

Übung 3: asymmetrische Verfahren und Signatur

Abgabetermin im Moodle-Forum im PDF-Format: 12. Mai 2014

Aufgabe 1

Angenommen, drei Personen wollen paarweise sicher miteinander kommunizieren. Wie viele Schlüssel werden benötigt, wenn sie sich für ein symmetrisches bzw. asymmetrisches Verfahren entscheiden? Wie sieht das bei 50 Kommunikationspartnern aus? Und allgemein für n Personen?

Anzahl der Kommunikationspartner	Benötigte Schlüssel für symmetrisches Verfahren	Benötigte Schlüsselpaare für asymmetrisches Verfahren
3		
50		
n		

Aufgabe 2

GnuPG ist eine freie Implementierung des OpenPGP-Standards und kann als Backend für viele Sicherheitslösungen dienen. Es implementiert unter anderem auch den besprochenen RSA-Algorithmus. Installiere GnuPG und ein passendes graphisches Frontend für deinen Email-Client (z.B. EnigMail für Thunderbird).

Aufgabe 3

Schreibe mir (mi.gamper@tsn.at) eine geheime E-Mail-Nachricht und **verschlüssele** diese mit Hilfe von GnuPG. Sorge dafür, dass nur ich diese Nachricht auch wieder entschlüsseln kann.

Aufgabe 4

Sorge dafür, dass ich sicherstellen kann, dass die obige Nachricht wirklich von dir ist. **Signiere** die Nachricht mit Hilfe von GnuPG.

Aufgabe 5

Stärke unser **Personal Web of Trust**, indem du meinen Public Key unterschreibst und damit bestätigst, dass der Public Key wirklich der von Michael Gamper ist.

Aufgabe 6

Um die Unversehrtheit eines Dokuments zu gewährleisten, wird auf vielen Downloadportalen der Hash-Wert des Programms angezeigt. Besonders in sicherheitskritischen Systemen, sollte nach dem Download und vor dem Ausführen der Hashwert mit dem Hash auf dem Portal verglichen werden. Überprüfe und dokumentiere den Hash des von dir heruntergeladenen Programms GnuPG.

Hash:

Aufgabe 7

MD5 gilt u.a. auf Grund der vergleichsweise hohen Kollisionswahrscheinlichkeit als unsicher. Weshalb relativiert sich dieser Umstand im Zusammenhang mit Hashes auf Download-Portalen?

Aufgabe 8

Überprüfe, ob dieses Dokument digital signiert ist. Wer hat nachweislich unterschrieben?

Vertraust du dieser Unterschrift?

Wäre diese Unterschrift rechtlich bindend?


Wäre diese Unterschrift auch gültig, wenn das Dokument nur in ausgedruckter Form vorliegen würde?

Aufgabe 8 (optional)

Informiere dich auf [Bürgerkarte.at](http://Buergerkarte.at) über die Möglichkeiten, Vorteile und Risiken der österreichischen Bürgerkarte. Falls deiner Meinung nach die Vorteile überwiegen, aktiviere den Dienst für dein Handy bzw. deine E-Card.

Aufgabe 9 (optional)

Thema „Speichern von Passwort-Hashes“. Verändere dein PHP-Projekt aus POS bzw. dein DA-Projekt so, dass nicht ausschließlich die Passwörter als Input für die Hash-Funktion verwendet werden. Füge einen Salt (und/oder Pepper) hinzu. Präsentiere deine Lösung bei Gelegenheit im DS-Unterricht und adaptiere die schriftliche Doku deiner Arbeit.

Signaturwert	kV+6qlAb1WuXAHlaJKFSqfKmuXW5ZGOBIhvT3i6g3QsfuFxaJfzqOm/tOnGQJzTU2I90KPuHsFtW899pen8xA==	
	Unterzeichner	Michael Gamper
	Aussteller-Zertifikat	CN=a-sign-premium-mobile-03,OU=a-sign-premium-mobile-03,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	562585
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:vl.1.0
	Parameter	etsi-bka-atrust-1.0:ecdsa-sha256:sha256:sha256:shal
Prüfinformation	Signaturprüfung unter: http://www.signaturpruefung.gv.at	
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument ist gemäß § 4 Abs. 1 Signaturgesetz einem handschriftlich unterschriebenen Dokument grundsätzlich rechtlich gleichgestellt.	
Datum/Zeit-UTC	2014-04-28T09:59:57Z	