Ideen und Konzepte der Informatik

Kryptographie

und elektronisches Banking

Antonios Antoniadis

(basiert auf Folien von Kurt Mehlhorn)

4. Dec. 2017

Übersicht

- Zwecke der Kryptographie
- Techniken
  - Seit mehr als 2000 Jahren: **Symmetrische Verschlüsselung**. Ceasar, One-Time Pad, Moderne Blockchiffres.
  - Seit 1978: **Asymmetrische Verschlüsselung, Public-Key Cryptographie**. RSA, ElGamal.
- Anwendungen
  - Electronic Banking
  - Digitale Unterschriften

Kryptographie, Zwecke

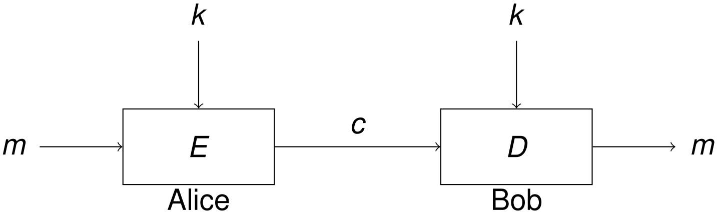
Kryptographie = **krypto** (geheim) + **graphie** (schreiben/Schrift)

Hauptziele, nach Wolfgang Ertel:

1. **Vertraulichkeit/Zugriffsschutz:** Nur berechtigte Personen können die Daten/Nachricht lesen.
2. **Integrität/Änderungsschutz:** Daten können nicht unbemerkt verändert werden.
3. **Authentizität/Fälschungsschutz:** Der Urheber der Daten oder der Absender der Nachricht soll eindeutig identifizierbar sein.
4. **Verbindlichkeit/Nichtabstreitbarkeit:** Urheberschaft sollte nachprüfbar und nicht abstreitbar sein.

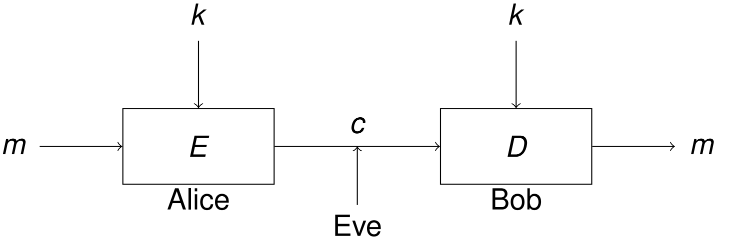
Symmetrische Verschlüsselung

Alice und Bob verabreden einen gemeinsamen Schlüssel k.



Symmetrische Verschlüsselung

Alice und Bob verabreden einen gemeinsamen Schlüssel k.



Eve = Eavesdropper (Lauscher)

Beispiel 1: Ceasar

- *D* und *E* das gleiche Gerät
- Schlüssel *k* ist Drehwinkel, bzw. um wieviele Buchstaben verschiebt sich „A“?
- *E* liest von innen nach außen
  D von außen nach innen.
- Einfach, aber sehr unsicher; nur 26 mögliche Schlüssel!

Notation

- m : Klartext, Nachricht, „message“
- c : Geheimtext, „cyphertext“
- E und D sind allgemein bekannte Geräte/Verfahren. Heute meistens Programme.
- Diese werden durch den Schlüssel k personalisiert.
- Ohne Kenntniss von k soll es praktisch unmöglich sein (kann je nach Anwendung Unterschiedliches bedeuten), m aus c zu bestimmen.
- Für alle m und k: $m = D(k, E(k, m))$.

Analogie

Man kann sich symmetrische Kryptographie wie folgt vorstellen:

- Alice und Bob kaufen sich eine Kiste und ein Vorhängeschloss mit zwei identischen Schlüsseln (k), jeweils einen.
- Nachricht (m) kommt in die Kiste, die Kiste wird mit dem Schlüssel verschlossen (Verfahren E). Kiste wird verschickt, und mit dem Schlüssel aufgemacht (Verfahren D).
- Ein Treffen oder ein vertrauenswürdiger Bote ist nötig.

Beispiel 2: One-Time Pad

(Anwendung: Rotes Telefon)

- Wie Ceasar, aber jeder Buchstabe des Textes hat einen eigenen Schlüssel, insbesondere:
- Schlüssel ist ein zufälliger Text (jeder Buchstabe ist gewürfelt) mit der gleichen Länge wie die Nachricht.
- Absolut sicher, aber der Schlüssel muss genauso lang wie die Nachricht sein.
- Schlüsselaustausch sehr aufwendig.

Beispiel 3: Moderne Blockchiffres

- Nachricht wird in Blöcke fester Länge (typisch 64,128, 256 Bits) zerlegt.
- Man hat einen Schlüssel der gleich lang wie jeder Block ist. Bei Länge 128 Bits gibt es also 2^{128} mögliche Schlüssel.
- Jeder Block wird mit diesem Schlüssel kodiert.
- Populäre Verfahren: DES (Data-Encryption-Standard), AES (Nachfolger)
- Sicherheit hängt von der Blocklänge ab. 128 Bit noch sicher.

Angriffe

- Caesar: Buchstabenhäufigkeit
- DES 56: Durch „Enumerierung“ mit Spezialhardware
- ENIGMA (Rätsel): Alan Turing

Zusammenfassung

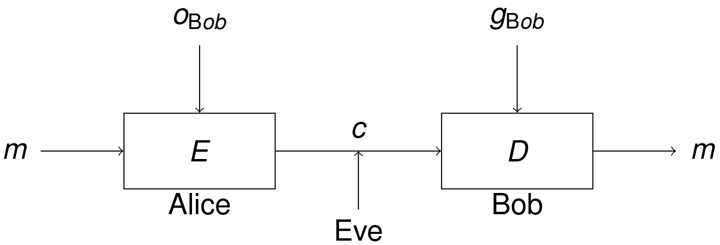
- Sender (Alice) und Empfänger (Bob) vereinbaren einen gemeinsamen Schlüssel k. Dieser muss geheim bleiben.
  - Früher: Treffen oder Bote.
  - Heute: asymmetrisches Verfahren zum Schlüsselaustausch.
- Caesar, One-Time Pad, AES128,...
- Sehr effiziente Ver- und Entschlüsselung.
- Bei vielen Teilnehmern steigt die Anzahl Schlüssel.

Asymmetrische Verschlüsselung

- (Empfänger) Bob erzeugt Schlüsselpaar $g_{\mathrm{B}ob}$ und $o_{\mathrm{B}ob}$. $g_{\mathrm{B}ob}$ bleibt geheim, $o_{\mathrm{B}ob}$ wird veröffentlicht.
- Jeder, der Bob eine Nachricht schicken will, benutzt $o_{\mathrm{B}ob}$ zum Verschlüsseln.
- Es ist sehr schwierig (nach heutiger Kenntnis) $g_{\mathrm{B}ob}$ aus $o_{\mathrm{B}ob}$ herzuleiten. Zum Entschlüsseln braucht man aber $g_{\mathrm{B}ob}$ welchen nur Bob hat.

Asymmetrische Verschlüsselung

$$m = D(g_{\mathrm{B}ob}, E(o_{\mathrm{B}ob}, m))$$



Analogie

Man kann sich Asymmetrische Verfahren wie folgt vorstellen:

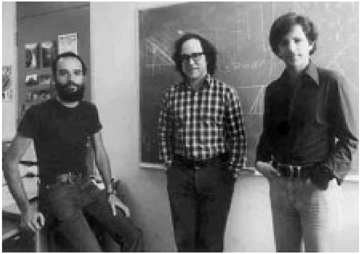
- Bob möchte in der Lage sein geheime Nachrichten zu bekommen.
- Er kauft viele identische Bügelschlösser und hinterlegt diese, offen, an öffentlichen Orten. Er behält den einzigen Schlüssel.
- Alice möchte Bob eine Nachricht m schicken: Sie tut die Nachricht in eine Kiste, verschließt die Kiste mit einem der Bügelschlösser und schickt die Kiste an Bob. Er ist der Einzige, der die Kiste öffnen kann.
- **Vorteil:** kein Treffen nötig.
- **Nachteile:**
  - Aufwändig
  - Woher weiß Alice, dass das Schloss wirklich zu Bob gehört?

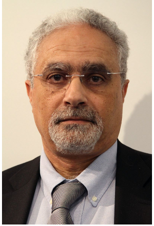
Notation

- E und D sind allgemein bekannte Geräte, heute meist Programme.
- Diese werden durch die Schlüssel personalisiert, also für Bob:
  - $E_{\mathrm{B}ob} = E$ mit Schlüssel $o_{\mathrm{B}ob}$ und
  - $D_{\mathrm{B}ob} = D$ mit Schlüssel $g_{\mathrm{B}ob}$.
- $E_{\mathrm{B}ob}$ ist öffentlich (also jeder kann damit eine Nachricht für Bob verschlüsseln).
- $D_{\mathrm{B}ob}$ ist nur von Bob ausführbar.

Erfinder

- RSA (Rivest-Shamir-Adleman, Turing Award), Rabin (Turing Award
- ElGamal und Elliptische Kurven





Sicherheit

- **RSA:**
  - Multiplizieren von 1000-stelligen Zahlen ist einfach, aber
  - sie aus dem Produkt zu berechnen, dauert mehr als 100 Jahre.
    Faktorisieren ist schwer!
- **ElGamal:** Ähnlich, aber mit diskreten Logarithmus bezüglich 2000-stellige Primzahl: Potenzieren einfach, Logarithmus schwer.
- 1000-stellige Primzahlen findet man leicht

Baby-Version, ElGamal

Darstellung aus Bongartz/Unger (Alg. der Woche)

- **Annahme:** Wir können multiplizieren und addieren/subtrahieren, aber dividieren ist sehr sehr schwer, daher:

Baby-Version, ElGamal

Darstellung aus Bongartz/Unger (Alg. der Woche)

- **Annahme:** Wir können multiplizieren und addieren/subtrahieren, aber dividieren ist sehr sehr schwer, daher:
- Aus p und f kann man $P = p \cdot f$ einfach berechnen, aber niemand kann aus f und $P (= p \cdot f)$ das p berechnen.

Baby-Version, ElGamal

- **Empfänger** wählt p und f; veröffentlicht f und $P = p \cdot f$, aber behält p geheim.
- **Sender** möchte m schicken, ($m < P$)
- Er wählt eine zufällige Zahl s und schickt öffentlich (s bleibt geheim)

$$s \cdot f \text{ und } N = m + s \cdot P.$$

- **Empfänger** berechnet

$$p \cdot (s \cdot f) = s \cdot P$$

und dann

$$m = N - s \cdot P.$$

Baby-Version, ElGamal

- **Empfänger** wählt p und f; veröffentlicht f und $P = p \cdot f$, aber behält p geheim.
- **Sender** möchte m schicken, ($m < P$)
- Er wählt eine zufällige Zahl s und schickt öffentlich (s bleibt geheim)

$$s \cdot f \text{ und } N = m + s \cdot P.$$

- **Eve** kennt $f, s \cdot f, P = p \cdot f$ und weiß nur, dass:

$$m \in \{N, N - P, N - 2P, N - 3P, \dots\}$$

- **Eve** muss $s \cdot P$ herausfinden, was aber ohne Kenntnis von p nicht möglich ist.

Details ElGamal

Zum Nachlesen.

- Im Wesentlichen ersetzt man Addieren durch Multiplizieren und Multiplizieren durch Potenzieren. Dann spielt der Logarithmus die Rolle der Division. Außerdem rechnet man Modulo einer Primzahl.

Modulo

- Grundmenge = $\{0, 1, \ldots n-1\}$, etwa $n = 7$.
- Addition, Subtraktion, Multiplikation $\mod n$, so dass das Ergebnis durch Restbildung wieder in die Grundmenge kommt. Z.B.

$$4 \cdot 6 = 24 \equiv 3 \mod 7$$
$$3 + 4 \cdot 2 = 11 \equiv 4 \mod 7.$$

- n prim (und $n > 1$), dann gibt es zu jedem $a \neq 0$ ein b sodass $a \cdot b \equiv 1 \mod n$ und es gibt ein g sodass

$$\{g, g^2, g^3, \ldots g^{n-1}\} = \{1, 2, \ldots n-1\}.$$

ElGamal

- **Empfänger** wählt Primzahl p, Erzeuger g und ein x, mit $g, x \in \{2, 3, \ldots, p-1\}$ und veröffentlicht (p, g, y) wobei $y = g^x \mod p$.
- Berechnung von y aus x ist leicht, aber von x aus y ist praktisch nicht möglich.
- **Sender** möchte m schicken, wählt s und schickt

$$(z = g^s \mod p, N = m \cdot y^s \mod p)$$

ElGamal

- **Empfänger** wählt Primzahl p, Erzeuger g und ein x, mit $g, x \in \{2, 3, \ldots, p-1\}$ und veröffentlicht (p, g, y) wobei $y = g^x \mod p$.
- Berechnung von y aus x ist leicht, aber von x aus y ist praktisch nicht möglich.
- **Sender** möchte m schicken, wählt s und schickt

$$(z = g^s \mod p, N = m \cdot y^s \mod p)$$

- **Eve** kennt y und weiß nur $m \in \{N, N/y, N/y^2, \ldots\}$

ElGamal

- **Empfänger** wählt Primzahl p, Erzeuger g und ein x, mit $g, x \in \{2, 3, \ldots, p-1\}$ und veröffentlicht (p, g, y) wobei $y = g^x \mod p$.
- Berechnung von y aus x ist leicht, aber von x aus y ist praktisch nicht möglich.
- **Sender** möchte m schicken, wählt s und schickt

$$(z = g^s \mod p, N = m \cdot y^s \mod p)$$

- **Empfänger** berechten $z^x = g^{sx} = y^s$ und dann $m = N/y^s \mod p$.

Zusammenfassung Asymmetrische Verschlüsselung

- Empfänger generiert einen geheimen und einen öffentlichen Schlüssel
- Es ist praktisch unmöglich vom öffentlichen Schlüssel zum privaten Schlüssel zu kommen.
- Sender verschlüsselt mit dem öffentlichen Schlüssel und Empfänger entschlüsselt mit dem geheimen Schlüssel

Elektronisches Banking

- Kunde kennt öffentlichen Schlüssel der Bank o_B
- Kunde erfindet geheimen Schlüssel k (Zufallszahl der Länge 256Bit) für symmetrisches Verfahren
- Kunde verschlüsselt k mit o_B und schickt den verschlüsselten Schlüssel an die Bank
- Bank entschlüsselt mit Hilfe ihres privaten Schlüssels g_B.
- Nun symmetrisches Verfahren mit k.

Elektronisches Banking

- Kunde kennt öffentlichen Schlüssel der Bank o_B
- Kunde erfindet geheimen Schlüssel k (Zufallszahl der Länge 256Bit) für symmetrisches Verfahren
- Kunde verschlüsselt k mit o_B und schickt den verschlüsselten Schlüssel an die Bank
- Bank entschlüsselt mit Hilfe ihres privaten Schlüssels g_B.
- Nun symmetrisches Verfahren mit k.
- **Problem:** Woher kenne ich den öffentlichen Schlüssel meiner Bank? Wir kommen zur Frage zurück...

Unterschriften

- **Eigenschaft:** Unterschreiber kann sie nicht abstreiten
- **Zweck:** Verbindlichkeit

Unterschriften

- **Eigenschaft:** Unterschreiber kann sie nicht abstreiten
- **Zweck:** Verbindlichkeit
- Was kann als Unterschrift dienen? Alles was nur der Unterschreiber kann:
  - Traditionell: handschriftliche Unterschrift, Fingerabdruck, Siegel, usw
  - Nun: Die Funktion D_X kann nur die Person X ausführen, weil nur sie ihren geheimen Schlüssel kennt.

Digitale Signaturen

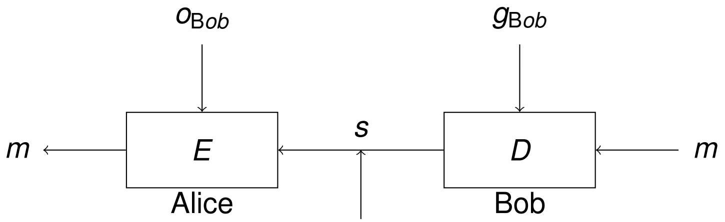
- Seien E_x und D_x die Funktionen von Person X und gelte auch $(E_x(D_x(z))) = z$ für alle z.

Digitale Signaturen

- Seien E_x und D_x die Funktionen von Person X und gelte auch $(E_x(D_x(z))) = z$ für alle z.
- Um m zu signieren, berechnet X den Text $s = D_x(m)$.
- Das Paar (m, s) ist das unterschriebene m.
- Vertragspartner überprüft, dass $E_x(s) = m$ gibt.
- Nur X kann s aus m erzeugen. Also kann X die Unterschrift nicht abstreiten.

Digitale Signaturen

$$m = D(g_{\mathrm{B}ob}, E(o_{\mathrm{B}ob}, m))$$



Wo, $s = D(g_{\mathrm{B}ob}, m) =$ Signatur von m

Elektronisches Banking, Forts.

- Die Bank hinterlegt ihren öffentlichen Schlüssel o_B bei einem Trustcenter
- Kunde kennt (fest eingebaut im Browser) den öffentlichen Schlüssel des TC und fragt nach Schlüssel der Bank
- TC signiert o_B und schickt an Kunden
- Kunde verifiziert die Unterschrift und benutzt dann o_B wie oben beschrieben.

Zusammenfassung

- Elektronisches Banking, Einkaufen im Netz, nutzt symmetrische und asymmetrische Kryptographie
- Kommunikation mit der Bank ist damit geschützt *https://...*
- **Vorsicht:** Verschlüsselte Übertragung garantiert nicht die Gesamtsicherheit, z.B. unsicheres Passwort.
- Vgl. erste Vorlesung: „Sicherheit und Privatheit“.

Passwörter Speichern

- h eine One-Way Funktion, z.B. Blockcypher
- Sei $c = h$(Passwort von AA)
- Speichere das Paar (AA, c)
- Die Authentizität wird bewiesen durch die Fähigkeit, c erzeugen zu können.

Passwörter Speichern

- h eine One-Way Funktion, z.B. Blockcypher
- Sei $c = h$(Passwort von AA)
- Speichere das Paar (AA, c)
- Die Authentizität wird bewiesen durch die Fähigkeit, c erzeugen zu können.
- Kann durch *brute-force* angegriffen werden, da Passwörter oft kurz
- Lösung: Maschine für h geht nach drei inkorrekten Auswertungen kaputt
- Automatische Verlängerung durch Zuffalstext, also speichern von (AA, zufäliges s, h(Passwort von AA, s)).

Buchempfehlung