Krypto-Begriffe

U23 Krypto-Mission

florob
Simon

Chaos Computer Club Cologne e.V.
http://koeln.ccc.de

4. Oktober 2015

Was ist Kryptographie?

Griechisch: κρυπτος (verborgen) + γραφειν (schreiben)

Mittel und Wege:

- Verschlüsseln einer Nachricht
- Verstecken einer Nachricht
- Empfänger garantieren
- Absender garantieren
- Inhalt garantieren

Kryptographie bedeutet geheimhalten, Kryptoanalyse bedeutet herauskriegen

Simon <schneid@cs.uni-bonn.de>

Begriffe

Nachricht ein Stück Information: Text, Zahlen, ein Bild, ...

Klartext lesbare Nachricht: x

Geheimtext, Kryptogramm verschlüsselte Nachricht: y

Ver-/Entschlüsseln Klartext in Geheimtext umwandeln (und umgekehrt)

Schlüssel Information, die Ver/-Entschlüsseln eindeutig macht: k

Kryptosystem Alles zusammen: Schlüsselerzeugung, Ver-/Entschlüsselung, Unterschriften, ...

Angriff, Knacken, Brechen Schlüssel finden, Nachricht ohne Schlüssel entschlüsseln, Nachricht ohne Schlüssel verändern, etc. pp.

Simon <schneid@cs.uni-bonn.de>

Verfahren

Symmetrische Kryptographie
: Entschlüsseln ist „Verschlüsseln rückwärts“

Schlüsselaustausch, Schlüsselverteilung
: Kommunikationspartner müssen ihre Schlüssel kennen

Asymmetrische Kryptographie
: Schlüsselfunktionen sind Einwegfunktionen, Schlüsselpaar $k = (e, d)$

Hybride Kryptographie Nachricht selbst symmetrisch verschlüsseln, den Schlüssel dazu asymmetrisch.

Simon <schneid@cs.uni-bonn.de>

Verfahren

Stromchiffre

Nachricht wird kontinuierlich verarbeitet

Blockchiffre

Nachricht muss ggf. in Stücke zerlegt werden

Landau-Notation („das große O“)

Vergleicht zwei Funktionen „auf lange Sicht“:

$$O(g) = \{h \mid \exists c \exists x_o \forall x > x_0 : h(x) \leq c \cdot g(x)\}$$

In $O(g)$ sind alle Funktionen, die grob betrachtet nicht größer werden als g. Schreibweise: $f = O(g)$ für $f \in O(g)$.

Beispiel

- Kasse im Supermarkt $= O(n)$ (linear)
- Kombinationsschloss durchprobieren $= O(c^n)$ (exponentiell)

Landau-Notation („das große O“)

Ω	ω	Θ	o	O
$\geq$	$>$	$=$	$<$	$\leq$

$$O(poly(n)) = \bigcup_{c \in \mathbb{N}} O(n^c)$$

Komplexitätsklasse $P \approx O(poly)$ heißt effizient

Einwegfunktion f: Berechnen ist effizient, Umkehren nicht.

Simon <schneid@cs.uni-bonn.de>

Reduktion

Vergleicht zwei Probleme, indem eins mit dem anderen gelöst wird.

$$A \leq_p B \Leftrightarrow \exists f : A \to B \in O(poly)$$

Aussprache: A kann polynomiell auf B reduziert werden.

A ist einfach Wenn B einfach ist, kann eine Lösung für A konstruiert werden.

B ist schwierig Wenn A schwierig ist, kann B nicht einfacher sein.

B ist nicht lösbar Wenn $A \leq_p B$, aber A nicht lösbar ist, kann B nicht lösbar sein.

Was ist „sicher“, was heißt „brechen“?

Angreifer benutzt ein Kryptosystem anders als geplant

Fähigkeit eines Angreifers, z.B:

- **CPA** : Darf Klartext bestimmen (Chosen Plaintext Attack)

Eigenschaft des Kryptosystems: z.B:

- **IND** Zwei Geheimtexte kann man nicht unterscheiden (INDistinguishability)
- **NM** Nachricht kann nicht unentdeckt verändert werden (Non-Malleability)

Sicherheitsbegriff kombiniert Fähigkeit und Eigenschaft, z.B. IND-CPA ist gerne gesehen :)

Siehe [[wiki:de:Sicherheitsbegriff]]

Kerckhoffs'sches Prinzip

Albert Einstein „Zwei Dinge sind unendlich: Das Universum und die menschliche Dummheit. Nur beim Universum bin ich mir nicht ganz sicher."

Bruce Schneider „Jeder kann ein Kryptosystem bauen, das er selbst nicht brechen kann."

Simon <schneid@cs.uni-bonn.de>

Kerckhoffs'sches Prinzip

Security by Obscurity Alles geheimhalten:
Funktionsvorschriften, Algorithmen, Schlüssel, etc. Was man nicht kennt, kann man nicht kaputtmachen.
Gegenbeispiele: Enigma, DVD-CSS, Xbox-Bootloader, WEP, Autoschlüssel, ...

Kerckhoffs' Prinzip Die Sicherheit eines Kryptosystems darf nur von der Geheimhaltung des Schlüssels abhängen.
Ermöglicht Peer Rewiew und *provable security*