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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2014/2015
Übungsblatt 9

Abgabetermin: 13.01.2015 bis 12:00 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 (über Uniworx als Einzelabgabe). Während des Semesters werden vier Übungsblätter ausgewählt, korrigiert und bewertet. Bei vier als korrekt bewerteten Lösungen (mind. 75% der erreichbaren Punkte) 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 20: **(H)** Asymmetrische Kryptographie & RSA (17 Punkte)

In der Vorlesung wurden symmetrische, asymmetrische und hybride Kryptosysteme im Detail erläutert.

a. Erläutern Sie knapp die Eigenschaften asymmetrischer Verschlüsselung.

b. Welche Probleme der symmetrischen Verschlüsselung löst die asymmetrische Verschlüsselung? Welche hingegen nicht bzw. welchen gravierenden Nachteil weist sie auf?

c. Wieviele Schlüssel benötigen Sie, wenn 10 Personen paarweise miteinander, abgesichert mithilfe eines symmetrischen Verschlüsselungsverfahrens kommunzieren wollen.

d. Eine potentiell geeignete Lösung für das Schlüsselsaustausch-Problem symmetrischer Verschlüsselungsverfahren stellen sog. *Key Distribution Center* (KDC) dar. Erläutern Sie knapp wie die Kommunikation zwischen den Teilnehmern Alice und Bob unter Verwendung eines zentralen KDC grundsätzlich ablaufen könnte (Tipp: Sitzungsschlüssel!). Nennen Sie außerdem mindestens einen gravierenden Nachteil des Einsatzes eines zentralen KDC.

e. Alice und Bob wollen auf einem sicheren Weg eine Nachricht m austauschen. Gleichzeitig soll Bob in der Lage sein, die Authentizität der Nachricht zu überprüfen. Welche Schritte sind bei Verwendung asymmetrischer Verschlüsselung zu durchlaufen? Welchen Vorteil hätte man, wenn man statt eines asymmetrischen Verfahrens ein hybrides Verfahren einsetzen würde?

f. Erläutern Sie knapp die Funktionsweise des RSA Verfahrens. Welchen Besonderheit im Hinblick auf die Wahl der Primzahlen p und q erkennen Sie in RFC 3447 (PKCS#1 RSA Cryptography Specification)?

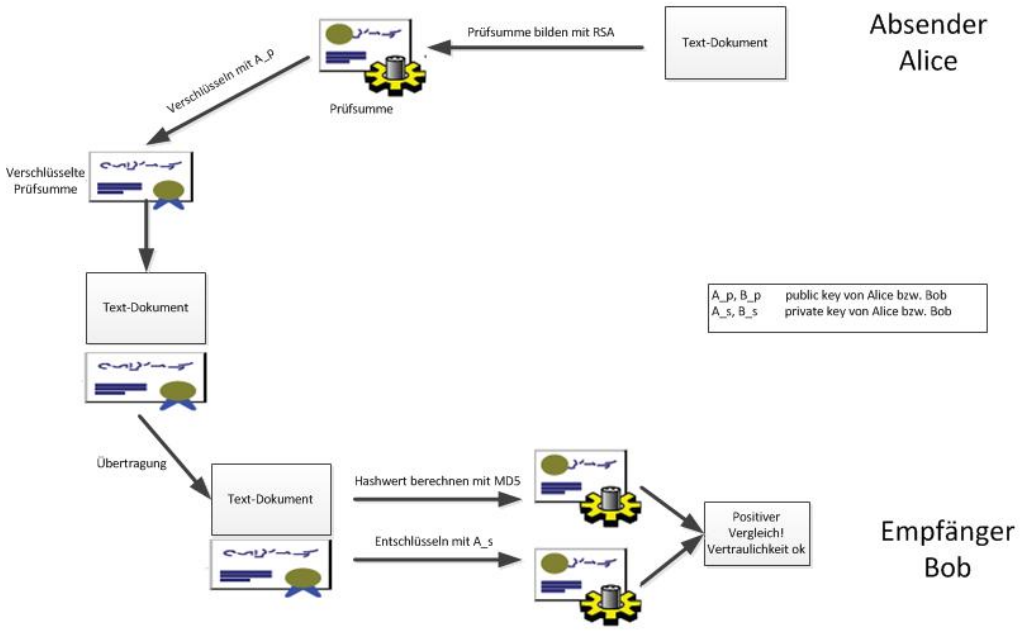

Abbildung 1: Fehlerhafter Ablauf einer digitalen Signatur

g. Gegeben seien zwei Primzahlen $p = 11$ und $q = 31$, sowie die ganzzahlige Klartext-Nachricht $m = 12$. Berechnen Sie den Chiffretext mithilfe des in der Vorlesung beschriebenen RSA-Verfahrens, verwenden Sie hierbei als Verschlüsselungsexponent $e = 17$. Achten Sie darauf, dass ihr Lösungsweg nachvollziehbar ist!

h. Überprüfen Sie Ihr in der vorherigen Teilaufgabe berrechnetes Ergebnis durch Entschlüsselung. Achten Sie darauf, dass insbesondere die Berechnung des Exponenten d nachvollziehbar ist.

i. Verschlüsseln Sie mit dem RSA-Verfahren den String *IT*. Die Ganzzahl-Codierung für Buchstaben laute $A = 01$. $B = 02, \ldots, Z = 26$. Wählen Sie geeignete Primzahlen p und q, sodass Ihr RSA-Modul für die Verschlüsselung ausreichend groß ist. Berechnen Sie den Chiffretext, verwenden Sie hierzu für den Verschlüsselungsexponenten $e = 257$. Überprüfen Sie auch hier Ihre Berechnung durch eine anschließende Entschlüsselung.

j. Abbildung 1 zeigt den generellen Ablauf für eine digitale Signatur, in dem jedoch 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 und begründen Sie ihre Antwort kurz.

Aufgabe 21: (H) Schlüssellängen und Komplexitätsabschätzungen (5 Punkte)

a. Wie lange dauert es, mit einem gegebenen Rechner (1 CPU-Kern, 3 GHz, ca. $3 * 10^6$ Schlüssel pro Sekunde) einen symmetrischen Schlüssel der Länge 56 Bit / 128 Bit mittels Brute Force zu brechen?

b. Nehmen wir an, Sie könnten die Brute-Force-Attacke beliebig parallelisieren und Ihnen stünden 100.000 CPU-Kerne zur Verfügung. Wie würden sich dadurch die Zeiten für das Erraten der symmetrischen Schlüssel der Länge 56 Bit / 128 Bit ändern?

c. In Ihrem Unternehmen wurde eine Passwortrichtline eingeführt: „Ein Passwort muss mindestens 8 Zeichen, davon mindestens 2 Ziffern oder Sonderzeichen enthalten.“ Welche Komplexität erhofft sich ein Sicherheitsverantwortlicher dadurch (deutsche Tastatur)?

d. Welche Komplexität wird Ihrer Meinung nach wirklich erreicht?

e. Ein Kollege meint, ein Passwort nach der Richtline „kombiniere 4 beliebige Worte“ wäre der Komplexität nach sicherer. Stimmt dies?

Aufgabe 22: (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

Wie lautete die Nachricht im Klartext? Für Berechnungen mit großen Zahlen können Sie auf Computeralgebra-Systeme, z.B. Wolfram-Alpha o.ä. zurückgreifen.