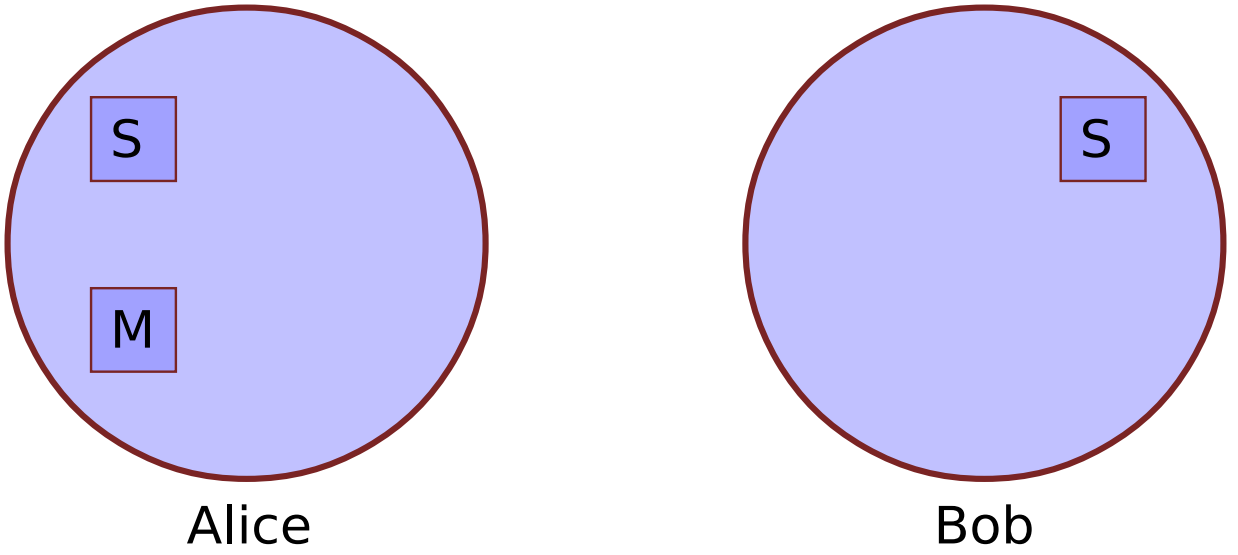
Kryptographie

Schlüsselaustausch
Diffie-Hellmann-Merkle

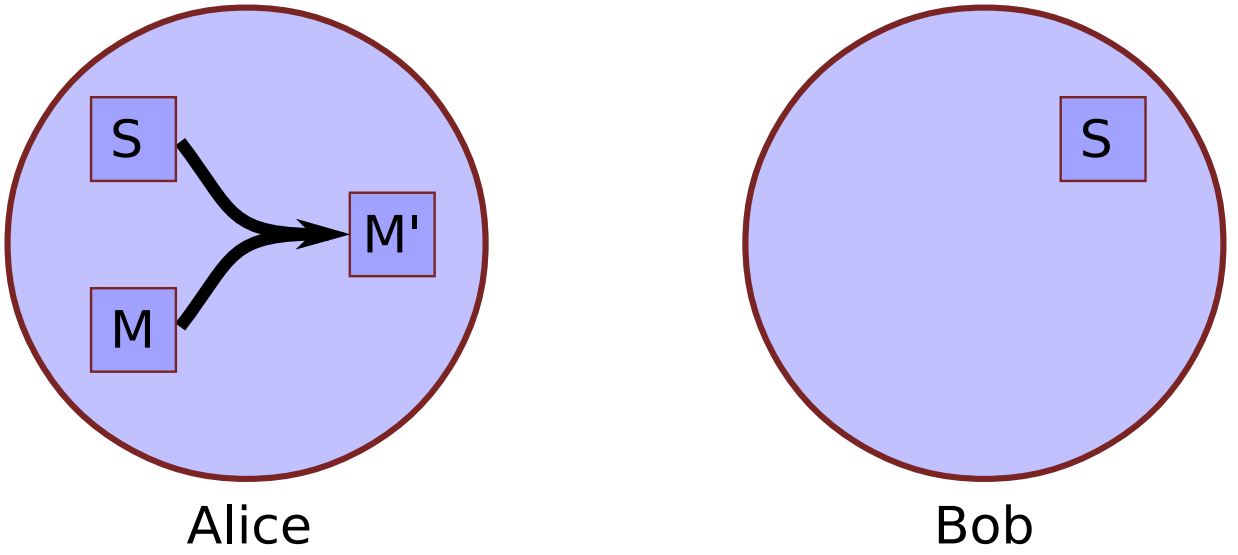
Symmetrische Verschlüsselung

- Alice schreibt Nachricht M an Bob
  - Geheimer Schlüssel S ist beiden bekannt



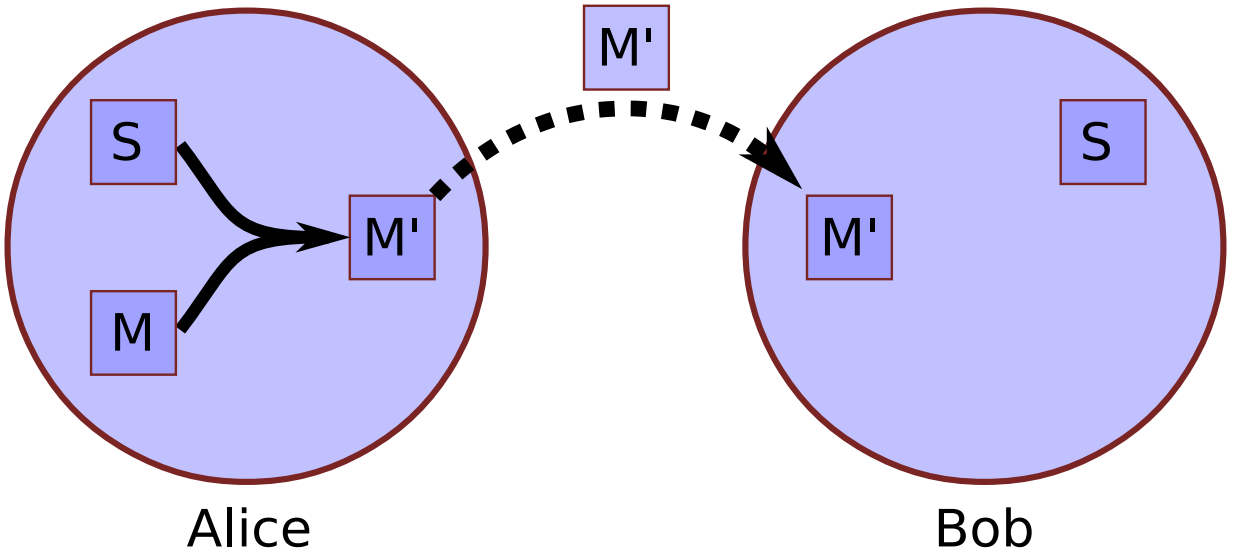
Symmetrische Verschlüsselung

- Alice schreibt Nachricht M an Bob
  - M wird mit Schlüssel S zu M‘ verschlüsselt
  - S idealerweise so lang wie M
  - Keinen Schlüssel zweimal benutzen



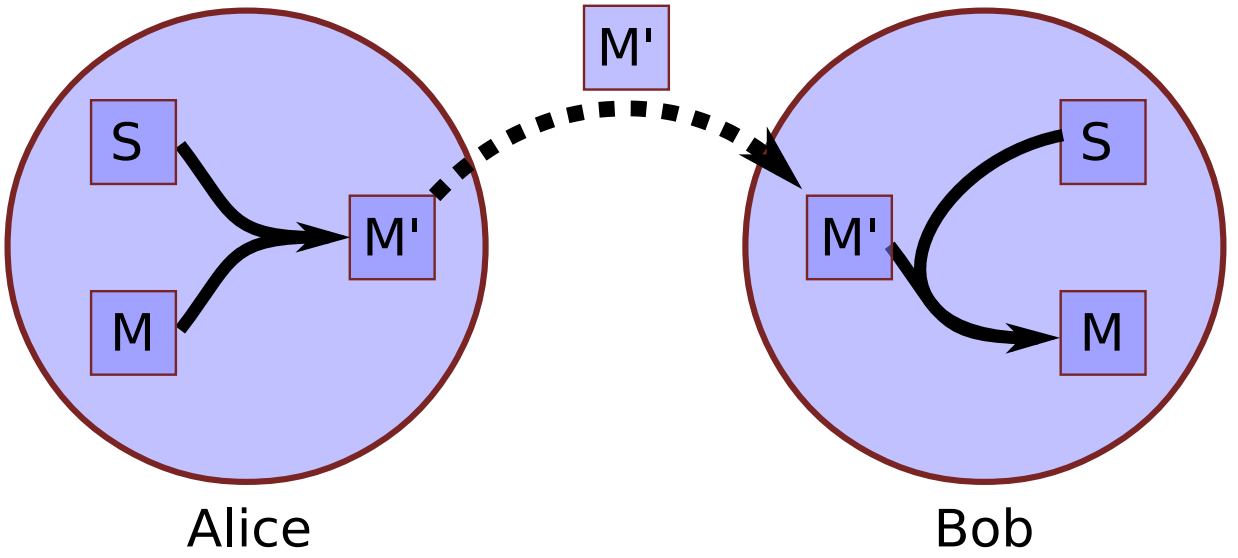
Symmetrische Verschlüsselung

- Verschlüsselte Nachricht M‘
  - Über unsichere Verbindung übertragen
  - Angreifer kennt Schlüssel S nicht



Symmetrische Verschlüsselung

- Bob empfängt verschlüsselte Nachricht M‘
  - M‘ mit Schlüssel S zu M entschlüsselt
  - Bob liest entschlüsselte Nachricht M



Symmetrische Verschlüsselung

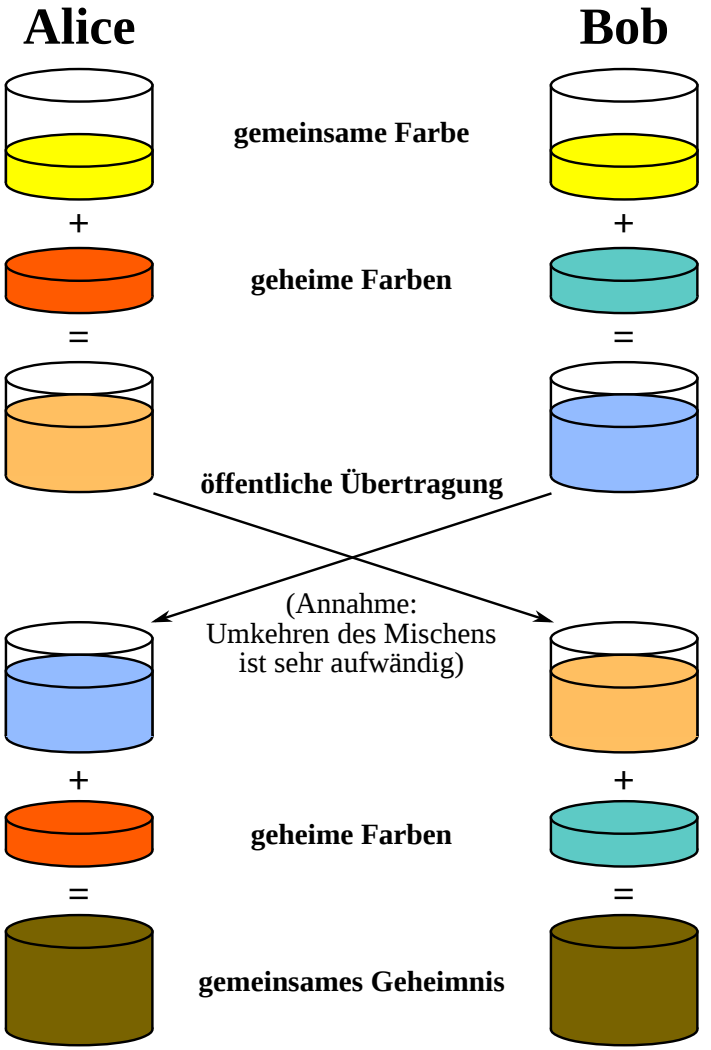
- Wie wird Schlüssel S transportiert?
  - Pseudo Random Generator
  - Geheimkurier
  - Quantenkommunikation

- Probleme Schlüsseltransport
  - Teuer
  - Sicherheitskritisch

Geheime Farbmischung

- Anahmen
  - Farbmischung einfach
  - Entmischung aufwändig
- Einigung gemeinsame Farbe
- Wahl geheime Farben
- Übertragung Mischfarben
- Mischfarbe erneut mischen

  → Gemeinsame Geheimfarbe

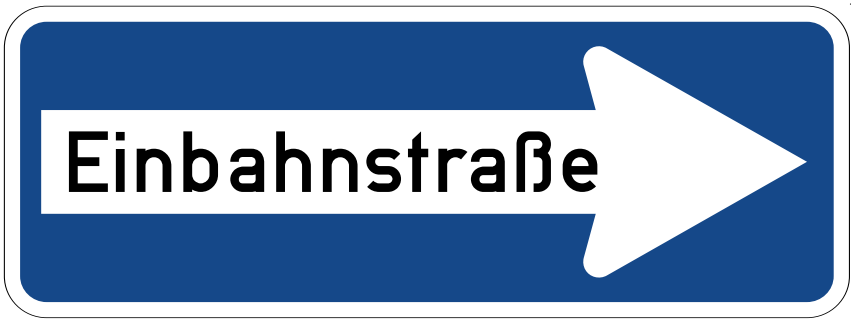


Idee Schlüsselaustausch

- Einwegfunktion
  - e(x) = y einfach (Polynomiell)
  - $e^{-1}(y) = x$ aufwendig (Exponentiell)
- Drei Zufallszahlen
  - Geheime Zufallszahl Alice
  - Geheime Zufallszahl Bob
  - Gemeinsam gewählte öffentliche Zufallszahl
- Gemeinsame geheime Zahl
  - Ähnlich geheimer Farbmischung erzeugt

Mathematische Einwegfunktion

- Diskrete Exponentialfunktion
  - $E(x) = b^x \bmod m$
  - Rest bei Division von E^x durch m
  - Für x tausend Bit lang in Sekunden berechenbar
  - $E^{-1}(x)$ für gängige Längen praktisch nicht berechenbar
  - Sichere Schlüssellänge gemäß Stand der Technik



Modulo Notation

$$k \equiv m \mod p \Leftrightarrow \frac{k}{p} \text{ und } \frac{m}{p} \text{ haben gleichen Rest}$$

Modulo Notation

$$k \equiv m \mod p \Leftrightarrow \frac{k}{p} \text{ und } \frac{m}{p} \text{ haben gleichen Rest}$$

- Beispiele
  - $256 \equiv 3 \mod 11 \quad (256:11 = 23 \text{ Rest } 3 \text{ und } 3:11 = 0 \text{ Rest } 3)$

Modulo Notation

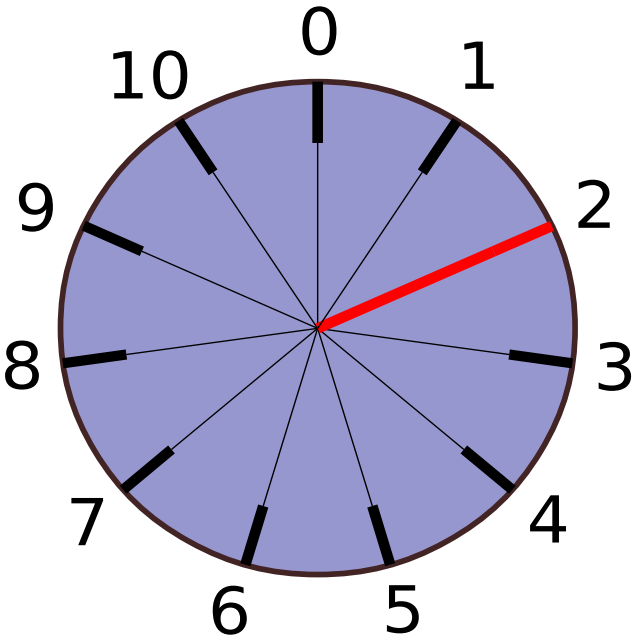
$$k \equiv m \mod p \Leftrightarrow \frac{k}{p} \text{ und } \frac{m}{p} \text{ haben gleichen Rest}$$

- Beispiele
  - $256 \equiv 3 \mod 11 \quad (256:11=23 \text{ Rest } 3 \text{ und } 3:11=0 \text{ Rest } 3)$
  - $32 \equiv 21 \mod 11 \quad (32:11=2 \text{ Rest } 10 \text{ und } 21:11=1 \text{ Rest } 10)$

Restklassengruppen

- Restklassengruppe $\mathbb{Z}_p$ (p Primzahl) ist Menge
  - $\mathbb{Z}_p = \{ 0, 1, 2, \ldots, p - 1 \}$
  - Mit der Operation
    $o : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$; $k \circ m := k\ m \bmod p$.

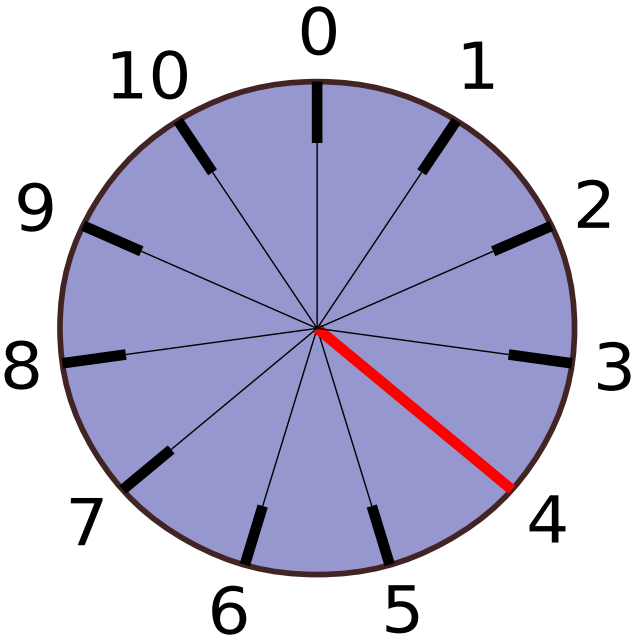
- Beispiel $\mathbb{Z}_p$ mit p = 11:
  - $2^1 = 1 \circ 2 \equiv 2 \bmod 11$



Restklassengruppen

- Restklassengruppe $\mathbb{Z}_p$ (p Primzahl) ist Menge
  - $\mathbb{Z}_p = \{ 0, 1, 2, \ldots, p - 1 \}$
  - Mit der Operation
    $o : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$; $k \circ m := k\ m \bmod p$.

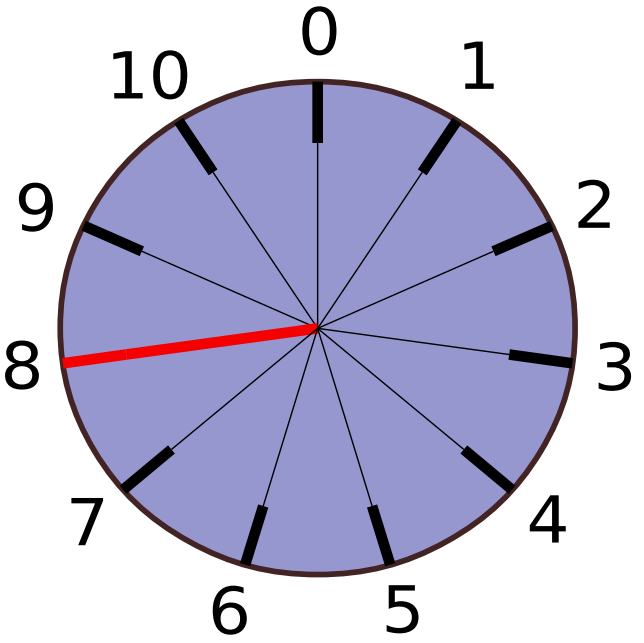
- Beispiel $\mathbb{Z}_p$ mit p = 11:
  - $2 \circ 2 \equiv 4 \bmod 11$



Restklassengruppen

- Restklassengruppe $\mathbb{Z}_p$ (p Primzahl) ist Menge
  - $\mathbb{Z}_p = \{ 0, 1, 2, \ldots, p - 1 \}$
  - Mit der Operation
    $o : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$; $k \circ m := k\ m \bmod p$.

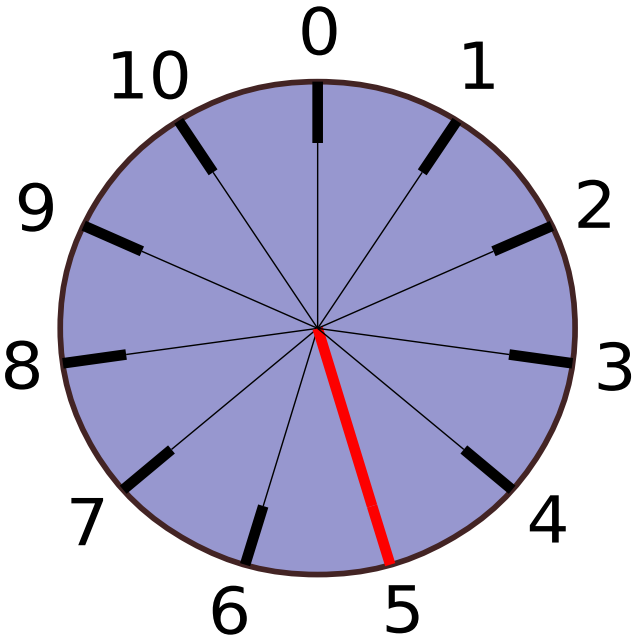
- Beispiel $\mathbb{Z}_p$ mit p = 11:
  - $4 \circ 2 \equiv 8 \bmod 11$



Restklassengruppen

- Restklassengruppe $\mathbb{Z}_p$ (p Primzahl) ist Menge
  - $\mathbb{Z}_p = \{ 0, 1, 2, \ldots, p - 1 \}$
  - Mit der Operation
    $o : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$; $k \circ m := k\ m \bmod p$.

- Beispiel $\mathbb{Z}_p$ mit p = 11:
  - $8 \circ 2 \equiv 16 \equiv 5 \bmod 11$



Erzeuger

- $g \in \mathbb{Z}_p$ heißt Erzeuger von $\mathbb{Z}_p \setminus \{ 0 \}$
  $:\Leftrightarrow \{ g \bmod p, g^2 \bmod p, \ldots, g^{p-1} \bmod p \} = \mathbb{Z}_p \setminus \{0\}$
- Beispiel: g = 2 ist ein Erzeuger von $\mathbb{Z}_{11} \setminus \{0\}$

i	1	2	3	4	5	6	7	8	9	10
2^i	2	4	8	16	32	64	128	256	512	1024
$2^i \bmod 11$	2	4	8	5	10	9	7	3	6	1

Diskreter Logarithmus

- $g^a \bmod p = A \Leftrightarrow \log_g(A) \bmod p = a$

- Beispiel:
  - $2^4 \bmod 11 = 5 \Leftrightarrow \log_2(5) \bmod 11 = ?$

Diskreter Logarithmus

- $g^a \bmod p = A \Leftrightarrow \log_g(A) \bmod p = a$

- Beispiel:
  - $2^4 \bmod 11 = 5 \Leftrightarrow \log_2(5) \bmod 11 = 4$

Diskreter Logarithmus

- $g^a \bmod p = A \Leftrightarrow \log_g(A) \bmod p = a$

- Beispiel:
  - $2^4 \bmod 11 = 5 \Leftrightarrow \log_2(5) \bmod 11 = 4$
  - Berechnung für große Zahlen sehr zeitaufwendig
  - Zahlen tausende Bits lang
    → Rechenzeit länger als Alter des Universums
  - Sichere Schlüssellänge steigt mit Stand der Technik

    Bundesamt Sicherheit in der Informationstechnik:

    RSA bis 2022: Schlüssellänge > 2000 Bit

DHM-Schlüsseltausch

- Alice und Bob bestimmen
  - Primzahl p
  - Erzeuger g
  - → Restklassengruppe $\mathbb{Z}_p \setminus \{0\}$

DHM-Schlüsseltausch

- Alice und Bob bestimmen p,g
- Alice und Bob erzeugen jeweils
  - Geheime zufällige Zahl a bzw. b
  - $a,b \in \mathbb{Z}_p \setminus \{0\} = \{ 1, \ldots, p-1\}$

DHM-Schlüsseltausch

- Alice und Bob bestimmen p,g
- Alice und Bob erzeugen jeweils a bzw. b
- Alice und Bob berechnen jeweils
  - $A = g^a \bmod p$

    bzw.
  - $B = g^b \bmod p$

DHM-Schlüsseltausch

- Alice und Bob bestimmen p,g
- Alice und Bob erzeugen jeweils a bzw. b
- Alice und Bob berechnen jeweils A bzw. B
- A und B über unsicheres Medium übertragen
- Beide berechnen nun
  - $K_{Alice} = B^a \bmod p$

    bzw.
  - $K_{Bob} = A^b \bmod p$

DHM-Schlüsseltausch

- Alice und Bob bestimmen p,g
- Alice und Bob erzeugen jeweils a bzw. b
- Alice und Bob berechnen jeweils A bzw. B
- A und B über unsicheres Medium übertragen
- Beide berechnen nun K_{Alice} und K_{Bob}
- Ergebnis $K_{Alice} = K_{Bob}$
  - Für beide Partner identisch
  - Schlüssel für weitere Kommunikation

DHM-Schlüsseltausch

- Alice und Bob bestimmen p,g
- Alice und Bob erzeugen jeweils a bzw. b
- Alice und Bob berechnen jeweils A bzw. B
- A und B über unsicheres Medium übertragen
- Beide berechnen nun K_{Alice} und K_{Bob}
- Ergebnis $K_{Alice} = K_{bob}$= Gemeinsamer Schlüssel
  - Austausch temporärer Sitzungsschlüssel

    → weiter mit symmetrischer Verschlüsselung

Probleme DHM-Verfahren

- „Man in the middle attack“

  → Keine Verifizierung von Alice und Bob

Probleme DHM-Verfahren

- „Man in the middle attack“
- „Angriff auf diskreten Logarithmus“
  - Verfahren basiert auf schwierig zu berechnendem diskreten Logarithmus.
  - Verfahren 1976 vorgestellt
  - Ersetzung von Multiplikation und Eponentation

    → Punktaddition & Skalarmultiplikation auf elliptischen Kurven
  - Vielfacher Einsatz im Internet (TLS, SSL, ...)

Geschichtliche Entwicklung

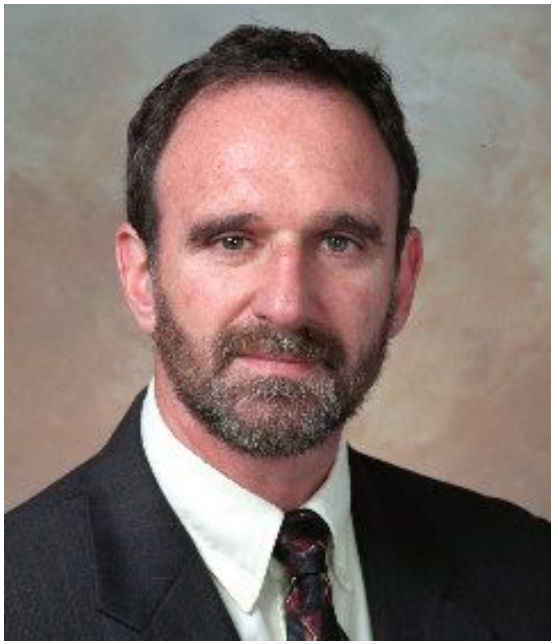
- Öffentliche Forschung
  - Ralph Merkle
  - Whitfield Diffie und Martin Hellman
- Geheime Forschung
  - Clifford Cocks
  - Malcom Williamson

Ralph Merkle

- 1974 (veröffentlicht 1978)
  - 1.Schritt zur Entwicklung asymmetrischer Verfahren
  - „Merkles Puzzle“

Whitfield Diffie & Martin Hellman

- 1976
  - Aufbauend auf Merkles Puzzle
  - „New Directions in Cryphtography“
  - Vergleich mit kopernikanischer Wende
  - Vorarbeiten für RSA-Kryptosystem
  - Turing Award 2015



Geheime Forschung

- 1973
  - Clifford Cocks vom britischen Geheimdienst GCHQ
  - Entwickelt RSA sehr ähnliches Verfahren
  - 1. asymmetrisches Kryptoverfahren
  - Veröffentlichung erst 1997

- 1975
  - Malcom Williamson (GCHQ) entwickelt Diffie-Hellman ähnliches Schlüsselaustauschverfahren

Fragen?

Quellen

- BSI TR-02102-1 "...Empfehlungen und Schlüsse llängen"
- Fernuni Hagen - Das Diffie-Hellman Verfahren
- de.wikipedia.org
- halbleiterbauelemente.de/lehre/dhm-austausch/