Cryptography Engineering

READ

Confidentiality → Encryption

Integrity → Hash Function

WRITE

ursprünglich

Sender: $m \longrightarrow E_k(m) \rightarrow$ Empfänger

Key k

$\rightarrow D_k(E_k(m))$

geheime Schlüssel

bei Sender / Empfänger "gleich"

Symmetrische Verfahren

sonst

asymmetrische bzw. public key Verfahren

1976 Diffie, Hellman

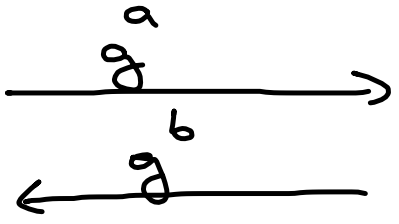
Public key Kryptographie

$g \in G$

Alice | Bob

Diffie-Hellman Schlüsselaustausch

Zufallszahl a | Zufallszahl b



$(g^b)^a = g^{ab} = (g^a)^b$

Diskrete Zahlenmengen

$\mathbb{Z}$ ganze Zahlen

Begrenzung mit Obergrenze n allgemein

p Primzahl

Bezeichnung: $\mathbb{Z}/n\mathbb{Z}$ RSA

$\mathbb{Z}/p\mathbb{Z}$ Diffie-Hellman

Rechenregeln

$\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, 3, \ldots, p-1\}$

" $\mathbb{Z}$ modulo $p\mathbb{Z}$ "

- Grundrechenart $+, -, \cdot$ ausführen
- Ergebnis mod p mit (meist) positivem Rest darstellen

Diffie – Hellman – Schlüsselaustausch

p Primzahl $\quad p = 11$

g Erzeuger (generator) $\quad g = 2$

Alice		Bob
$a = 8$		$b = 9$
$g^a \bmod p$	$\xrightarrow{2^8 \bmod 11 \equiv 3}$	
	$\xleftarrow{2^9 \bmod 11 \equiv 6}$	$g^b \bmod p$
6^8		$3^9 \bmod 11$
$\equiv 4 \equiv$		

Tools:

PARI/GP

OpenSSL

Übung:

Diffie-Hellman

mit 2048-Bit

Parameterlänge demonstrieren

können (PARI/GP)