Diffie-Hellman, RSA, etc.

mathematische Grundlagen asymmetrischer Verschlüsselungsverfahren

pesco@hamburg.ccc.de

Chaos Computer Club Hamburg

SIGINT ’09, 22.–24. Mai 2009

Gliederung

Gliederung

Gliederung

Gliederung

Gliederung

Zielsetzung

- Kryptoverfahren als mysteriöse black boxes?
- Mathematik als reine Mathematikerdomäne?
- Inside the box for fun and profit!

Zielsetzung

- Kryptoverfahren als mysteriöse black boxes?
- Mathematik als reine Mathematikerdomäne?
- Inside the box for fun and profit!

Zielsetzung

- Kryptoverfahren als mysteriöse black boxes?
- Mathematik als reine Mathematikerdomäne?
- Inside the box for fun and profit!

Eine Bemerkung zum Ablauf

- Dies ist ein mathematischer Vortrag.
- Das Ziel ist Allgemeinverständlichkeit!
- Aber ich weiß wie sowas läuft...
- Bitte Handzeichen, wenn Ihr einen Moment braucht!
- Nachfragen erwünscht

Eine Bemerkung zum Ablauf

- Dies ist ein mathematischer Vortrag.
- Das Ziel ist Allgemeinverständlichkeit!
- Aber ich weiß wie sowas läuft...
- Bitte Handzeichen, wenn Ihr einen Moment braucht!
- Nachfragen erwünscht

Eine Bemerkung zum Ablauf

- Dies ist ein mathematischer Vortrag.
- Das Ziel ist Allgemeinverständlichkeit!
- Aber ich weiß wie sowas läuft...
- Bitte Handzeichen, wenn Ihr einen Moment braucht!
- Nachfragen erwünscht

Eine Bemerkung zum Ablauf

- Dies ist ein mathematischer Vortrag.
- Das Ziel ist Allgemeinverständlichkeit!
- Aber ich weiß wie sowas läuft...
- Bitte Handzeichen, wenn Ihr einen Moment braucht!
- Nachfragen erwünscht

Eine Bemerkung zum Ablauf

- Dies ist ein mathematischer Vortrag.
- Das Ziel ist Allgemeinverständlichkeit!
- Aber ich weiß wie sowas läuft...
- Bitte Handzeichen, wenn Ihr einen Moment braucht!
- Nachfragen erwünscht

Stoffpräsentation

- Fokus auf Struktur
- Zusammenhänge begründet
  - im Vortrag bewusst stark verkürzt
  - siehe Paper (→Pentabarf) für Details
- Verwendete Resultate ohne Beweis
  - siehe Standardliteratur

Stoffpräsentation

- Fokus auf Struktur
- Zusammenhänge begründet
  - im Vortrag bewusst stark verkürzt
  - siehe Paper (→Pentabarf) für Details
- Verwendete Resultate ohne Beweis
  - siehe Standardliteratur

Stoffpräsentation

- Fokus auf Struktur
- Zusammenhänge begründet
  - im Vortrag bewusst stark verkürzt
  - siehe Paper (→Pentabarf) für Details
- Verwendete Resultate ohne Beweis
  - siehe Standardliteratur

Elementares

- Notation
- Teilbarkeit
- Primzahlen
- Modulo-Rechnung

Gruppen

- Menge
- Verknüpfung ($\cdot$)
  - assoziativ
  - u.U. kommutativ
- Neutrales Element (1)
- Inverse (x^{-1})

Gruppen

- Menge
- Verknüpfung ($\cdot$)
  - assoziativ
  - u.U. kommutativ
- Neutrales Element (1)
- Inverse (x^{-1})

Gruppen

- Menge
- Verknüpfung $(\cdot)$
  - assoziativ
  - u.U. kommutativ
- Neutrales Element (1)
- Inverse (x^{-1})

Gruppen

- Menge
- Verknüpfung ($\cdot$)
  - assoziativ
  - u.U. kommutativ
- Neutrales Element (1)
- Inverse (x^{-1})

Gruppen

- Menge
- Verknüpfung $(\cdot)$
  - assoziativ
  - u.U. kommutativ
- Neutrales Element (1)
- Inverse (x^{-1})

Gruppen: Beispiel

- $\mathbb{Q}\backslash\{0\}$: Rationale Zahlen ohne 0
- Verknüpfung: Multiplikation
- Neutral: 1
- Inverse: $\frac{1}{x}$

Restklassen

- Intuition: Wie wrap-around bei 32-bit ints. ;)
- Setze gleich: alle ganzen Zahlen mit gleichem Rest *modulo n*
- Sprich: *x* “kongruent” *y* modulo *n*.
- $x \equiv y \pmod{n}$
- Notation: $\mathbb{Z}_n$ = Zahlen modulo *n*.

Restklassen

- Intuition: Wie wrap-around bei 32-bit ints. ;)
- Setze gleich: alle ganzen Zahlen mit gleichem Rest *modulo n*
- Sprich: x “kongruent” y modulo n.
- $x \equiv y \pmod{n}$
- Notation: $\mathbb{Z}_n =$ Zahlen modulo n.

Restklassen

- Intuition: Wie wrap-around bei 32-bit ints. ;)
- Setze gleich: alle ganzen Zahlen mit gleichem Rest *modulo n*
- Sprich: *x* “kongruent” *y* modulo *n*.
- $x \equiv y \pmod{n}$
- Notation: $\mathbb{Z}_n$ = Zahlen modulo *n*.

Restklassen

- Intuition: Wie wrap-around bei 32-bit ints. ;)
- Setze gleich: alle ganzen Zahlen mit gleichem Rest *modulo n*
- Sprich: *x* “kongruent” *y* modulo *n*.
- $x \equiv y \pmod{n}$
- Notation: $\mathbb{Z}_n$ = Zahlen modulo *n*.

Restklassen

- Intuition: Wie wrap-around bei 32-bit ints. ;)
- Setze gleich: alle ganzen Zahlen mit gleichem Rest *modulo n*
- Sprich: *x* “kongruent” *y* modulo *n*.
- $x \equiv y \pmod{n}$
- Notation: $\mathbb{Z}_n =$ Zahlen modulo *n*.

Restklassen: Beispiel

- $\mathbb{Z}_q$: ganze Zahlen modulo Primzahl
- Verknüpfung: Multiplikation modulo p
- Neutral: 1
- $\mathbb{Z}_q \backslash \{0\}$:
  - Zahlentheorie: Inverse existieren!
  - $\Rightarrow$ Gruppe!

Restklassen: Beispiel

- $\mathbb{Z}_q$: ganze Zahlen modulo Primzahl
- Verknüpfung: Multiplikation modulo p
- Neutral: 1
- $\mathbb{Z}_q \backslash \{0\}$:
  - Zahlentheorie: Inverse existieren!
  - $\Rightarrow$ Gruppe!

Restklassen: Beispiel

- $\mathbb{Z}_q$: ganze Zahlen modulo Primzahl
- Verknüpfung: Multiplikation modulo p
- Neutral: 1
- $\mathbb{Z}_q \backslash \{0\}$:
  - Zahlentheorie: Inverse existieren!
  - $\Rightarrow$ Gruppe!

RSA: Modulare Exponentiation

$$m^e \pmod{n}$$

- Gruppe: $\mathbb{Z}_n$
- $m =$ Nachricht
- $e =$ “Verschlüsselungsexponent”

RSA: Modulare Exponentiation

$$m^e \pmod{n}$$

- Gruppe: $\mathbb{Z}_n$
- $m =$ Nachricht
- $e =$ “Verschlüsselungsexponent”

RSA: Modulare Exponentiation

$$m^e \pmod{n}$$

- Gruppe: $\mathbb{Z}_n$
- $m =$ Nachricht
- $e =$ “Verschlüsselungsexponent”

Trapdoor: Eulerscher Satz

$$m^{\varphi(n)} \equiv 1 \pmod{n}$$

- $\varphi(pq) = (p-1)(q-1)$
- Leicht, wenn Faktorisierung von $n = pq$ bekannt!

Trapdoor: Eulerscher Satz

$$m^{\varphi(n)} \equiv 1 \pmod{n}$$

- $\varphi(pq) = (p-1)(q-1)$
- Leicht, wenn Faktorisierung von $n = pq$ bekannt!

Trapdoor: Eulerscher Satz

$$m^{\varphi(n)} \equiv 1 \pmod{n}$$

- $\varphi(pq) = (p-1)(q-1)$
- Leicht, wenn Faktorisierung von $n = pq$ bekannt!

Entschlüsselung

- Invertiere e modulo $\varphi(n)$
- $\Rightarrow \quad ed \equiv 1 \pmod{n}$
- d.h. $ed = 1 + k\varphi(n)$

$$m^{ed} = m^{1+k\varphi(n)} = m \cdot m^{k\varphi(n)} = m$$

Entschlüsselung

- Invertiere e modulo $\varphi(n)$
- $\Rightarrow \quad ed \equiv 1 \pmod{n}$
- d.h. $ed = 1 + k\varphi(n)$

$$m^{ed} = m^{1+k\varphi(n)} = m \cdot m^{k\varphi(n)} = m$$

Entschlüsselung

- Invertiere e modulo $\varphi(n)$
- $\Rightarrow \quad ed \equiv 1 \pmod{n}$
- d.h. $ed = 1 + k\varphi(n)$

$$m^{ed} = m^{1+k\varphi(n)} = m \cdot m^{k\varphi(n)} = m$$

Entschlüsselung

- Invertiere e modulo $\varphi(n)$
- $\Rightarrow \quad ed \equiv 1 \pmod{n}$
- d.h. $ed = 1 + k\varphi(n)$

$$m^{ed} = m^{1+k\varphi(n)} = m \cdot m^{k\varphi(n)} = m$$

Eine Anekdote zu RSA

Festplattenkrypto mit GnuPG. . .

$$\text{pub} = (e, n) \quad \text{priv} = (d, n)$$

Eine Anekdote zu RSA

Festplattenkrypto mit GnuPG...

$$\text{pub} = (e, n) \quad \text{priv} = (d, n)$$

Diffie-Hallman

- A priori kein Verschlüsselungsverfahren!
- Aber leicht zu bilden: “ElGamal”
- Grundlage für *diverse* andere Verfahren

Diffie-Hallman

- A priori kein Verschlüsselungsverfahren!
- Aber leicht zu bilden: “ElGamal”
- Grundlage für *diverse* andere Verfahren

Diffie-Hallman

- A priori kein Verschlüsselungsverfahren!
- Aber leicht zu bilden: “ElGamal”
- Grundlage für *diverse* andere Verfahren

Exponentiation in einer endlichen Gruppe

$$g^x \quad , g \in G_q$$

- g *Erzeuger* von G_q
- $x \in \mathbb{N}$

Diffie-Hellman Schlüsselaustausch

1. Alice: $0 \leq a < q$
   Bob: $0 \leq b < q$
2. $g^a \longrightarrow$ Bob
   $g^b \longrightarrow$ Alice
3. Alice: $(g^b)^a = g^{ab}$
   Bob: $(g^a)^b = g^{ab}$

Diffie-Hellman Schlüsselaustausch

1. Alice: $0 \leq a < q$
   Bob: $0 \leq b < q$
2. $g^a \longrightarrow$ Bob
   $g^b \longrightarrow$ Alice
3. Alice: $(g^b)^a = g^{ab}$
   Bob: $(g^a)^b = g^{ab}$

Diffie-Hellman Schlüsselaustausch

1. Alice: $0 \leq a < q$
   Bob: $0 \leq b < q$
2. $g^a \longrightarrow$ Bob
   $g^b \longrightarrow$ Alice
3. Alice: $(g^b)^a = g^{ab}$
   Bob: $(g^a)^b = g^{ab}$

Sicherheit von Diffie-Hellman

- $g^a, g^b \mapsto g^a b$
  - “Diffie-Hellman-Problem” (DH)
- effizientestes bekanntes Verfahren: $g^a \mapsto a$
  - “Diskreter Logarithmus” (DL)

Sicherheit von Diffie-Hellman

- $g^a, g^b \mapsto g^a b$
  - “Diffie-Hellman-Problem” (DH)
- effizientestes bekanntes Verfahren: $g^a \mapsto a$
  - “Diskreter Logarithmus” (DL)

Möglichkeiten für G_q

- Schwierigkeit von DH/DL hängt von G_q ab
- Üblich: Untergruppe von Z_p
- 90's Buzzword: Punkte auf elliptischen Kurven

Möglichkeiten für G_q

- Schwierigkeit von DH/DL hängt von G_q ab
- Üblich: Untergruppe von Z_p
- 90's Buzzword: Punkte auf elliptischen Kurven

Möglichkeiten für G_q

- Schwierigkeit von DH/DL hängt von G_q ab
- Üblich: Untergruppe von Z_p
- 90's Buzzword: Punkte auf elliptischen Kurven

Eine Anekdote zu Diffie-Hellman

Spielen mit MACs und Montgomery-Multiplikation. . .

Cheat Sheet ;)

$$m^{ed} = m^{1+k\varphi(n)} = m \quad \text{(RSA)}$$

$$g^{ab} = (g^a)^b = (g^b)^a = g^{ab} \quad \text{(D-H)}$$

Details, Literatur $\rightarrow$ Paper in Pentabarf

Danke fürs Zuhören!