Wert M berechnet werden?

   (iv) Zum Entschlüsseln von enc.bin wurde erneut RC4 verwendet. Wie können Sie sicherstellen, dass bei der Übertragung keine Fehler auftraten?

Aufgabe 18: (Z) (optional) RSA-Verschlüsselung

Die folgende Nachricht **68094034 128468343 143911297 122013244** wurde mit dem RSA-Verfahren mit den Parametern N=289648273 und e=17 verschlüsselt. Dabei wurde wie folgt vorgegangen: Der alphanumerische Klartext wurde zu Gruppen von je 3 Buchstaben zusammengefasst. Jeder solcher Dreiergruppen xyz, mit $x, y, z \in \{A, B, \ldots, Z\}$ wurde die Zahl $W(xyz) := w(x) \cdot 26^2 + w(y) \cdot 26 + w(z) \mod N$ zugeordnet, wobei $w : \{A, B, \ldots, Z\} \to \{0, 1, \ldots, 25\}$ jedem Buchstaben einen Wert anhand der Tabelle

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25