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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2024/2025
Übungsblatt 8

Besprechung: Do, 19.12.2024 um 14:00 Uhr

Aufgabe 1: (T) Schlüssellängen und Komplexitätsabschätzungen

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 2: (T) Verschlüsselung und RSA

In der Vorlesung wurden symmetrische, asymmetrische und hybride Kryptosysteme im Detail erläutert. Der Algorithmus RSA wurde in PKCS#1 spezifiziert.

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

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

c. Gegeben seien zwei Primzahlen $p = 11$ und $q = 31$, sowie die ganzzahlige Klartext-Nachricht $m = 12$. Berechnen Sie den Chiffretext mithilfe des RSA-Verfahrens, verwenden Sie hierzu als Verschlüsselungsexponent $e = 17$. Achten Sie darauf, dass ihr Lösungsweg nachvollziehbar ist und überprüfen Sie Ihr Ergebnis durch entsprechendes Entschlüsseln.

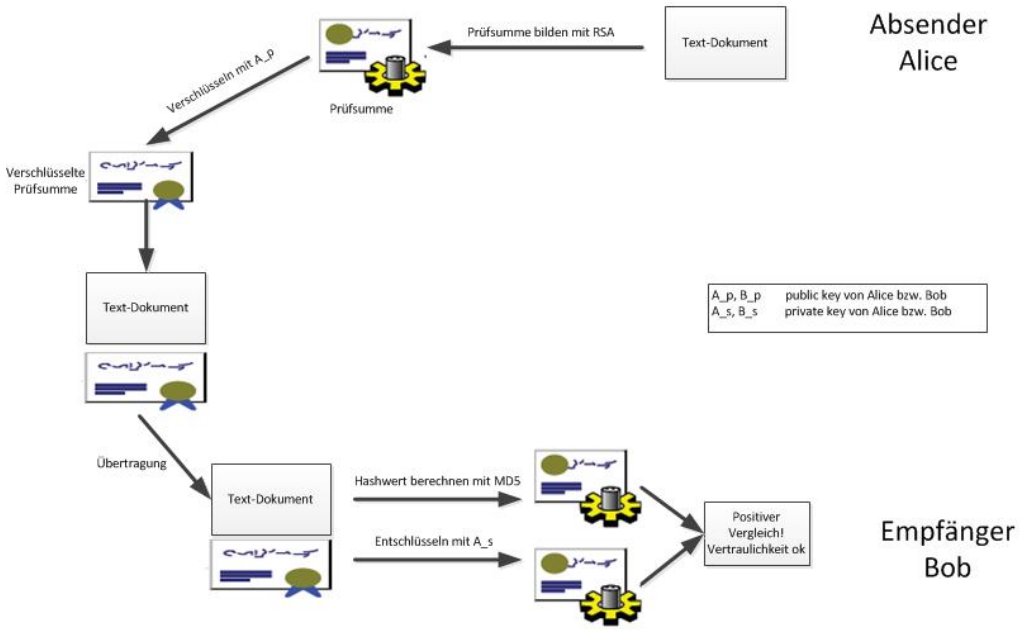

Abbildung 1: Fehlerhafter Ablauf einer digitalen Signatur

d. 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 3: (H) RSA-Verschlüsselung dechiffrieren

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.