Einführung in die Informationssicherheit

Florian Mendel

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology
Inffeldgasse 16a, A-8010 Graz, Austria

http://www.iaik.tugraz.at/

L1 – Sicherheit und Kryptographie

Einführung in die Informationssicherheit

Basierend auf den Folien von Mario Lamberger aus dem WS 12/13

Sicherheitssensitive Systeme – Geld abheben

- Kunden erhalten Bankomatkarten um Geld von ihrem Konto beheben zu können
- Das System besteht aus mehreren Entitäten:
  - Kunde
  - Bankomatkarte
  - Bankomat
  - Bank

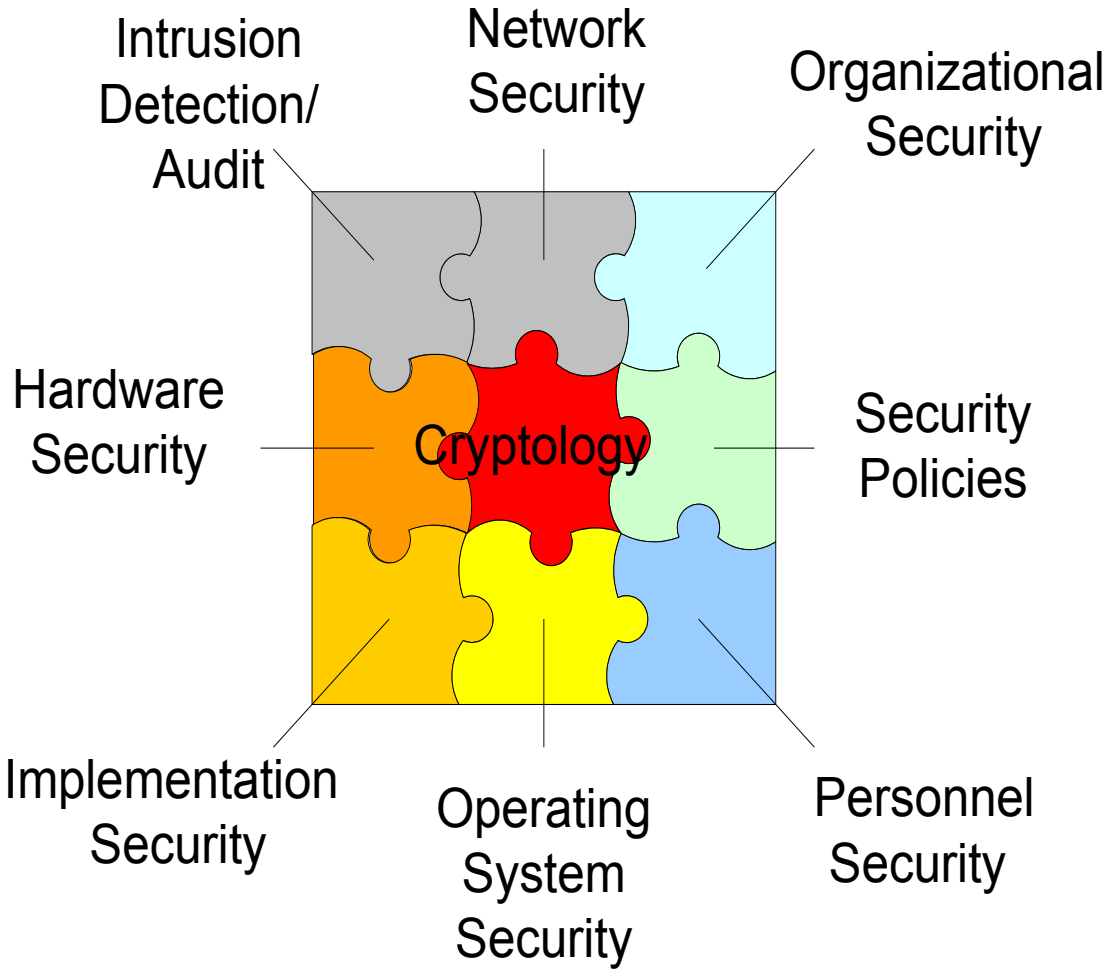
Sicherheitssensitive Systeme – Geld abheben

- Security Anforderungen:
  - Nur registrierte Kunden dürfen Geld beheben.
  - Man kann nur mit Originalkarten Geld beheben.
  - Nur vertrauenswürdige Geldmaschinen dürfen mit der Karte kommunizieren
  - Die Kommunikation zwischen Bankomat und Karte muss vertrauenswürdig sein.
  - Die Bank selbst muss vertrauenswürdig sein.
- Authentizität, Vertraulichkeit (Confidentiality), Netzwerksicherheit, Hardwaresicherheit, Sicherheit der Organisation, etc.

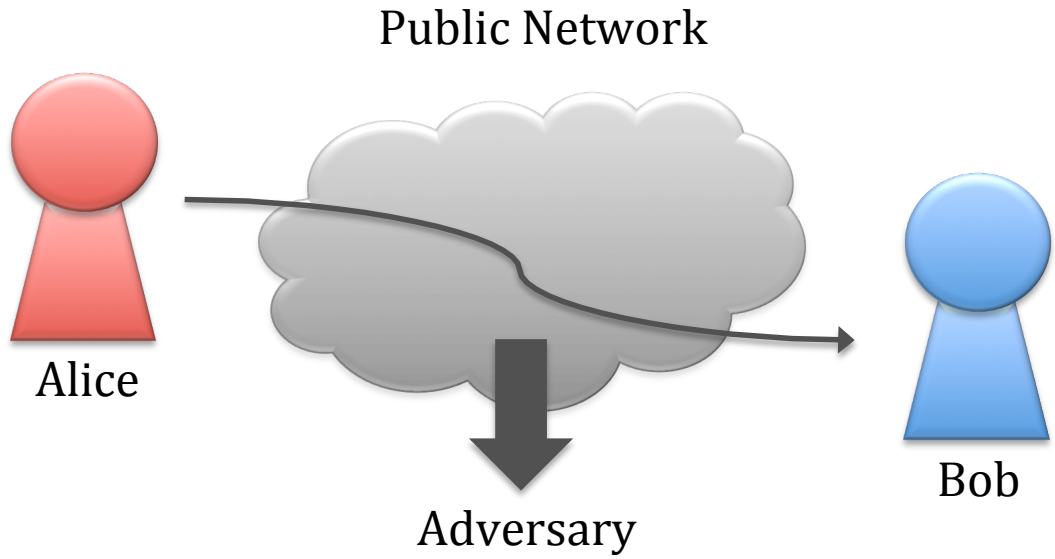
Sicherheitssensitive Systeme – Geld abheben

- Kunde: Beweist seine Identität durch Eingabe des PIN-Codes und Besitz der Karte.
- Bankomatkarte: Beweist ihre Identität, aber wie?
  - Durch sogenanntes Challenge-Response Protokoll.
- Bankomat: Beweist, dass er vertrauenswürdig ist?
  - Ebenfalls durch Challenge-Response Protokoll

Security


Intrusion Detection/ Audit
Network Security
Organizational Security
Hardware Security
Cryptology
Security Policies
Implementation Security
Operating System Security
Personnel Security

Das allgemeine Szenario



- Alice und Bob wollen sicher über ein (unsicheres) offenes Netzwerk kommunizieren

Basic Security Services (CIA)

- Confidentiality (Vertraulichkeit)
- Integrity (Integrität)
- Authenticity (Authentizität)
  - Daten
  - Entitäten
- Non-repudiation

Vertraulichkeit (Confidentiality)

- Wird durch Verschlüsselung erreicht und gewährleistet, dass nur dafür vorgesehene Parteien die Kommunikation lesen können.
- Standardisierte Algorithmen (am meisten verbreitet):
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)
- Symmetrische Chiffren (ciphers):
  - Verschlüsselung/Encryption: $C = E(P, K)$
  - Entschlüsselung/Decryption: $P = D(C, K)$

DES (DEA)

- Der erste starke Verschlüsselungsalgorithmus, der der “Öffentlichkeit” zugänglich gemacht wurde.
- DES ist eine sogenannte Block Chiffre:
  - Daten mit einer fixen und vorgegebenen Blocklänge werden mit einem geheimen Schlüssel verschlüsselt.
- Verschlüsselung ist eine mathematische Funktion die Daten (Plaintext) und den geheimen Schlüssel als Input nimmt um den verschlüsselten Text (Ciphertext) zu produzieren.

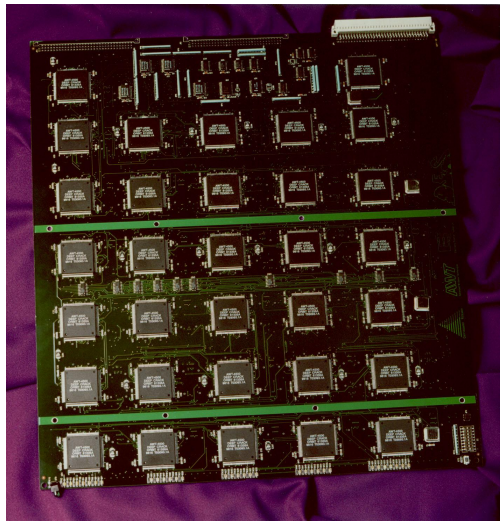
Attacken auf Block-Chiffren

- Brute-force key search:
  - Anwendbar auf alle Kryptosysteme.
  - Benötigt ein Ciphertext/Plaintext - Paar.
  - Durchsucht den kompletten Schlüsselraum, bis der richtige gefunden wird.

- DES benutzt Schlüssel mit 56 bits:
  - 1998 EFF Descracker benötigte 78 Std.
  - 1999 EFF Descracker + 100.000 PCs benötigte 22 Std.
  - `w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker`

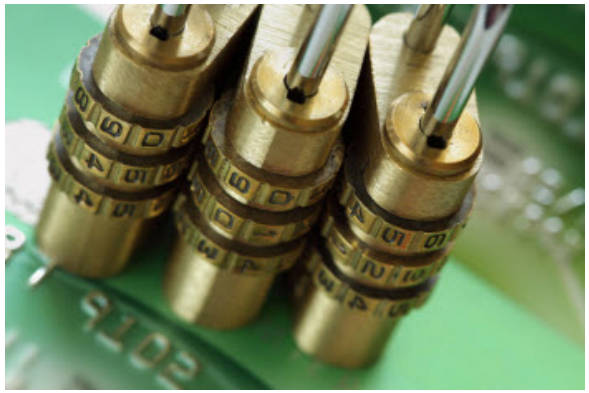
Challenges

- Sogenannte “Challenges” werden benutzt, um die Sicherheit von Chiffren in der Praxis zu testen.
- Die DES Challenge (von den RSA Labs), war so eine Initiative, um die Sicherheit von DES zu testen.



Sichere Blockchiffren

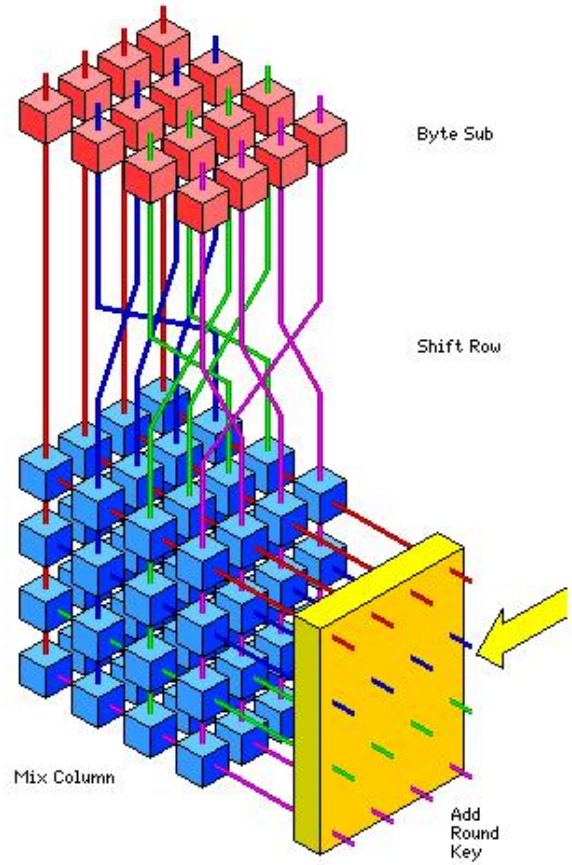
- 3-DES: Hat eine Schlüssellänge von 168 bits
  - $E(E(E(P, K_1), K_2), K_3)$
  - Löst das Problem der Brute-Force Attacke
  - Langsam (nicht an moderne Technolgie angepasst)
  - Theoretische Attacken existieren



http://cpnusa.com/2013/04/triple-des/

Sichere Blockchiffren

- Advanced Encryption Standard (AES)
  - Joan Daemen, Vincent Rijmen
  - NIST contest winner
  - 4 Operationen: SubBytes, ShiftRows, MixColumns, AddRoundKey
  - 10, 12, 14 Runden für Schlüssellänge von 128, 192, 256 bits



http://www.quadibloc.com/crypto/co0404.htm

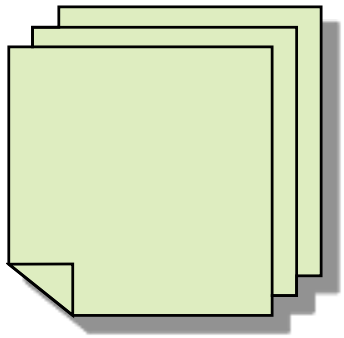
Attacken auf Blockchiffren

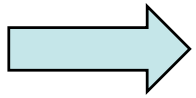
- Short-cut Attacken: Ausnutzen der spezifischen Struktur der zugrundeliegenden mathematischen Funktion
  - Differentielle Kryptoanalyse: untersucht Abhängigkeiten zwischen Input- und Output-Differenzen.
  - Lineare Kryptoanalyse: untersucht lineare Abhängigkeiten zwischen Input-bits und Output-bits.
- Keine signifikante Short-cut Attacke existiert für vollen AES.
  - 2009-2010: Related-key Attacken auf AES-192/256
  - 2011: Erste Attacke auf AES-128 (2^{126} statt 2^{128} Encr.)

Message Integrity – Hashfunktionen

- Hashfunktionen (kryptographische Prüfsummen) versichern, dass Daten nicht verändert wurden.
- Der Output einer Hashfunktion wird als Hashwert, Hash, oder "message digest" bezeichnet.
- Standardisierte Algorithmen (am weitesten verbreitet):
  - MD5 (vollständig gebrochen 2004)
  - SHA-1 (theoretische Attacke 2005)
  - SHA-2 (verdächtig, weil gleiche Struktur, beste Attacken $\rightarrow$ IAIK)
  - SHA-3: Keccak (announced October, 2, 2012)
    `http://keccak.noekeon.org`

Anwendungen von Hashfunktionen



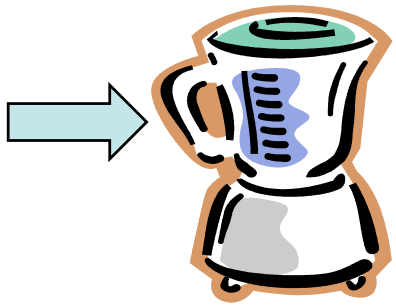


98246

Representative

Commitment

012345
6789…



?

Randomizer

Eigenschaften von Hashfunktionen

- Eine Hashfunktion nimmt Daten beliebiger Länge und berechnet einen Hashwert von fixer Länge.
- Gebräuchlich: Hashwert hat 160, 256, 512 bits
- Der Hashwert wird als Stellvertreter für die Nachricht benutzt:
  - verkürzte Repräsentation der Nachricht

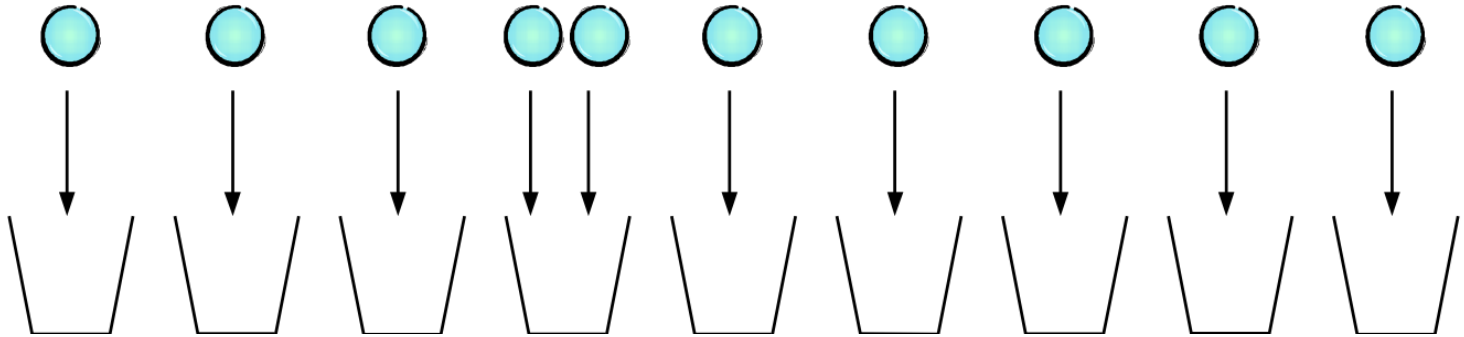
Hashfunktionen

- Verwendung: Berechne den Hashwert einer Nachricht: $HV = H(M)$ und versende (M, HV).
- Ein anderer Benutzer kann den Hashwert überprüfen:
  - Er erhält (M', HV)
  - Berechne: $HV' = H(M')$
  - Nachricht wurde nicht verändert wenn $HV' = HV$

Sicherheitsanforderungen an eine Hashfunktionen

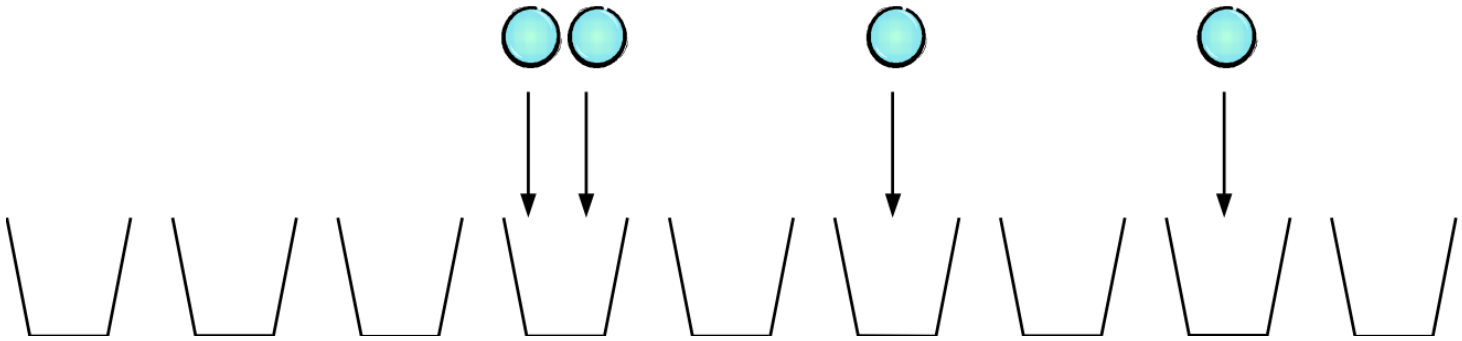
- Eine Hashfunktion ist eine Einwegfunktion:
  - Es ist praktisch unmöglich, zu einem Hashwert ein Urbild zu finden. (preimage resistance)
- Schwache Kollisionsresistenz:
  - Bei gegebenem X, ist es praktisch unmöglich ein zweites $X' \neq X$ zu finden, dass denselben Hashwert besitzt. (2nd preimage resistance)
- Starke Kollisionsresistenz:
  - Es is praktisch unmöglich, zwei Werte $X' \neq X$ zu finden, sodass $H(X) = H(X')$ gilt. (collision resistance)

Brute Force Attacken auf Hashfunktionen



- Wir haben k Bälle und n Urnen. ($k > n$)
- Wir werfen die Bälle in die Urnen:
  - Spätestens wenn wir den $(n+1)$-ten Ball werfen, befinden sich in mind. 1 Urne 2 Bälle
- Zusammenhang mit Hashfunktionen: Es muss immer 2 und mehr Nachrichten geben, die denselben Hashwert besitzen!

Attacken auf Hashfunktionen



- Geburtstagsattacke funktioniert für alle Hashfunktionen
  - Geburtstagsparadoxon impliziert, dass die Wahrscheinlichkeit für eine Kollision 50% ist, wenn $k \approx \sqrt{n}$
  - Daher sollte n mindestens 160 bits betragen
- Shortcut-Attacken benutzen wiederum die mathematische Struktur:
  - Differentielle Attacken
  - Noch keine Attacken bekannt für volle SHA-2 und SHA-3.

Hashfunktionen und IAIK

- IAIK arbeitet seit geraumer Zeit an der Analyse von Hashfunktionen
- Signifikante Beiträge zur Kryptoanalyse von SHA-1 etc.
- Eigenes Design im Finale des SHA-3 Wettbewerbs (Top 5)

`www.groestl.info`

Authentizität von Daten

- Hashfunktionen:
  - MDCs (Manipulation Detection Codes): Das sind die bereits eingeführten Hashfunktionen
  - MACs (Message Authentication Codes): Werden benutzt, um Authentizität von Daten zu gewährleisten
- MACs benutzen in der Berechnung einen geheimen Schlüssel:
  - $MC = MAC(M, K)$

Message Authentication Codes

- Vorgehensweise bei MACs:
  - $MC = MAC(M, K)$, (M, MC) werden zur Verfügung gestellt.
  - Verifikation: (M', MC)
    - Berechne: $MC' = MAC(M', K)$
    - Akzeptieren, wenn $MC' = MC$
- Standardisierte Algorithmen (am meisten verbreitet):
  - CBC-MAC (basiert auf Blockchiffre)
  - HMAC (basiert auf Hashfunktion)

Key Distribution Problem

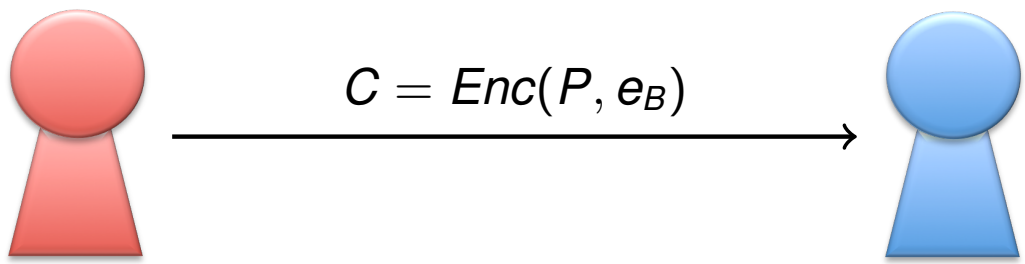
- Alle Verfahren, die wir besprochen haben, setzen voraus, dass beide Parteien einen gemeinsamen geheimen Schlüssel kennen
- Wie kann dieser geheime Schlüssel sicher von *A* nach *B* gebracht werden?
  - Persönliche Zustellung
  - Über sicheren Kanal (aber wozu brauchen wir dann noch Verschlüsselung/MACs?)
- Man muss etwas Neues erfinden!

Public Key Kryptographie

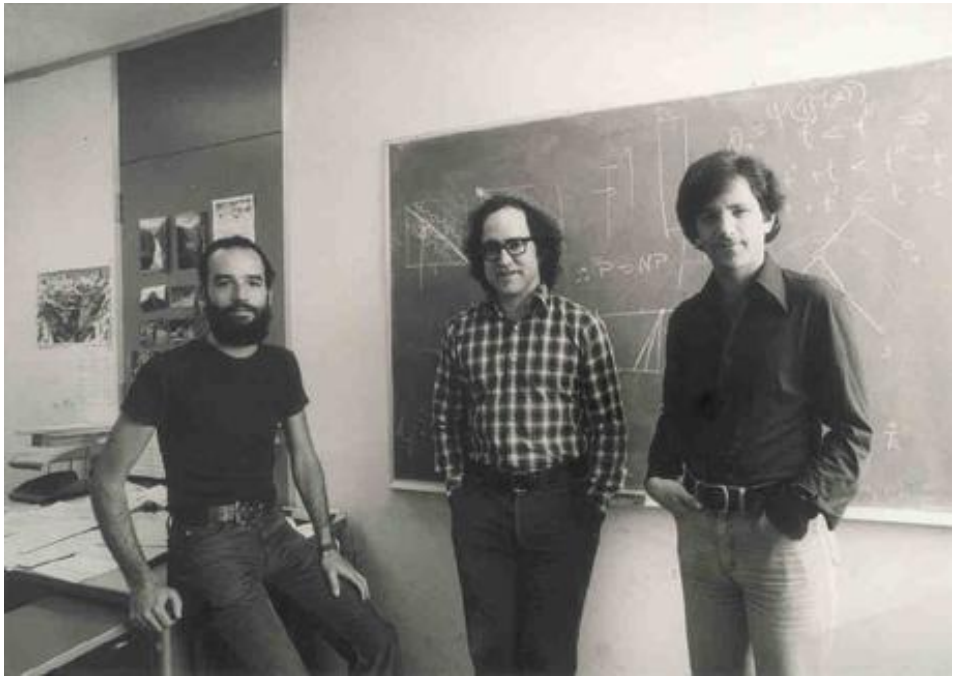
- Auch “Asymmetrische Verschlüsselung” genannt
- Zugrundeliegendes Konzept: “One-way trapdoor” Funktionen
  - Eine One-way Funktion (Einwegfunktion) ist schwer zu invertieren:
    - Bei gegebenem $f(x)$ ist es praktisch unmöglich, x zu finden
  - Eine One-way trapdoor Funktion ist schwer zu invertieren, es sei denn man besitzt zusätzliches Wissen (trapdoor):
    - Bei gegebenem $f(x)$ ist es praktisch unmöglich, x zu finden
    - Kennt man $f(x)$ und Trapdoor d, dann ist es leicht, x zu finden

Public Key Kryptographie

- Jede Partei besitzt nun ein Schlüsselpaar:
  - Öffentlicher Schlüssel e, kann jedem zugänglich gemacht werden
  - Privater Schlüssel d, dieser muss geheim gehalten werden
- Verschlüsselung (Alice will Bob eine Nachricht senden):
  - Alice benutzt Bob's öffentlichen Schlüssel e_B, berechnet $C = Enc(P, e_B)$ und sendet C an Bob
  - Bob entschlüsselt C mithilfe seines privaten Schlüssels und berechnet: $P = Dec(C, d_B)$



RSA



Paar et al.: Understanding Cryptography

- Ron Rivest
- Adi Shamir
- Leonard Adleman
- 1977

RSA

- One-way trapdoor-Funktion ist das IFP (= Integer Factorization Problem):
  - Gegeben $n = p \cdot q$ (p, q große Primzahlen), dann ist es praktisch unmöglich die Zahlen p und q zu finden.

$\Rightarrow$ Wähle großes n (2048 . . . 16384 bits)

RSA

- Schlüssel Generierung:
  - Wähle zwei große Primzahlen p und q und berechne $n = p \cdot q$.
  - Wähle einen öffentlichen Schlüssel e, $(0 < e < n)$
  - Berechne privaten Schlüssel via $d = e^{-1} \mod (p-1) \cdot (q-1)$
  - Key pair $((e, n), (d, p, q))$.
- Verschlüsselung: $C = M^e \mod n$
- Entschlüsselung: $M = C^d \mod n$

$\Rightarrow$ Siehe auch Sage Beispiel!

RSA Beispiel

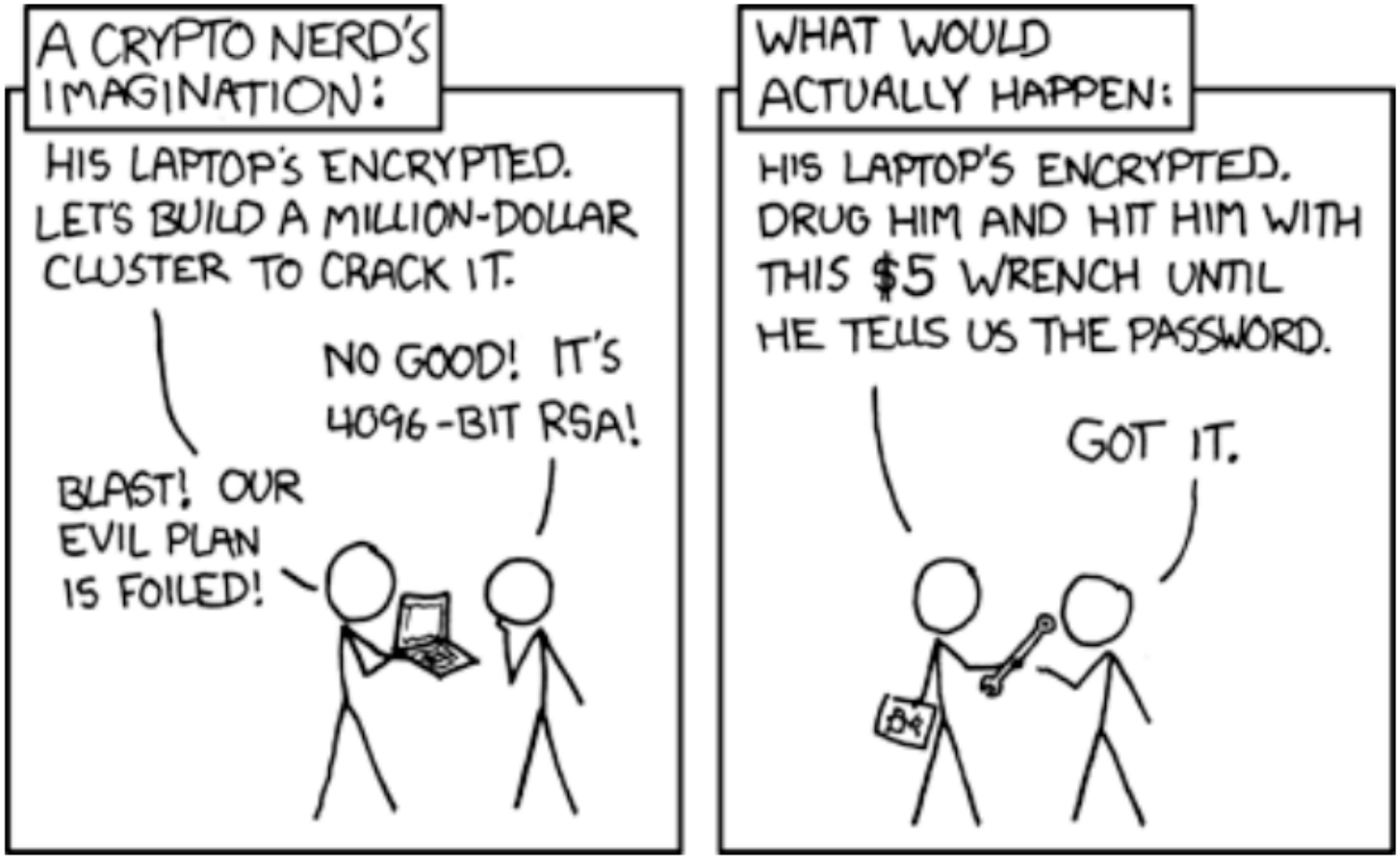
Modulare Arithmetik:

- $0, 5, 10, \cdots = 0 \mod 5$
- $1, 6, 11, \cdots = 1 \mod 5$
- $2, 7, 12, \cdots = 2 \mod 5$
- $3, 8, 13, \cdots = 3 \mod 5$
- $4, 9, 14, \cdots = 4 \mod 5$

Beispiel:

- $p = 11$, $q = 5$, $n = 55$,
  $(p-1) \cdot (q-1) = 40$
- Wähle $e = 3$, dann $d = 27$
  $(3 \cdot 27 = 81 = 1 \mod 40)$
- Wähle $M = 2$
  - $C = 2^{27} = 18 \mod 55$
  - $M = 18^3 = 2 \mod 55$

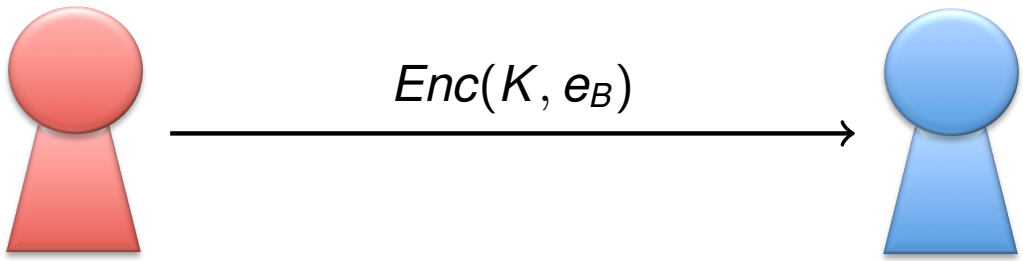
RSA Sicherheit



http://xkcd.com/538/

Key Transport

- Public Key Kryptographie kann benutzt werden, um geheime Schlüssel zu transportieren:
  - Angenommen, Alice will große Mengen von Daten an Bob schicken. PKC ist langsam, daher will sie AES Verschlüsselung benutzen.
  - Alice erzeugt einen AES Schlüssel K, verschlüsselt K mit Bob's öffentlichen Schlüssel e_B und schickt das Resultat an Bob.
  - Bob entschlüsselt den AES Schlüssel K mit seinem privaten Schlüssel.

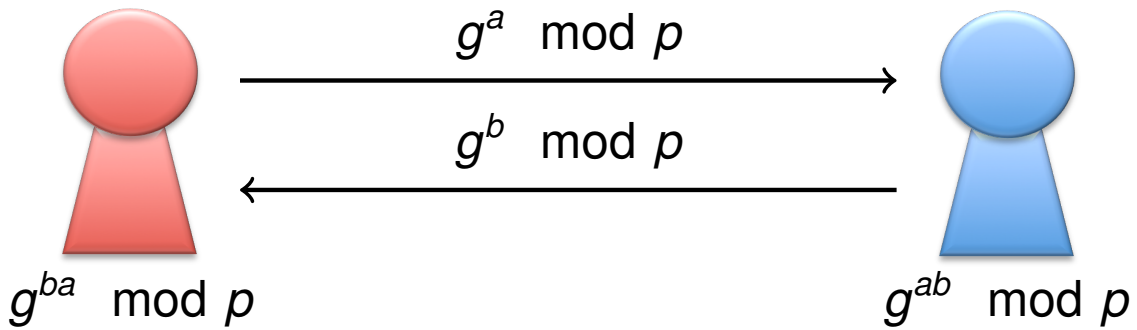


Key Agreement

- Vielleicht vertraut Bob Alice nicht 100%, dann möchte er auch bei der Generierung des AES Schlüssels K mitwirken.
- Key Agreement definiert auch den Beginn der Public Key Kryptographie:
  - Diffie und Hellman, 1976

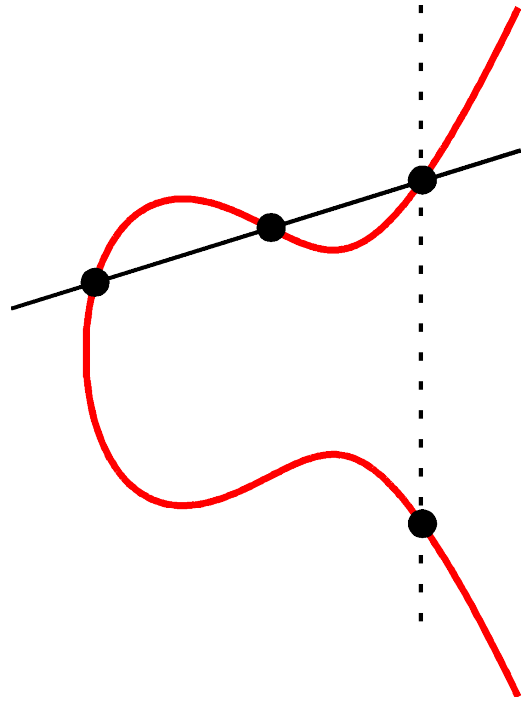
Diffie-Hellman Key-Agreement

- Basiert auf DLP (Diskretes Logarithmus Problem):
  - Gegeben g und g^a, dann ist es praktisch unmöglich, $a \mod p-1$ zu bestimmen
- Am Ende des Protokolls besitzen beide Parteien dieselbe Information.



Elliptische Kurven Kryptographie

- $y^2 = x^3 + ax + b \pmod{p}$
- Punkt-Arithmetik
- $Q = k \cdot P$
  - DL Problem (ECDLP)

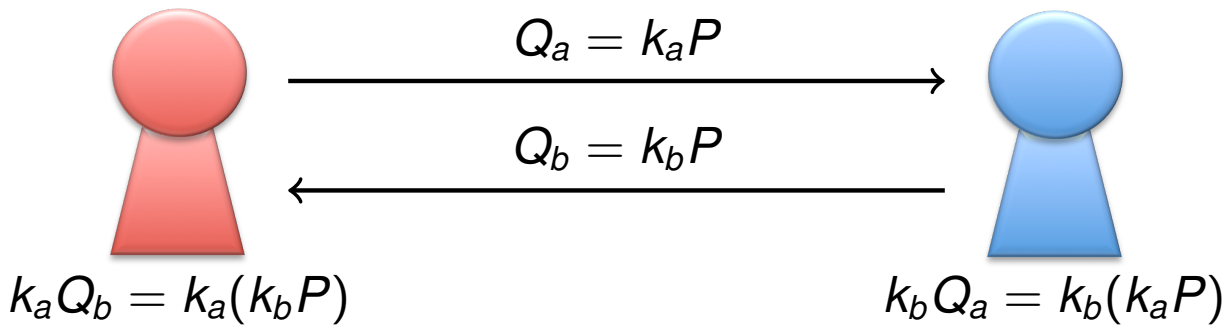


“Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques (RSA and Diffie-Hellman) now in use”

http://www.hpl.hp.com/research/info_theory/ellipbook.html

EC-Diffie-Hellman Key-Agreement

- Basiert auf Elliptic Curve Diskretes Logarithmus Problem (ECDLP):
  - Gegeben P und $Q = kP$, dann ist es praktisch unmöglich, k zu bestimmen
- Am Ende des Protokolls besitzen beide Parteien dieselbe Information.



Zusammenfassung

- Kryptographie bildet die Grundlage der modernen Informationssicherheit
- Symmetrische Kryptographie
  - Block Chiffre
  - Hash Funktionen
  - MACs
- Asymetrische Kryptographie
  - RSA, ECC
  - Key Transport

Vielen Dank für Ihre Aufmerksamkeit!