

Asymmetrische Verschlüsselungsverfahren

erarbeitet von: Emilia Winkler
Christian-Weise-Gymnasium Zittau

Gliederung

- 1) Prinzip der asymmetrischen Verschlüsselungsverfahren
- 2) Vergleich mit den symmetrischen Verschlüsselungsverfahren (Vor- und Nachteile)
- 3) hybride Verschlüsselungsverfahren
- 4) das Verfahren El Gamal
- 5) Quellen

Asymmetrische Verschlüsselungsverfahren

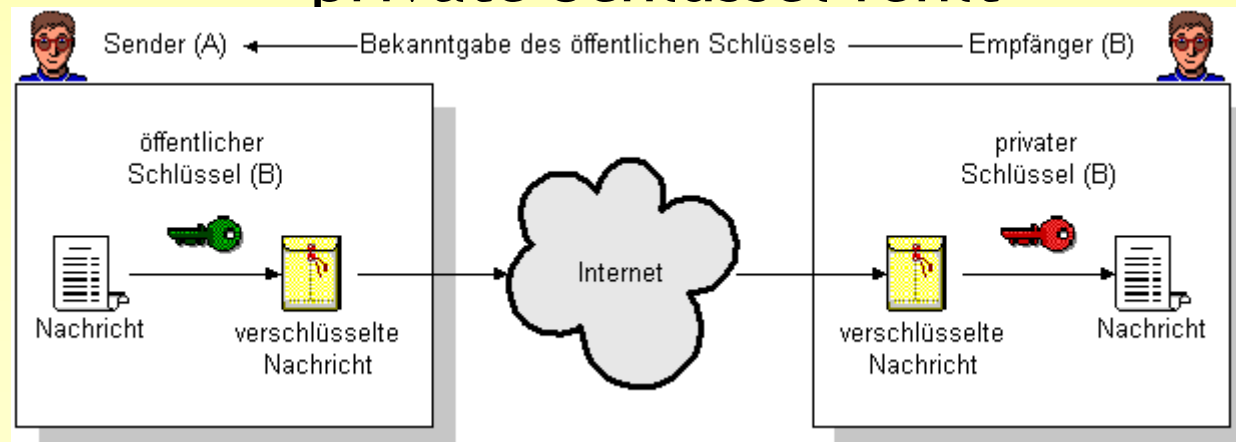
- Form der Datenverschlüsselung
- bekannt seit 1978
- Basis: zusammengehörendes Schlüsselpaar
- öffentlicher Schlüssel (public key)- Verschlüsselung
- privater Schlüssel (private key)- Entschlüsselung
- kein Schlüssel kann aus dem anderen hergeleitet werden

Prinzip der asymmetrischen Verschlüsselungsverfahren

- Empfänger generiert 2 verschiedene Schlüssel
- privater Schlüssel ist nur ihm bekannt und bleibt auch bei ihm
- öffentlicher Schlüssel wird dem Sender bekannt gemacht
- jeder darf den öffentlichen Schlüssel des Empfängers besitzen
- mit der Kenntnis des öffentlichen Schlüssels kann jeder für den Empfänger eine Nachricht verschlüsseln

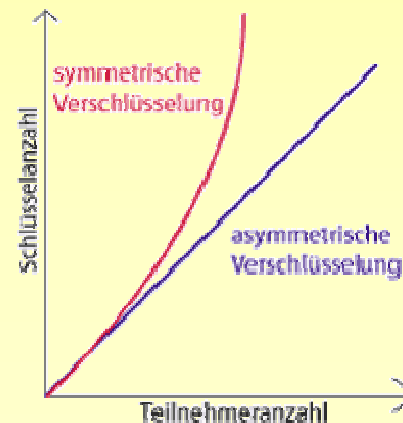
Prinzip der asymmetrischen Verschlüsselungsverfahren

- diese kann nur noch der Empfänger mit seinem privaten Schlüssel entschlüsseln
- wenn die Nachricht einmal verschlüsselt ist, kann der Sender sie nicht mehr entschlüsseln
- selbst wenn jemand den verschlüsselten Text und den öffentlichen Schlüssel abfängt, kann er die Nachricht noch nicht entschlüsseln, weil ihm der private Schlüssel fehlt



Vergleich mit symmetrischen Verschlüsselungsverfahren

<u>Asymmetrische</u>	→ ←	<u>Symmetrische</u>
hohe Sicherheit	→ ←	geringe Sicherheit
wenig Schlüssel	→ ←	enorm viele Schlüssel
Geheimnis bleibt klein	→ ←	Geheimhaltung schwierig
keine Probleme bei Schlüssel- verteilung	→ ←	Feind kann Schlüssel bei Übertragung abfangen
Authentifikation möglich		
Aufwand der „illegalen“		
Entschlüsselung hoch		



Vergleich mit symmetrischen Verschlüsselungsverfahren

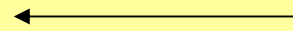
Asymmetrische

langsame Rechenzeit →

hoher Aufwand →

Sicherheit nicht bewiesen

Mittelsmannangriffe



Symmetrische

schnell

Aufwand gering

einfaches Schlüssel-
management

Hybride Verschlüsselungsverfahren

- > Kombination von symmetrischer und asymmetrischer Verschlüsselung
- Vorteile beider Verfahren genutzt:
 - * Schnelligkeit von symmetrischer Verschlüsselung
 - * Sicherheit von asymmetrischer Verschlüsselung
- verschicken von großen Datenmengen möglich
- heutzutage häufig eingesetzt

Hybride Verschlüsselungsverfahren

- reine Nutzdateien werden symmetrisch verschlüsselt
- Sender erstellt einen zufälligen symmetrischen Schlüssel -> „session key“
- dieser wird anschließend mit dem öffentlichen Schlüssel des Empfängers asymmetrisch verschlüsselt
 - > Schlüsselverteilungsproblem wird gelöst
- arbeiten schnell und sicher
- Empfänger entschlüsselt den „session key“ mit seinem eigenen privaten Schlüssel

Hybride Verschlüsselungsverfahren

- Daten an sich werden mit dem „session key“ ver- und entschlüsselt
- Empfänger kann mit dem „session key“ die eigentliche Nachricht entschlüsseln
- Nachteil der langsamen asymmetrischen Verschlüsselungsverfahren hier nicht entscheidend

Das Verfahren El Gamal

- 1985 von Taher El Gamal entwickelt
- = asymmetrischer Verschlüsselungsalgorithmus
- beruht auf diskretem Logarithmus (diskret= ganzzahlig)
oder Einwegfunktionen



f ist eine Einwegfunktion, wenn:

- * man $f(x)$ effizient berechnen kann, aber
- * kein effizientes Verfahren existiert, um x aus $f(x)$ zu berechnen
- * Bsp: $f(\text{Telefon})$: Name

Das Verfahren El Gamal

- baut auf Idee des Diffie-Hellman- Algorithmus auf
- Prinzip: öffentlicher und geheimer Schlüssel
- Schlüsselerzeugung kann mathematisch genau beschrieben werden
- man benötigt: * Primzahl p
 - * Primitivwurzel $g \bmod p$
 - * zufälliges $a \in \{2 \dots p-2\}$

-> $A = g^a \bmod p$
- öffentlicher Schlüssel: Tripel (p, g, A)
- geheimer Schlüssel: a

Das Verfahren El Gamal

- Sender wählt ein zufälliges $b \in \{1, \dots, p-2\}$
- $B = g^b \text{ mod } p$
- Klartext m wird verschlüsselt mit: $c = A^b m \text{ mod } p$
- Geheimtext (B, c) wird an Empfänger gesendet
- mit dem geheimen Schlüssel a kann der Empfänger die Nachricht wieder in Klartext verwandeln
- $m = B^x c \text{ mod } p \quad (x = p-1-a)$
- sehr sicheres Verfahren

Quellen

<http://iks-jena.de/mitarb/lutz/security/cryptfaq/q4.html>

<http://philippbauer.de/info/info/asymmetrische-verschluesSELUNG/>

<http://tcp-ip-info.de/security/verschluesSELUNG.htm>

http://de.wikipedia.org/wiki/Verschl%C3%BCssELungsverfahren#Asymmetrische_Verschl.C3.BCSSLUNG

<http://de.wikipedia.org/wiki/Elgamal-Kryptosystem>

<http://de.wikipedia.org/wiki/Einwegfunktion>

<http://nordwest.net/hgm/krypto/mod-asym.htm>

<http://ddi.cs.uni-potsdam.de/Lehre/e-commerce/elBez2-5/page06.html>