Thema: Moderne symmetrische Verschlüsselungsverfahren

Stromchiffre vs. Blockchiffre

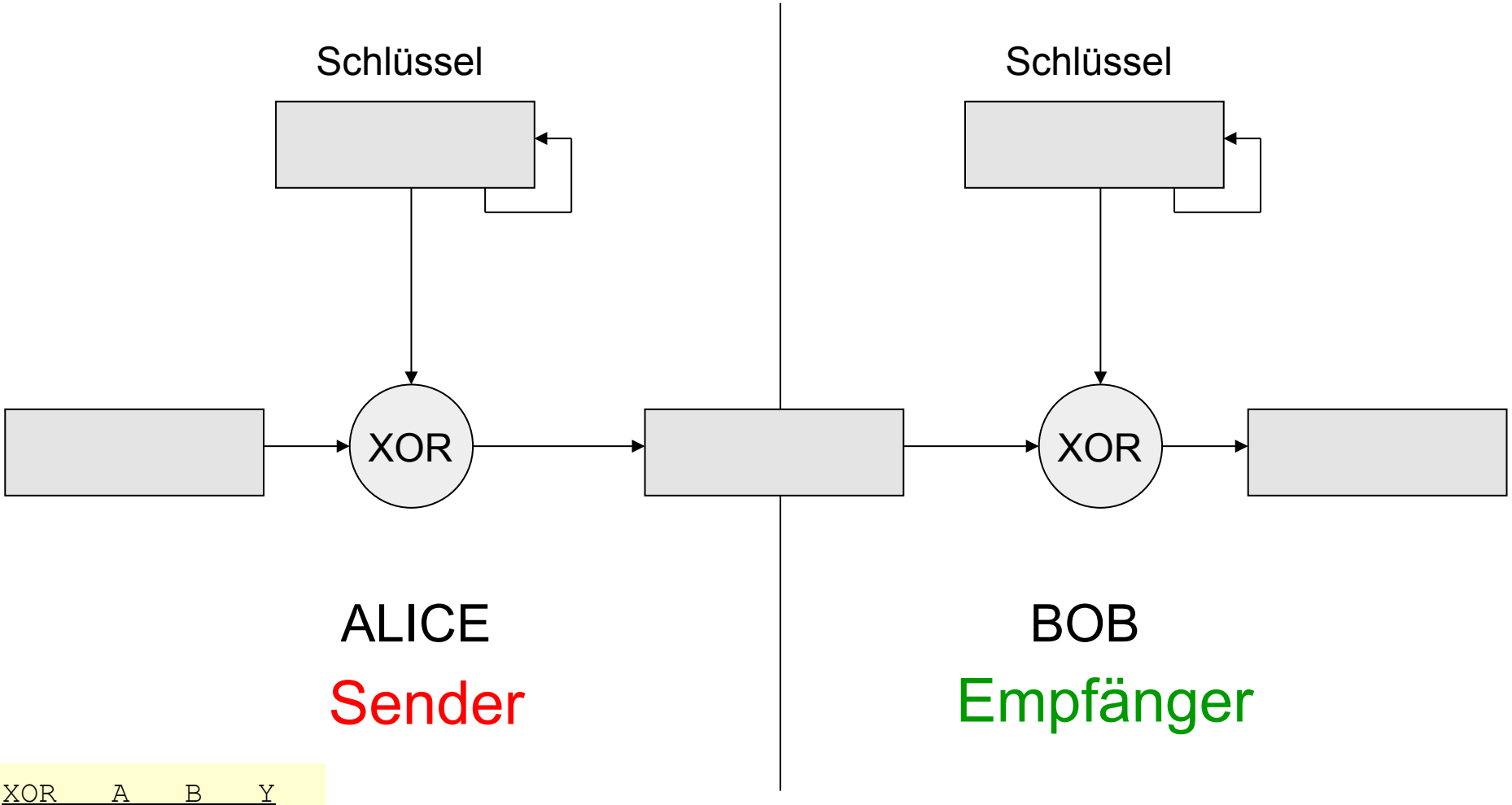
ARJ / Okt-2015

Blockchiffre : Algorithmus der einen Datenblock von 64 oder 128 Bit mittels Schlüsselwerts verschlüsselt.
Längerer Nachrichten werden vorerst in Blöcke unterteilt
Länge verschlüsselter Block 64 bzw. 128 Bit
Typ. Schlüsselllänge 112, 128 und 168 Bit.
Beispiele: DES, AES und IDEA.

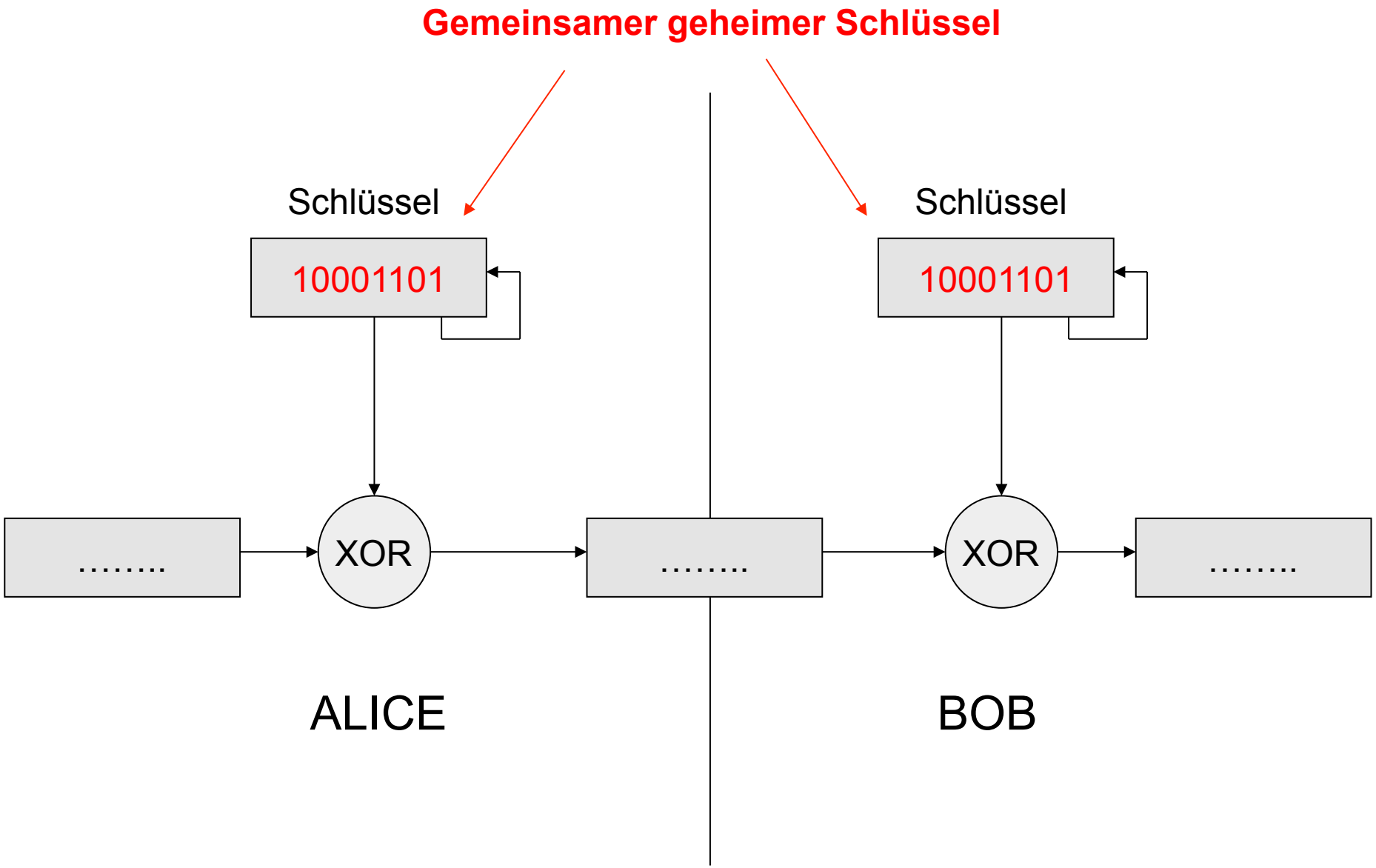
Stromchiffre: Symmetrische, kontinuierliche und verzögerungsfreie Ver- oder Entschlüsselung eines Datenstroms.
Stromchiffre ver- bzw. entschlüsselt Nachrichten Bit für Bit bzw. Zeichen für Zeichen.
Beispiele: XOR-Verschlüsselung, RC4, Scrambling 1000Base-T

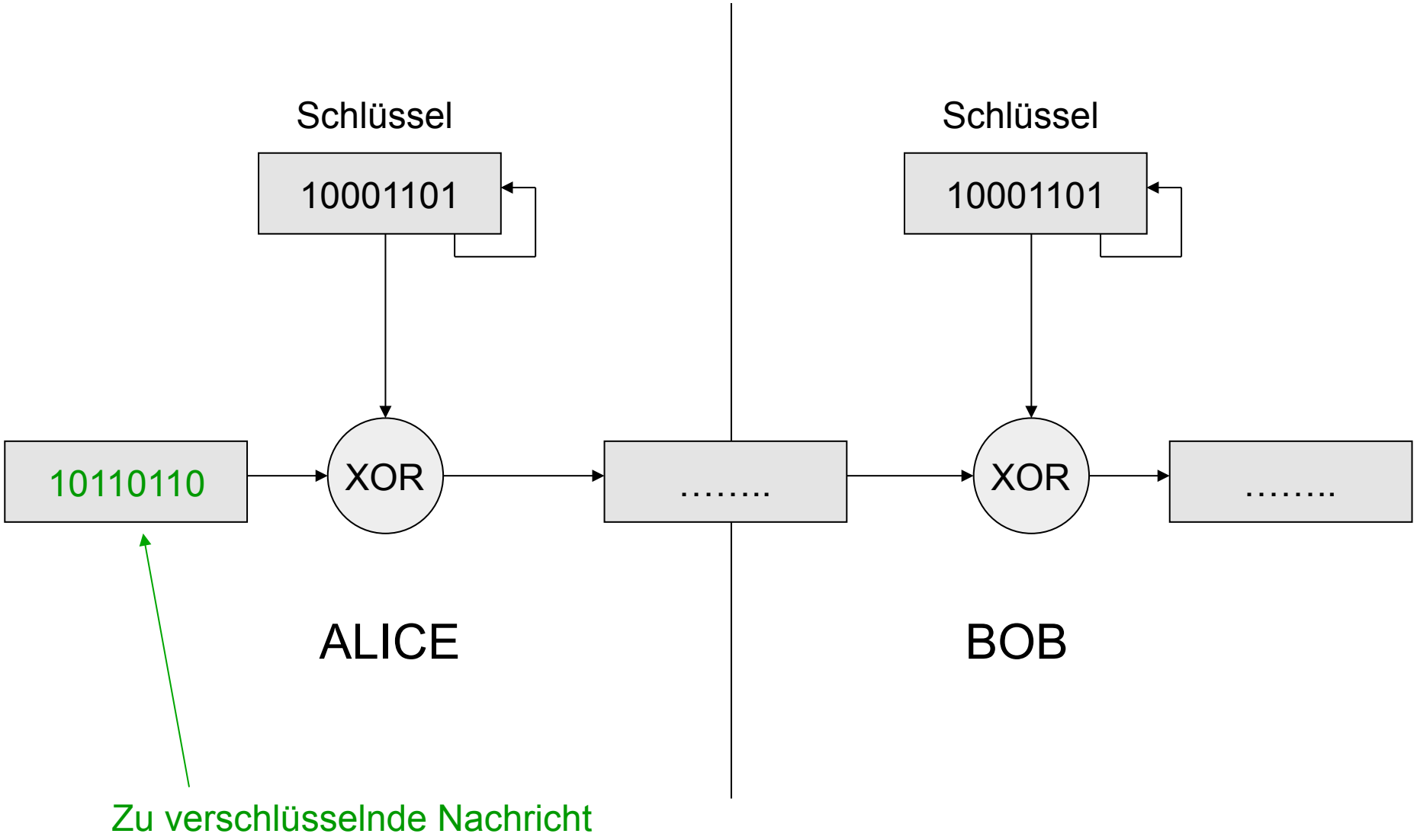
Probleme bei Stromchiffren:
Hat ein Angreifer Klartext UND Chiffretext, so kann er den Schlüsselstrom rekonstruieren. Weitere Nachrichten, die mit diesem Schlüsselstrom verschlüsselt werden, können also zumindest solange entschlüsselt werden, wie Bits im Schlüsselstrom vorliegen. Genau diese Lücke tritt bei der Verschlüsselung von drahtlosen Netzen mittels WEP auf. (Wired Equivalent Privacy)

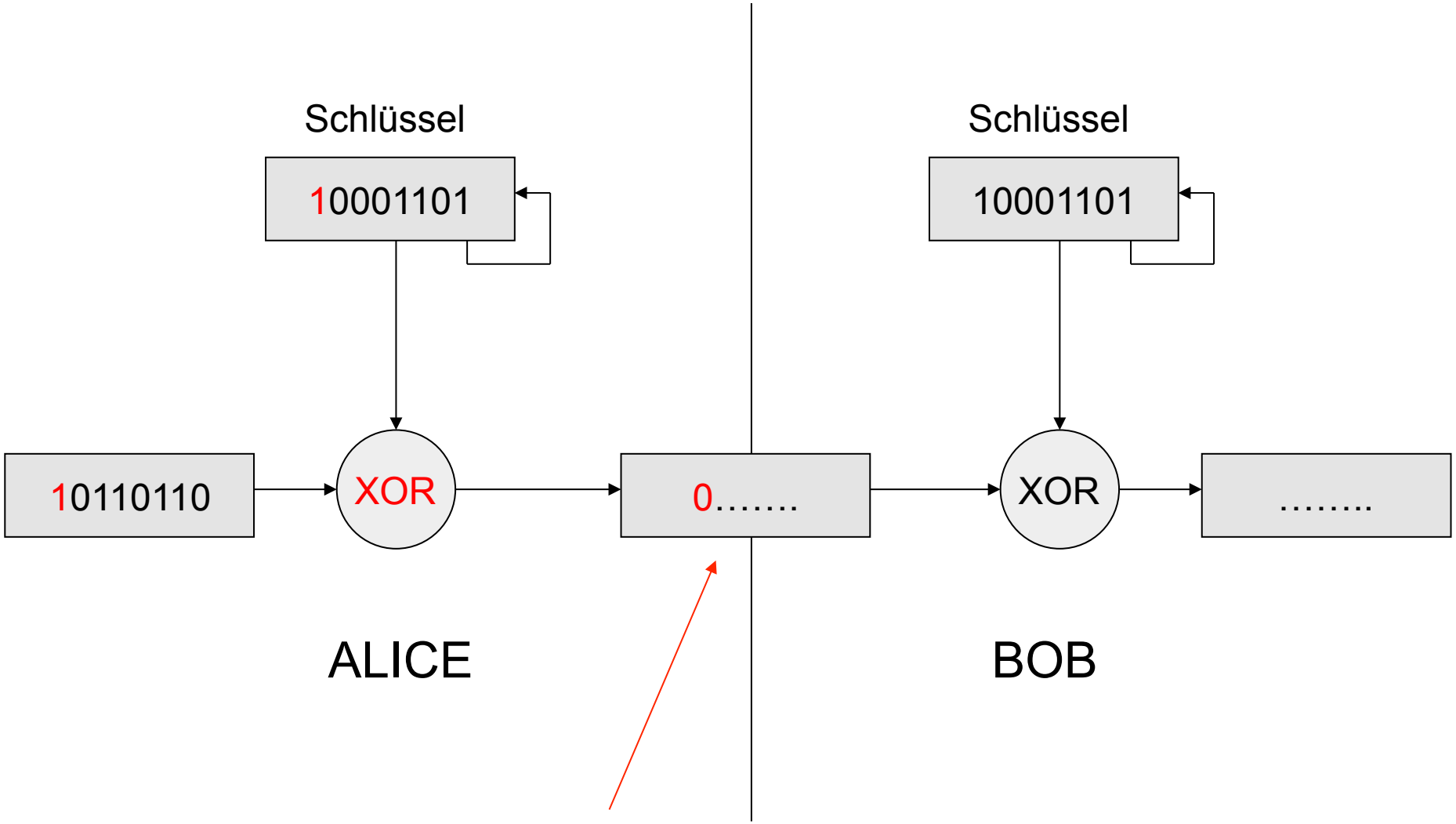
Die XOR-Stromchiffre

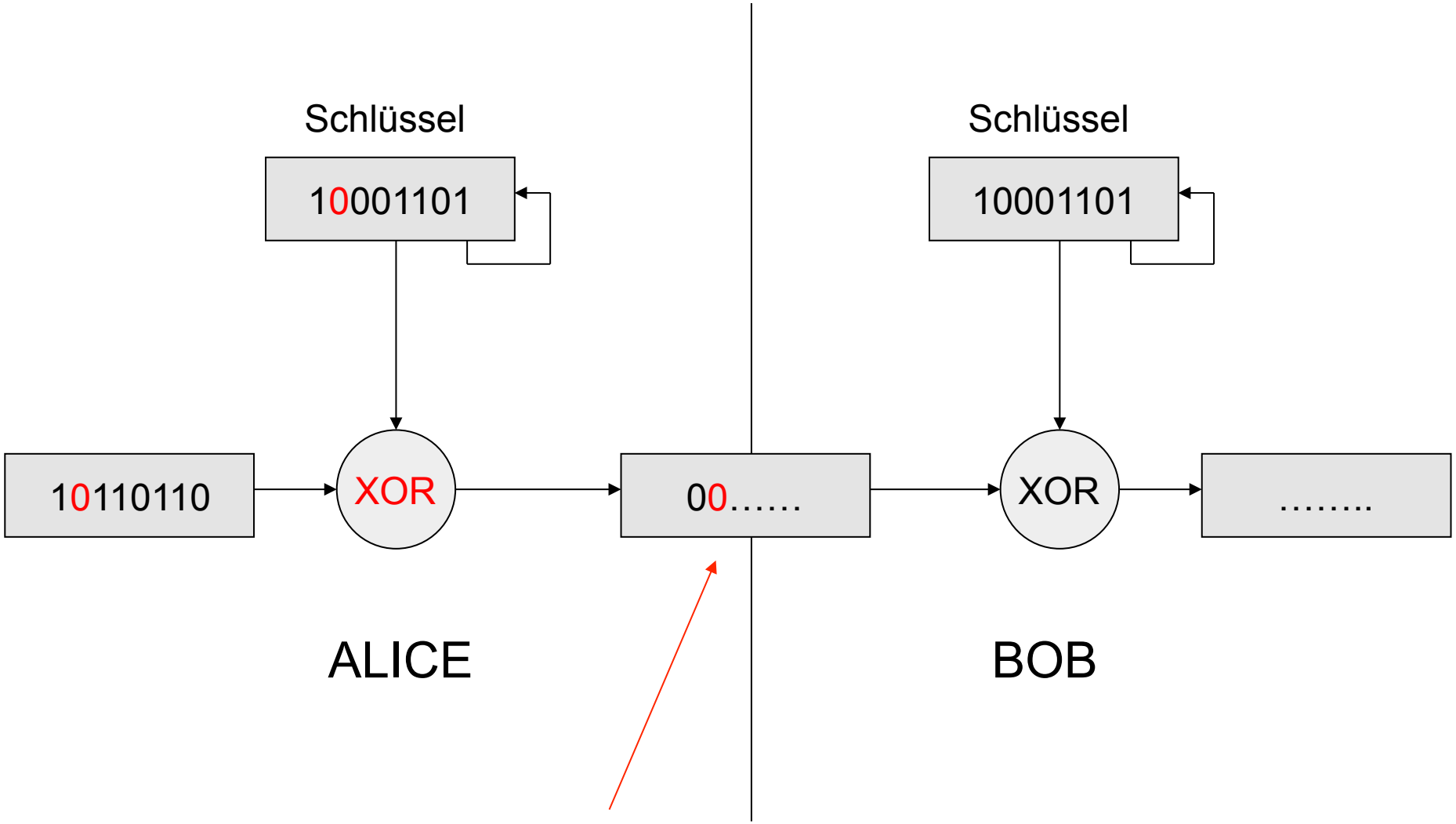


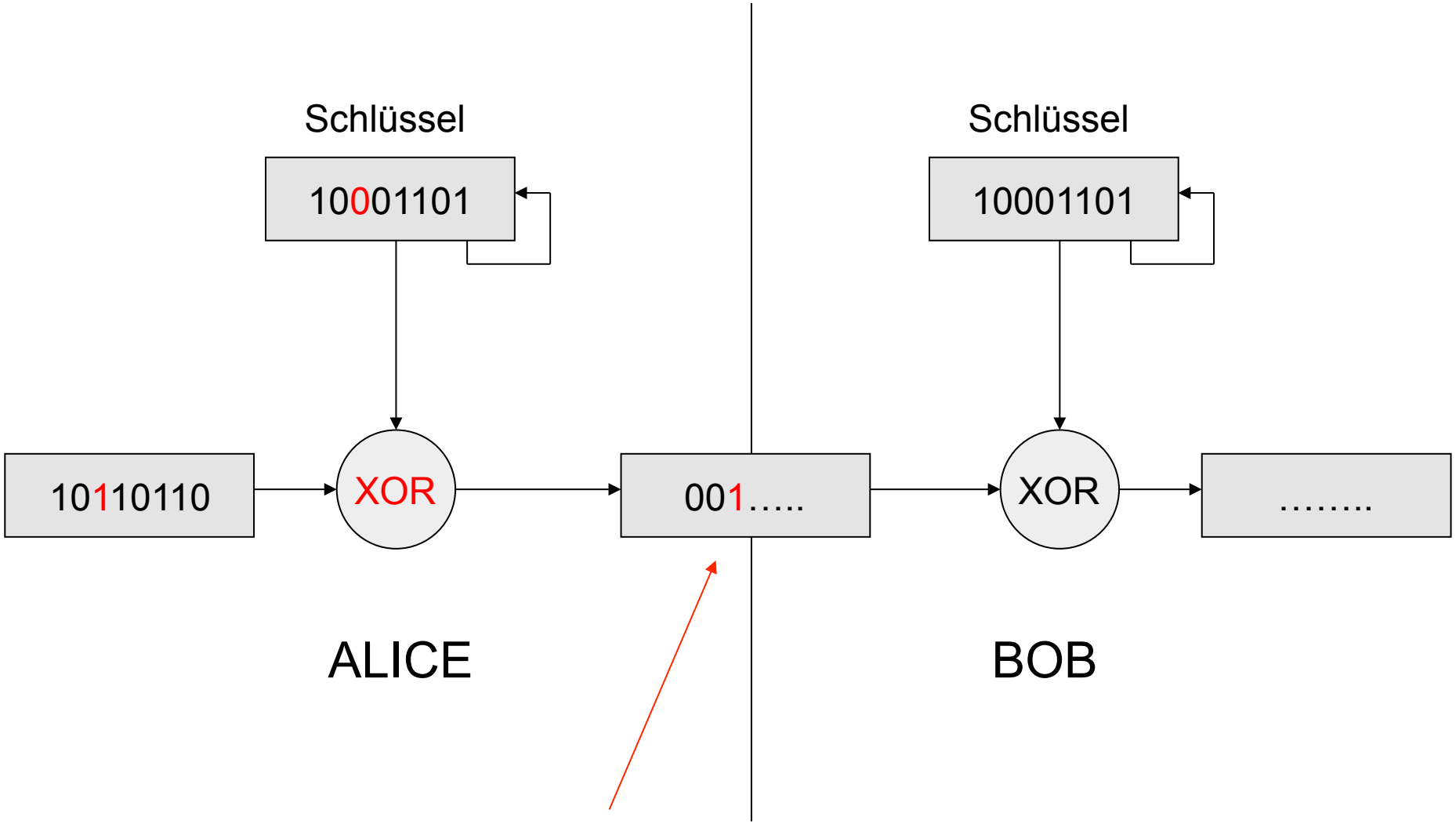
XOR	A	B	Y
	0	0	0
	0	1	1
	1	0	1
	1	1	0

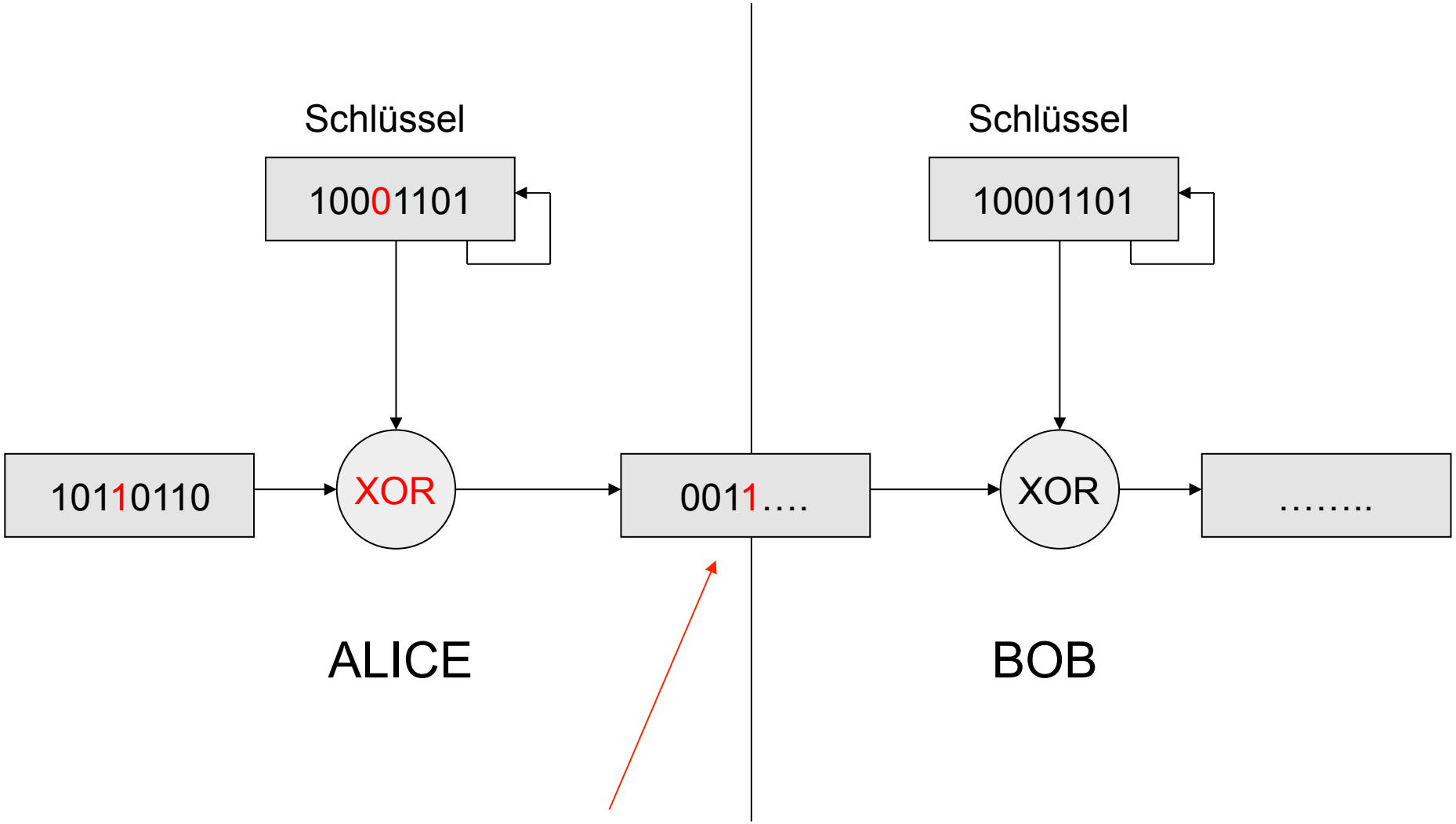

Gemeinsamer geheimer Schlüssel
Schlüssel
Schlüssel
10001101
10001101
XOR
XOR
ALICE
BOB

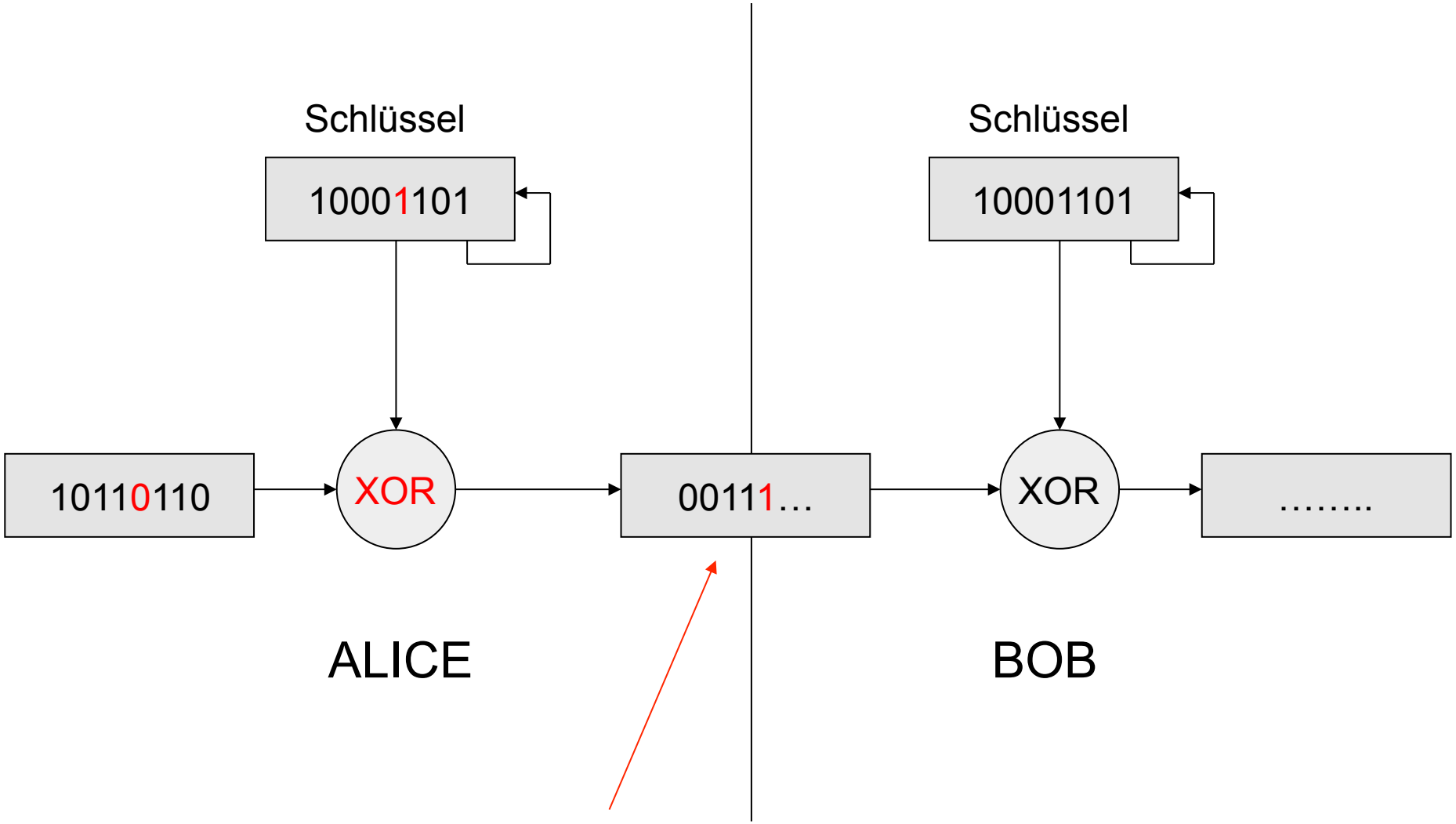

Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
……..
XOR
……..
ALICE
BOB
Zu verschlüsselnde Nachricht

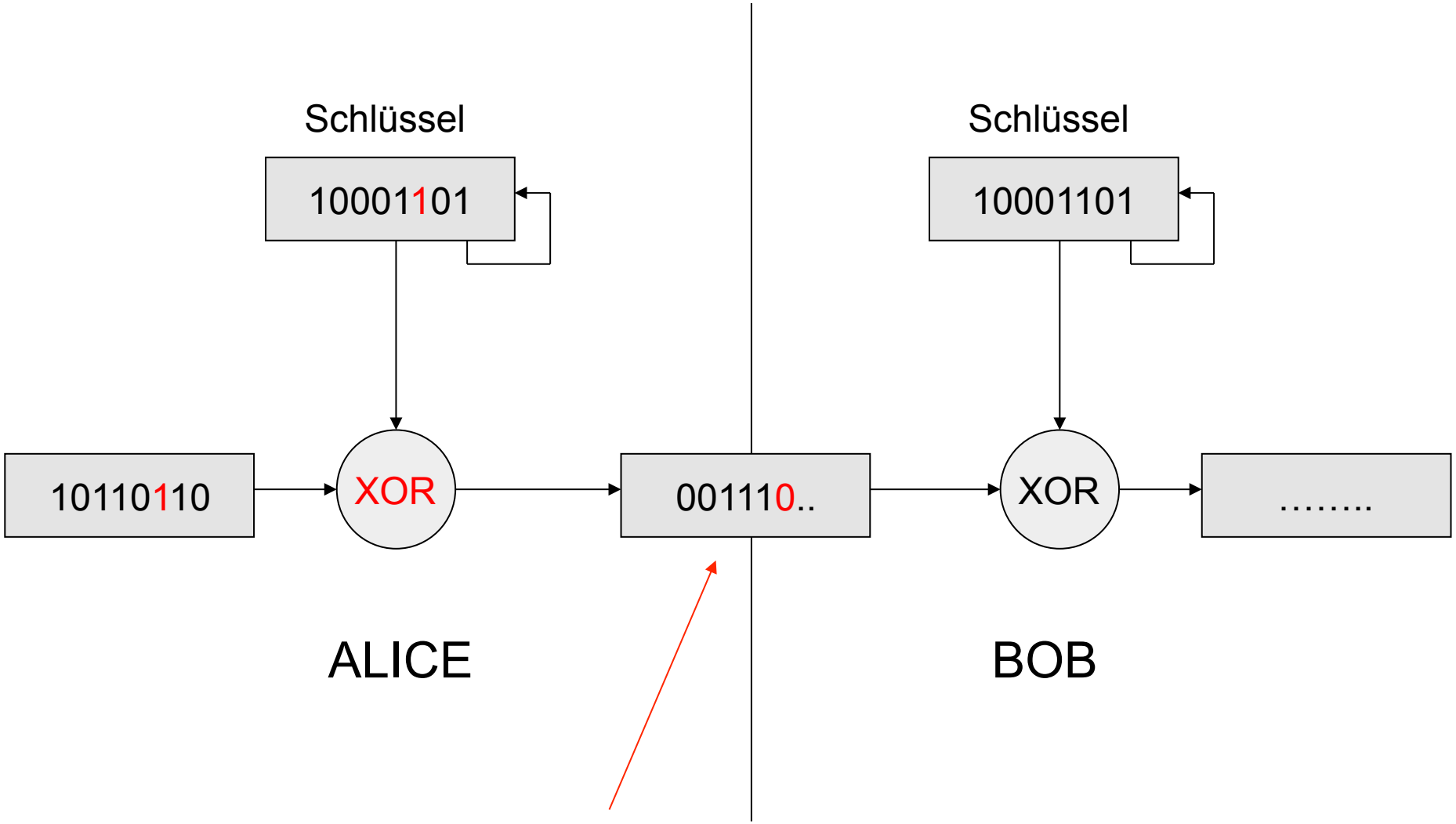

Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
0.....
XOR
.....
ALICE
BOB
1. Zeichen XOR-verschlüsselt

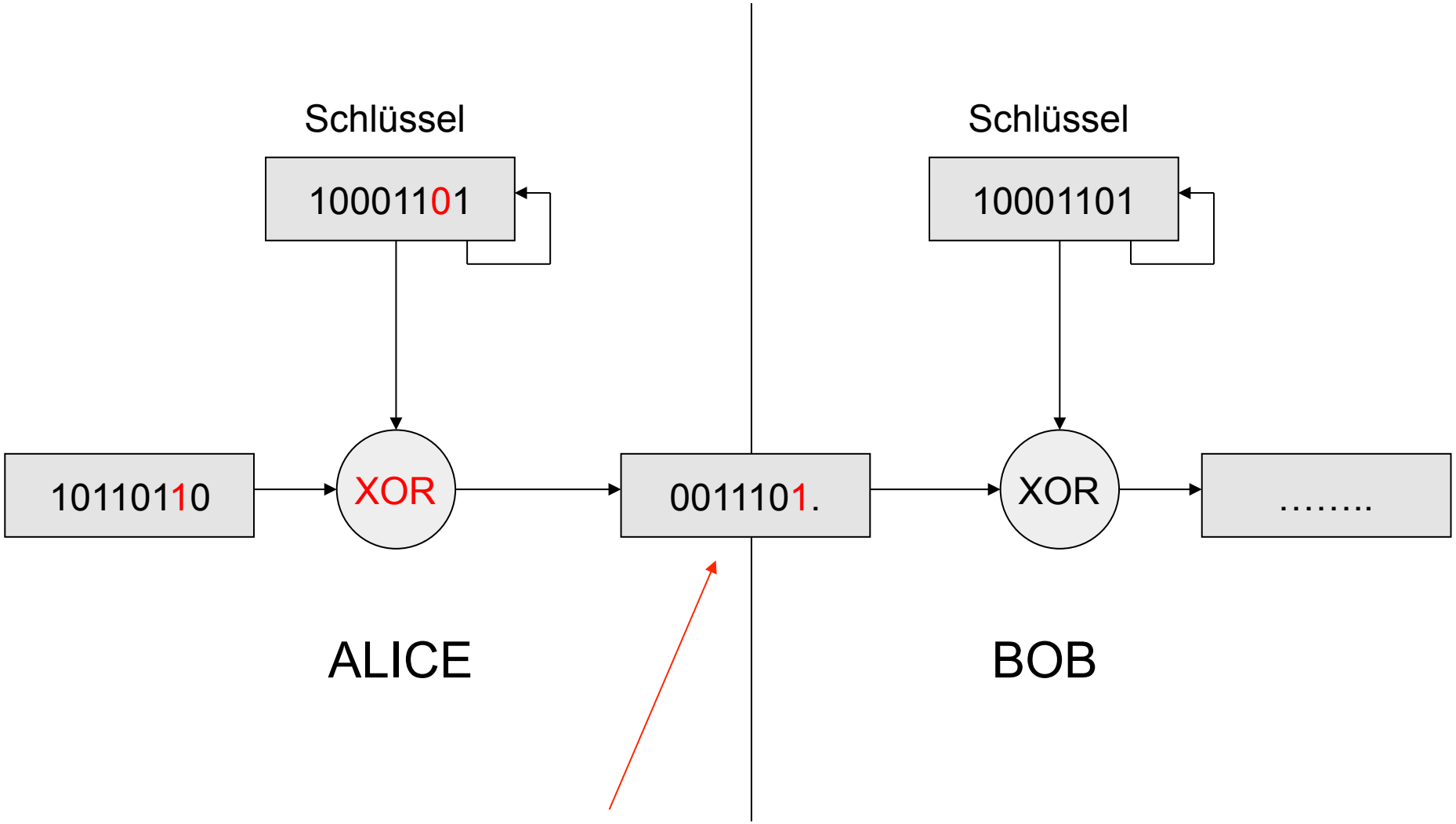

Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
00……
XOR
……..
ALICE
BOB
2. Zeichen XOR-verschlüsselt

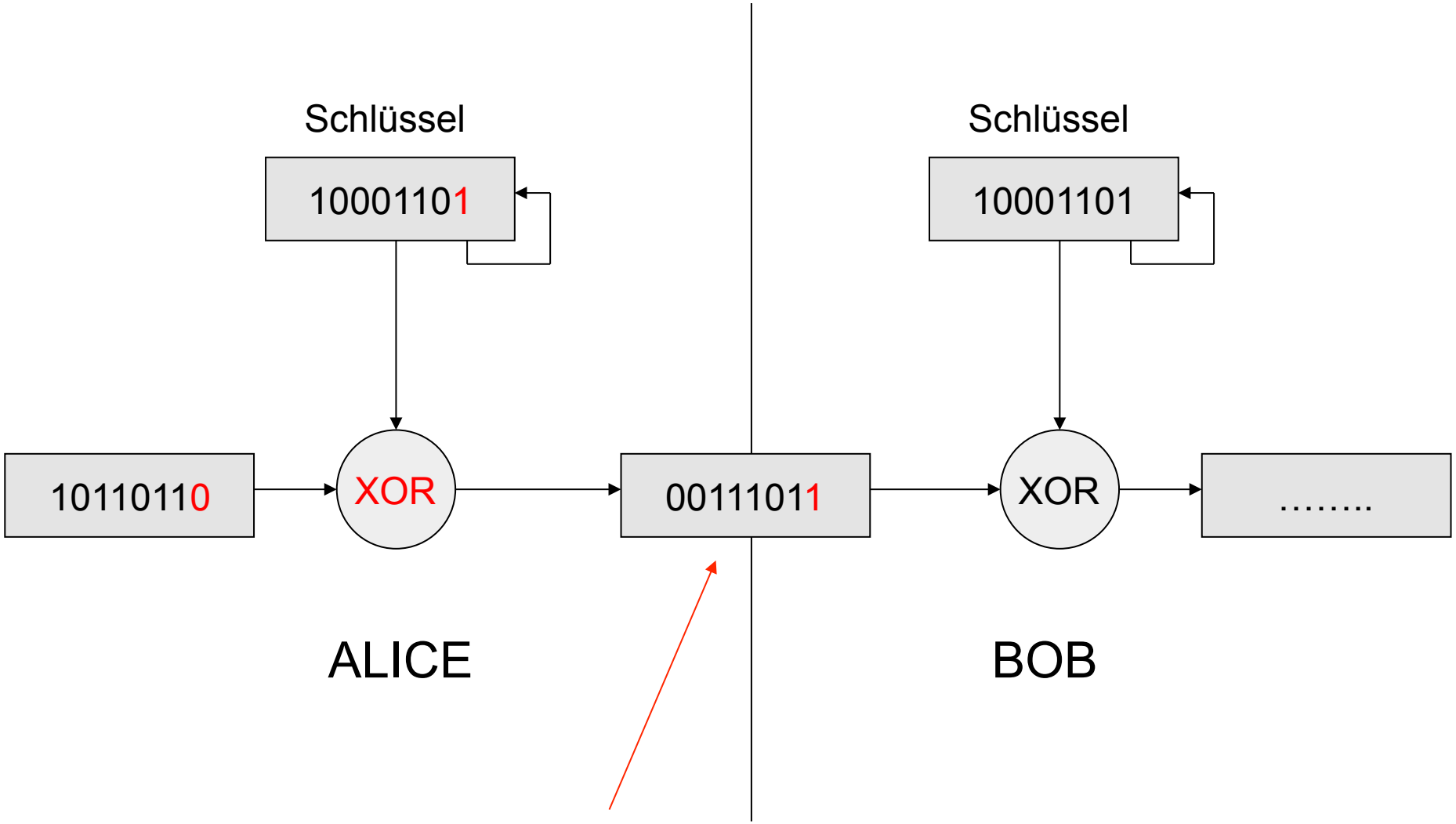

Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
001.....
XOR
.....
ALICE
BOB
3. Zeichen XOR-verschlüsselt

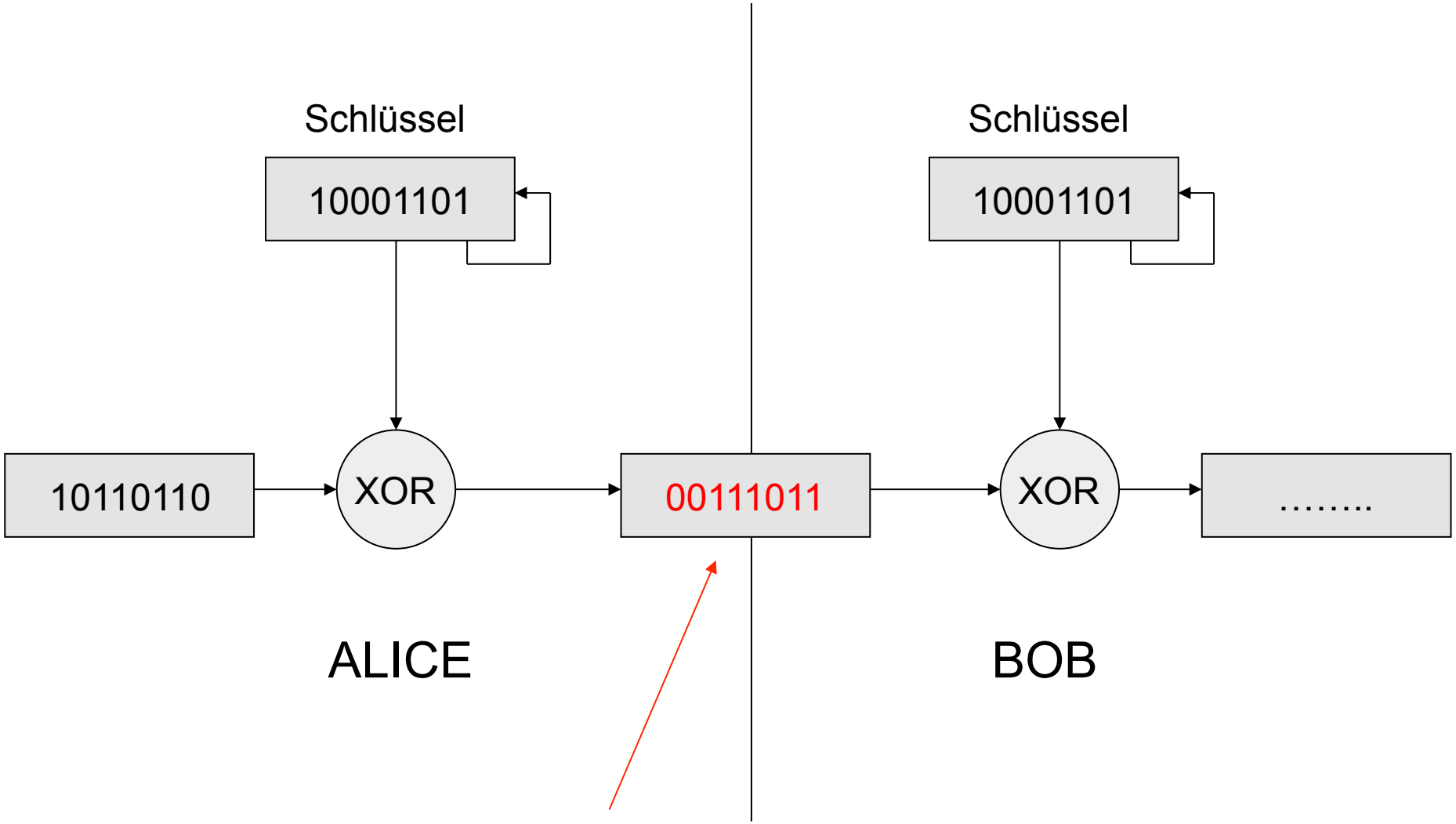

Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
0011....
XOR
.....
ALICE
BOB
4. Zeichen XOR-verschlüsselt

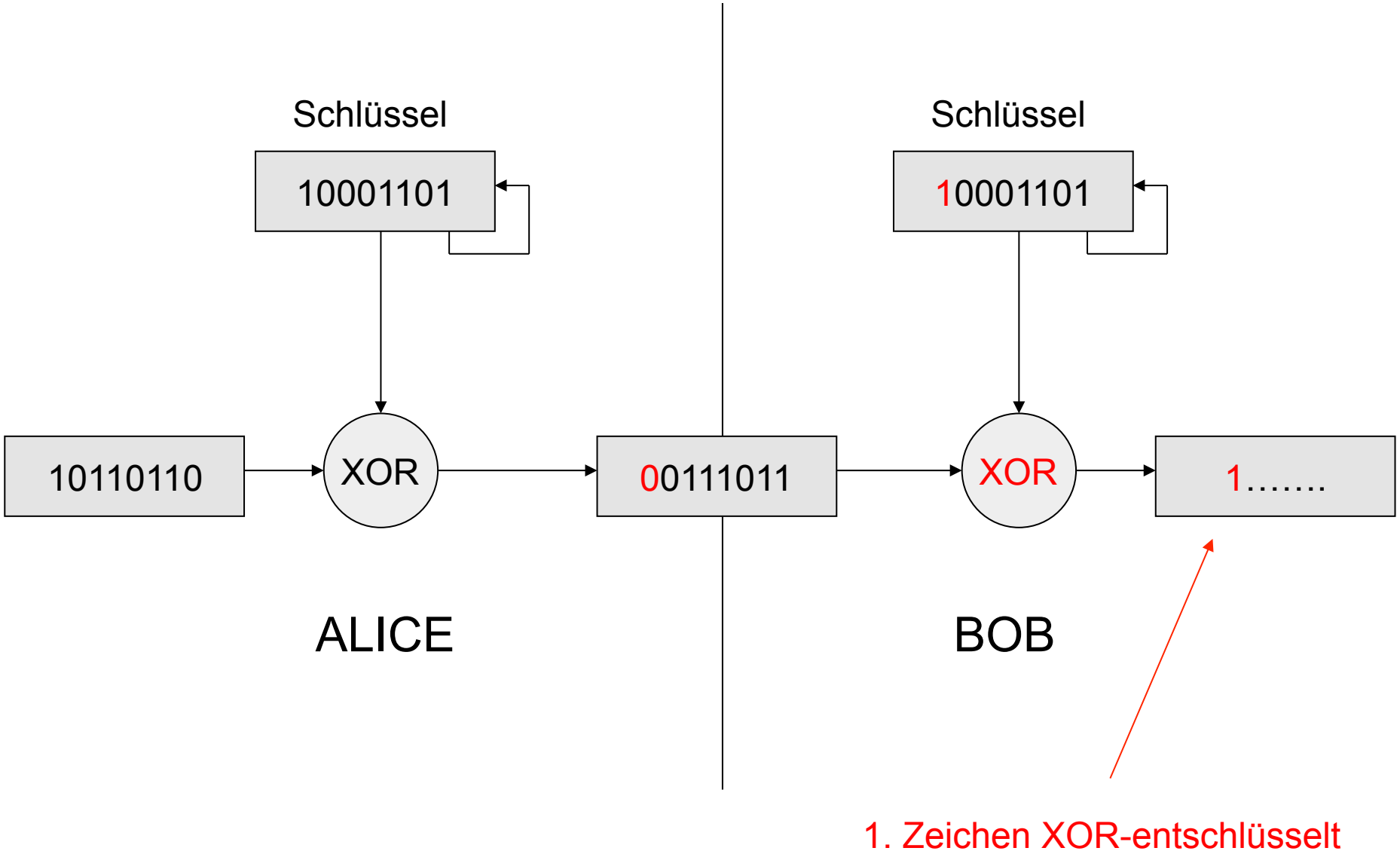

Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
00111…
XOR
……..
ALICE
BOB
5. Zeichen XOR-verschlüsselt

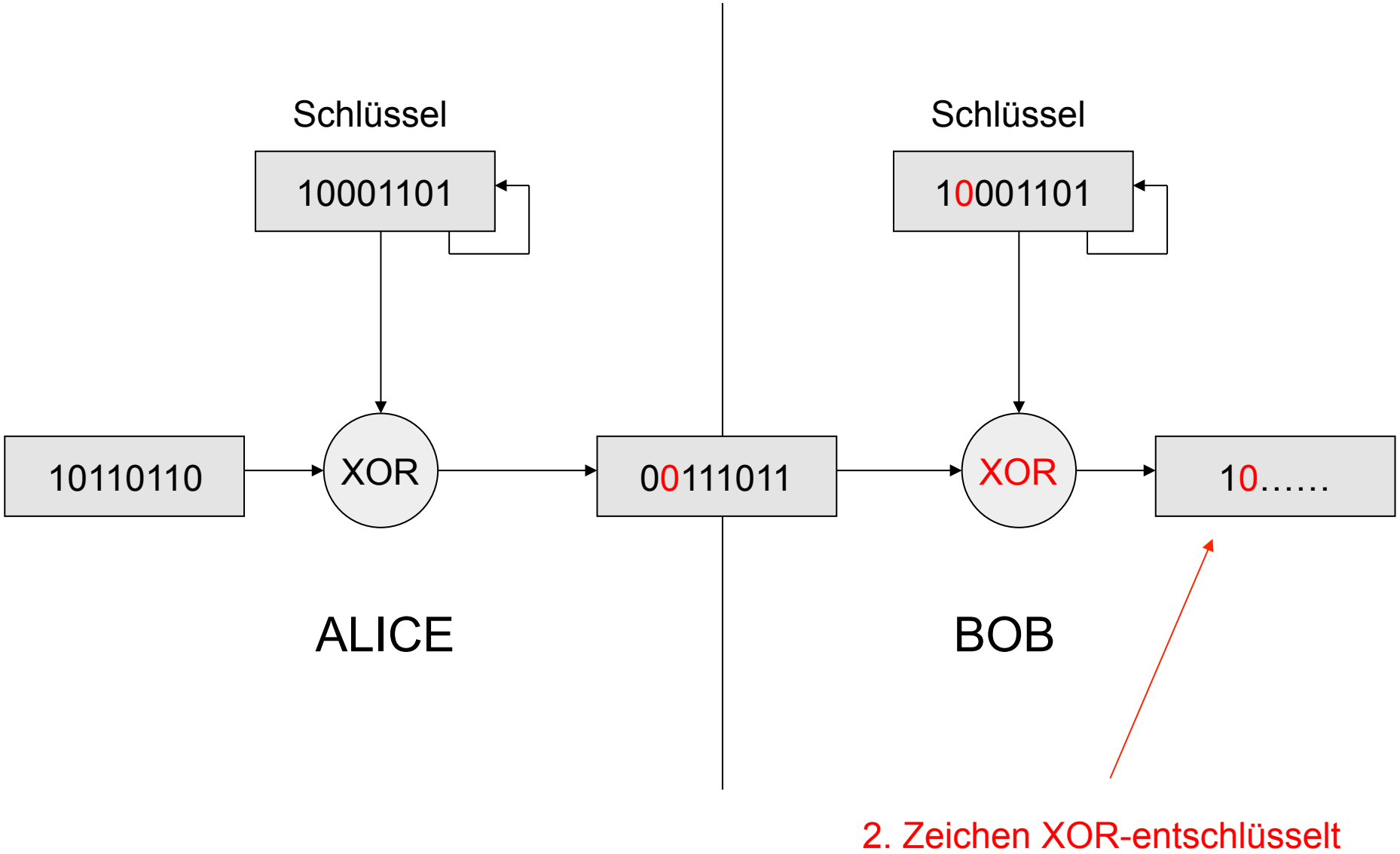

Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
001110..
XOR
……..
ALICE
BOB
6. Zeichen XOR-verschlüsselt

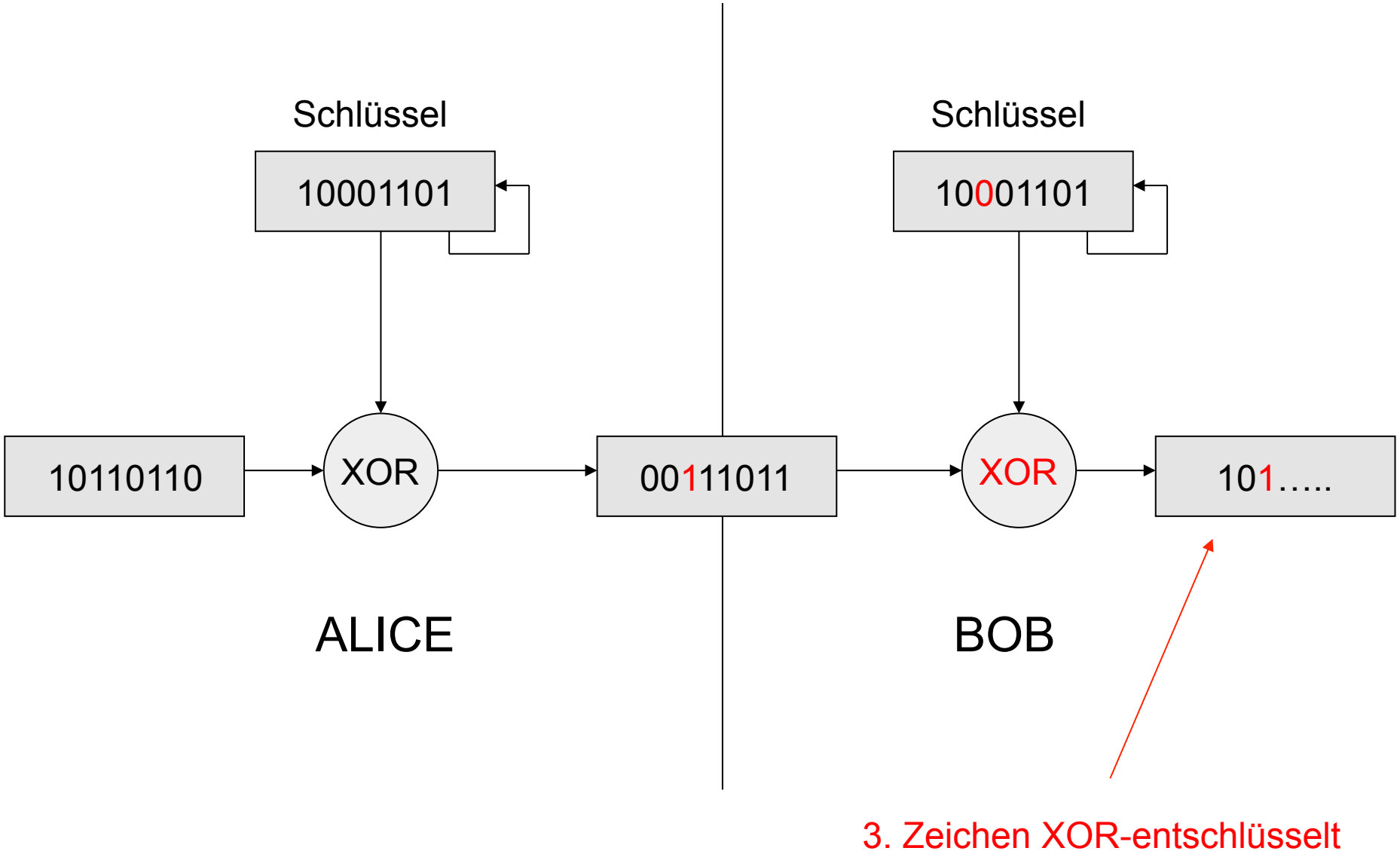

Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
0011101.
XOR
……..
ALICE
BOB
7. Zeichen XOR-verschlüsselt

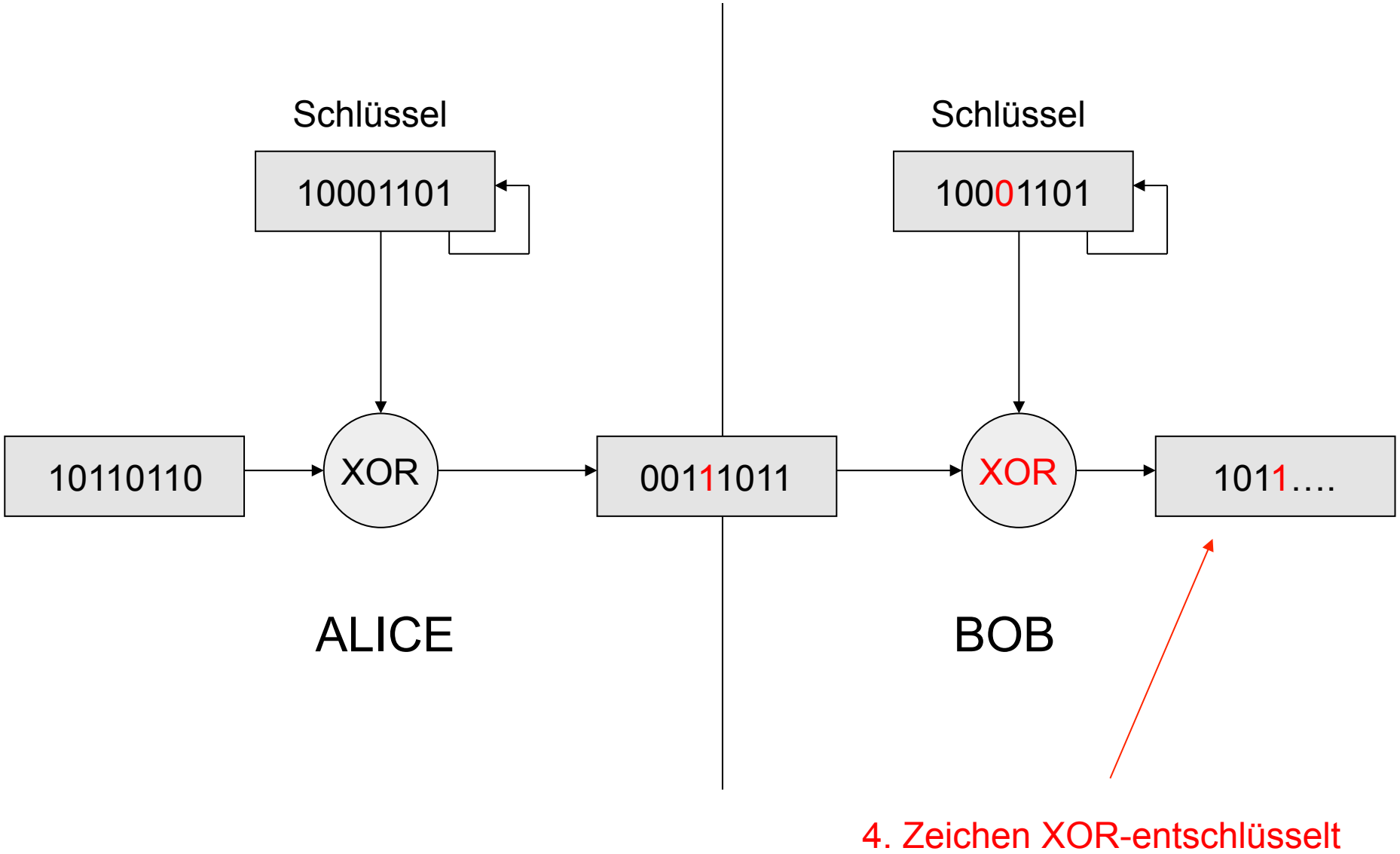

Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
00111011
XOR
……..
ALICE
BOB
8. Zeichen XOR-verschlüsselt

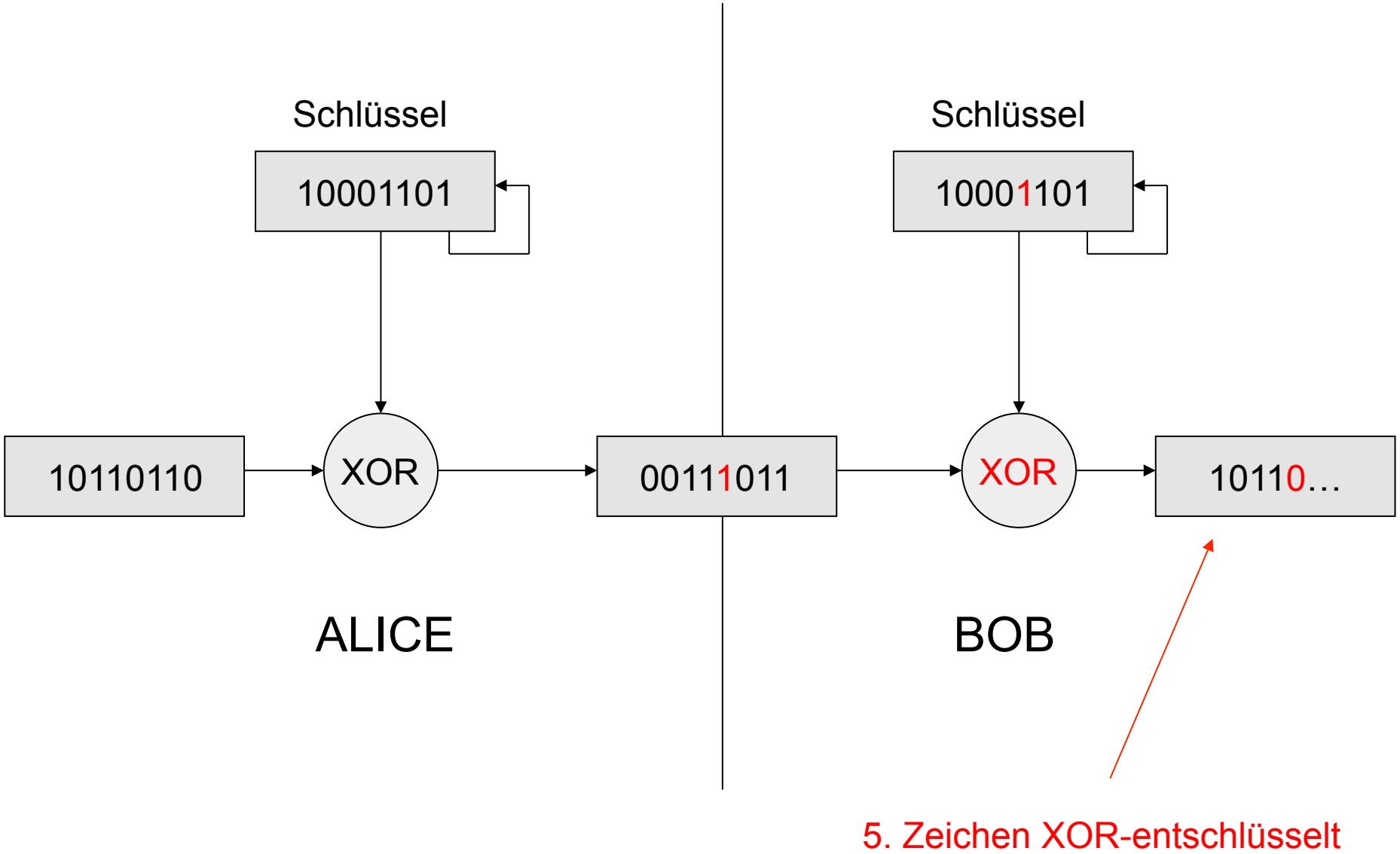

Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
00111011
XOR
……..
ALICE
BOB
Chiffre; Unlesbar für Aussenstehende!
Diese Chiffre kann über einen unsicheren
Kanal verschickt werden.

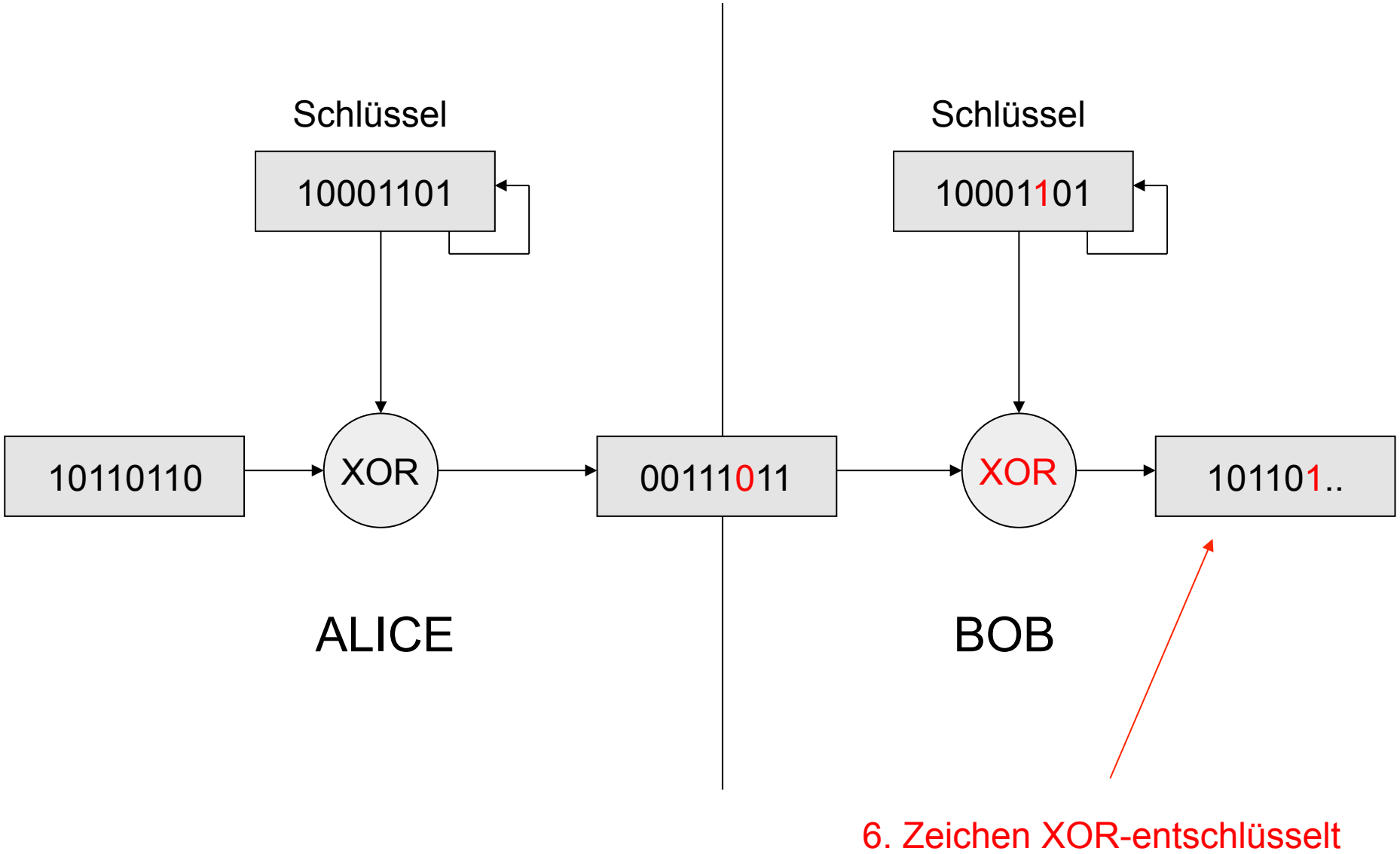

Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
00111011
XOR
1.....
ALICE
BOB
1. Zeichen XOR-entschlüsselt

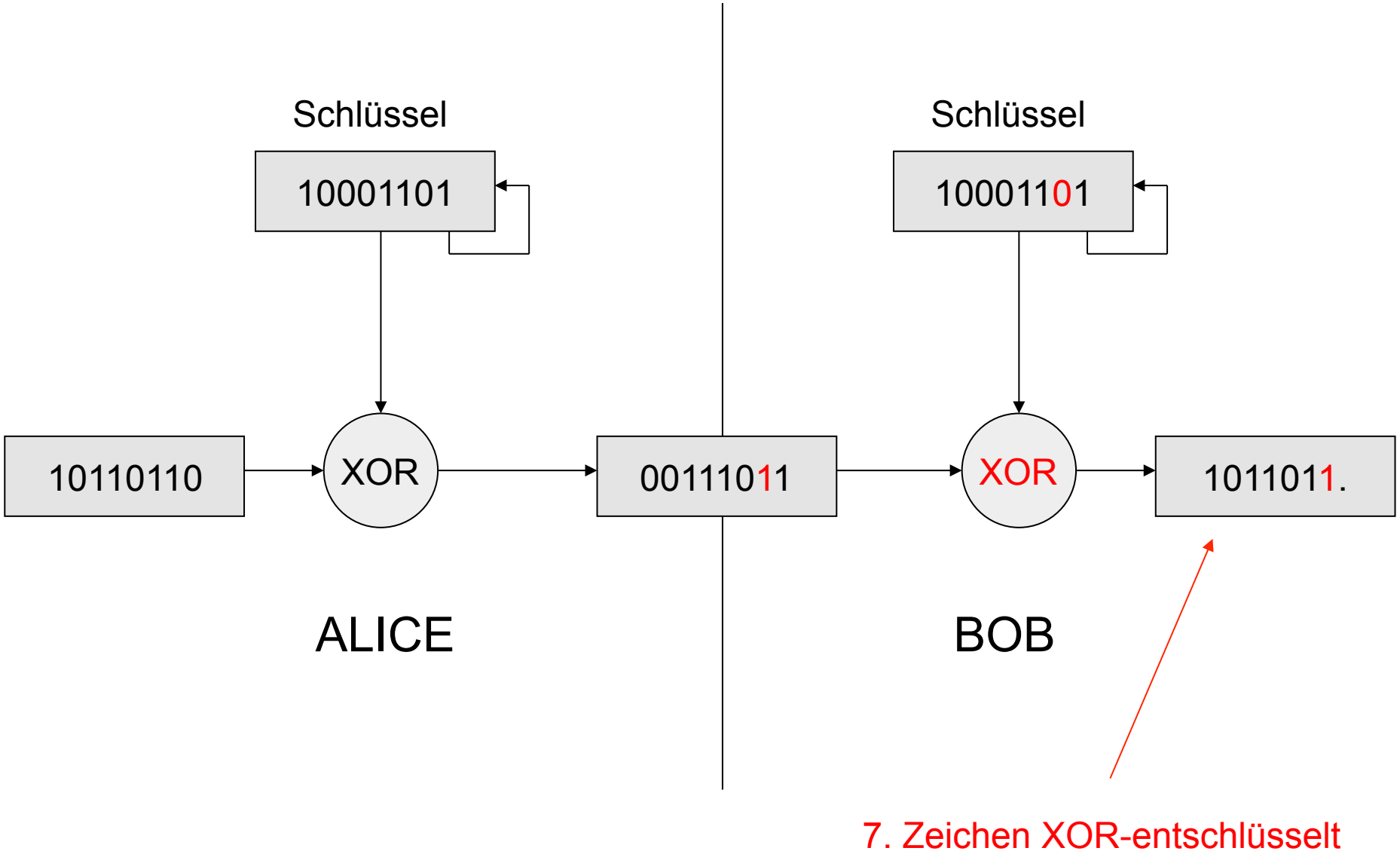

Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
00111011
XOR
10……
ALICE
BOB
2. Zeichen XOR-entschlüsselt

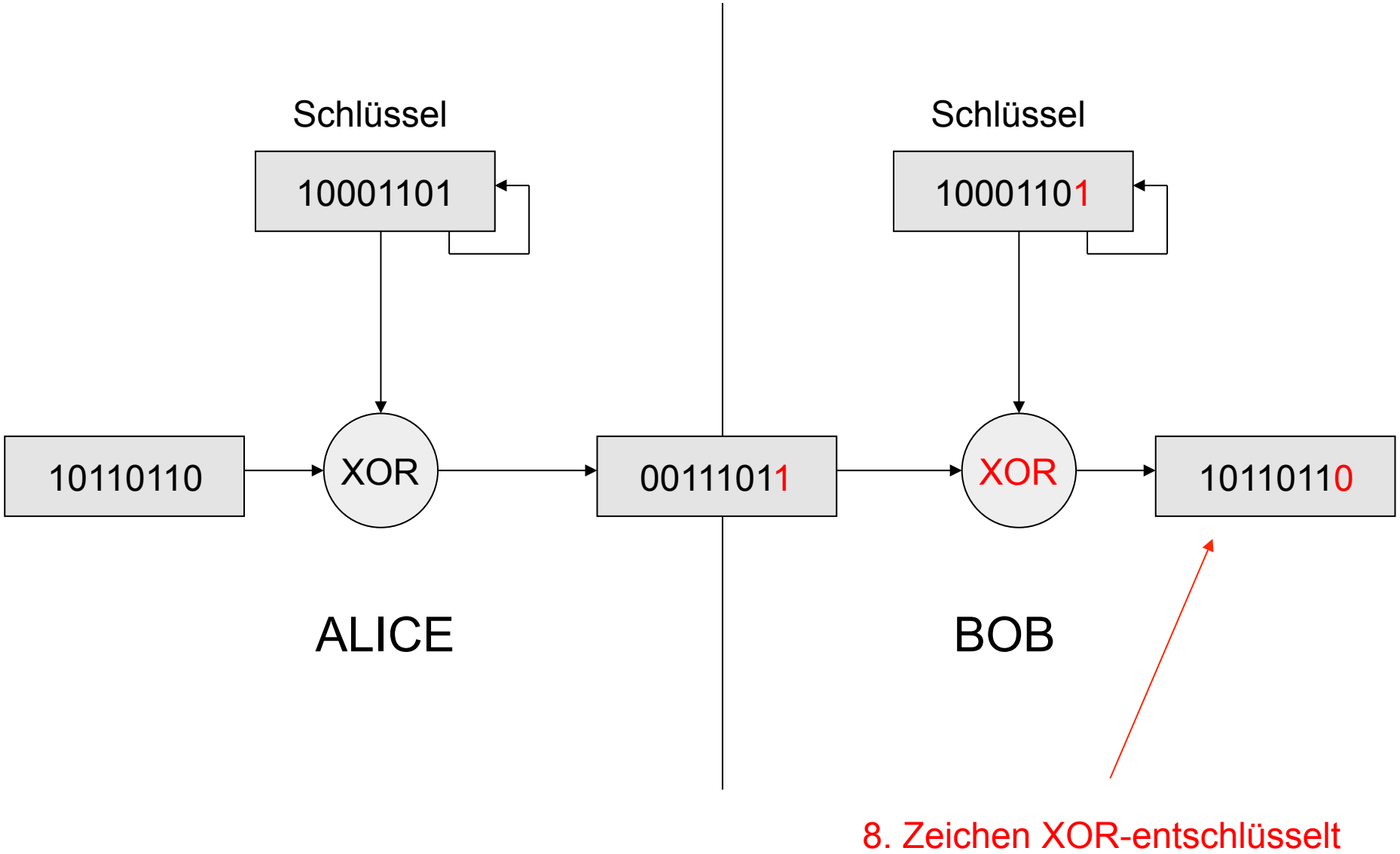

Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
00111011
XOR
101.....
ALICE
BOB
3. Zeichen XOR-entschlüsselt

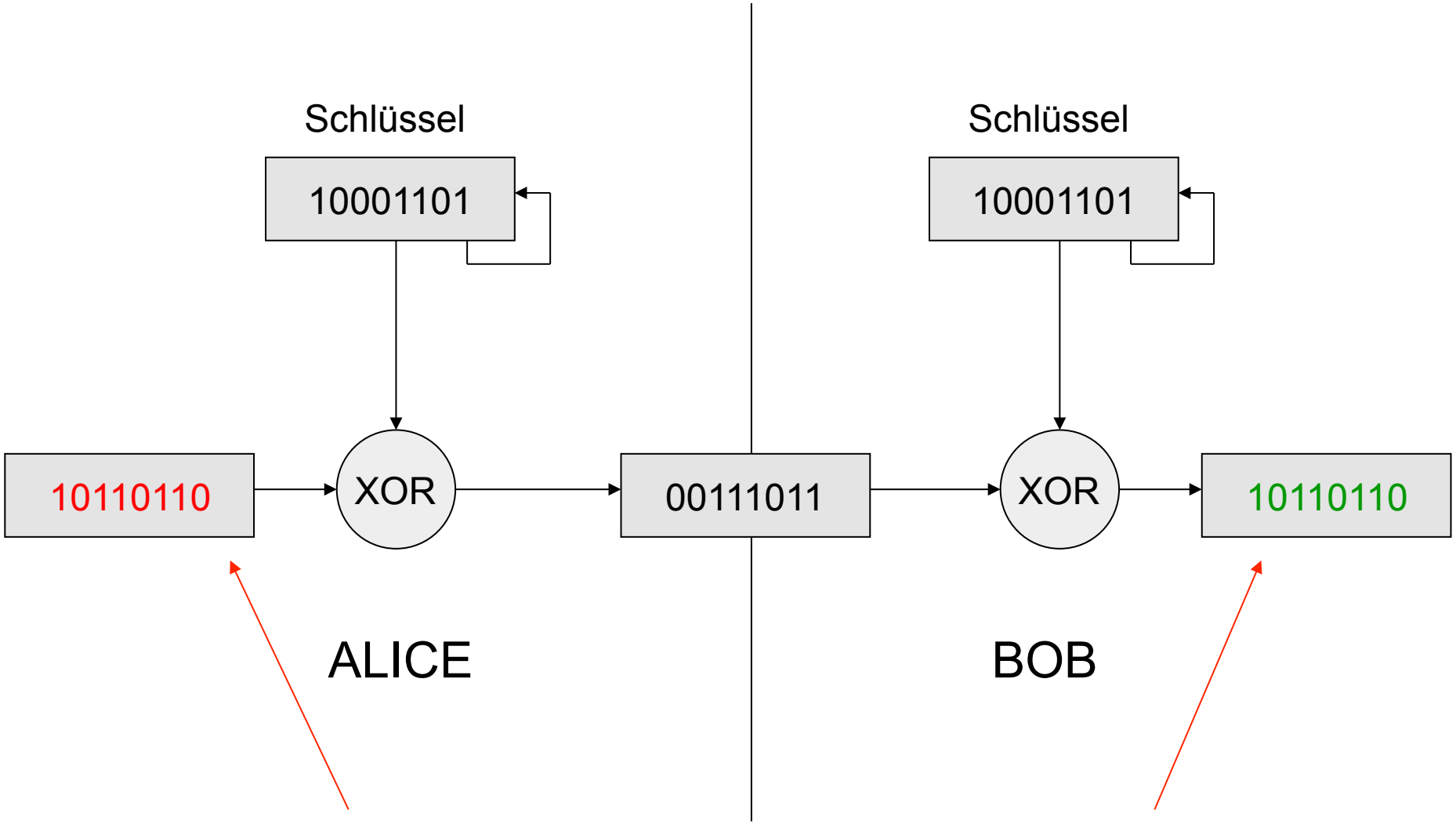

Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
00111011
XOR
1011....
ALICE
BOB
4. Zeichen XOR-entschlüsselt


Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
00111011
XOR
10110…
ALICE
BOB
5. Zeichen XOR-entschlüsselt


Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
00111011
XOR
101101..
ALICE
BOB
6. Zeichen XOR-entschlüsselt


Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
00111011
XOR
1011011.
ALICE
BOB
7. Zeichen XOR-entschlüsselt


Schlüssel
10001101
Schlüssel
10001101
10110110
XOR
00111011
XOR
10110110
ALICE
BOB
8. Zeichen XOR-entschlüsselt



Sender und Empfänger haben identische Daten

RC4 ist ein in den 80‘er Jahren von Ron Rivest entwickelter Stromchiffre-Algorithmus.

Häufigste Anwendung : Sichere **SSL**-Verbindung bzw. Verschlüsselung des Datenstroms bei Webbrowsern

Aufgabe zur XOR-Stromchiffre

Verschlüsseln sie die Dezimalzahl 2015 mit XOR-Stromchiffre.
Der binäre Schlüssel lautet: **`1000'1101`**
Zur Kontrolle entschlüsseln sie die erhaltene Chiffre wieder.
Hinweis: Sie müssen die Dezimalzahl zuerst in Biär umrechnen.
Der Schlüssel wiederholt sich immer wieder.
Der Datenstrom beginnt mit der Übertragung des MSB's, also von links nach rechts.