KRYPTPOGRAPHIE

Grundlagen, Geschichte, Anwendung

Referat von Pawel Strzyzewski, Wintersemester 2006, FH Aachen
Seminare »Privacy 2.0« und »We-Blog«

Übersicht

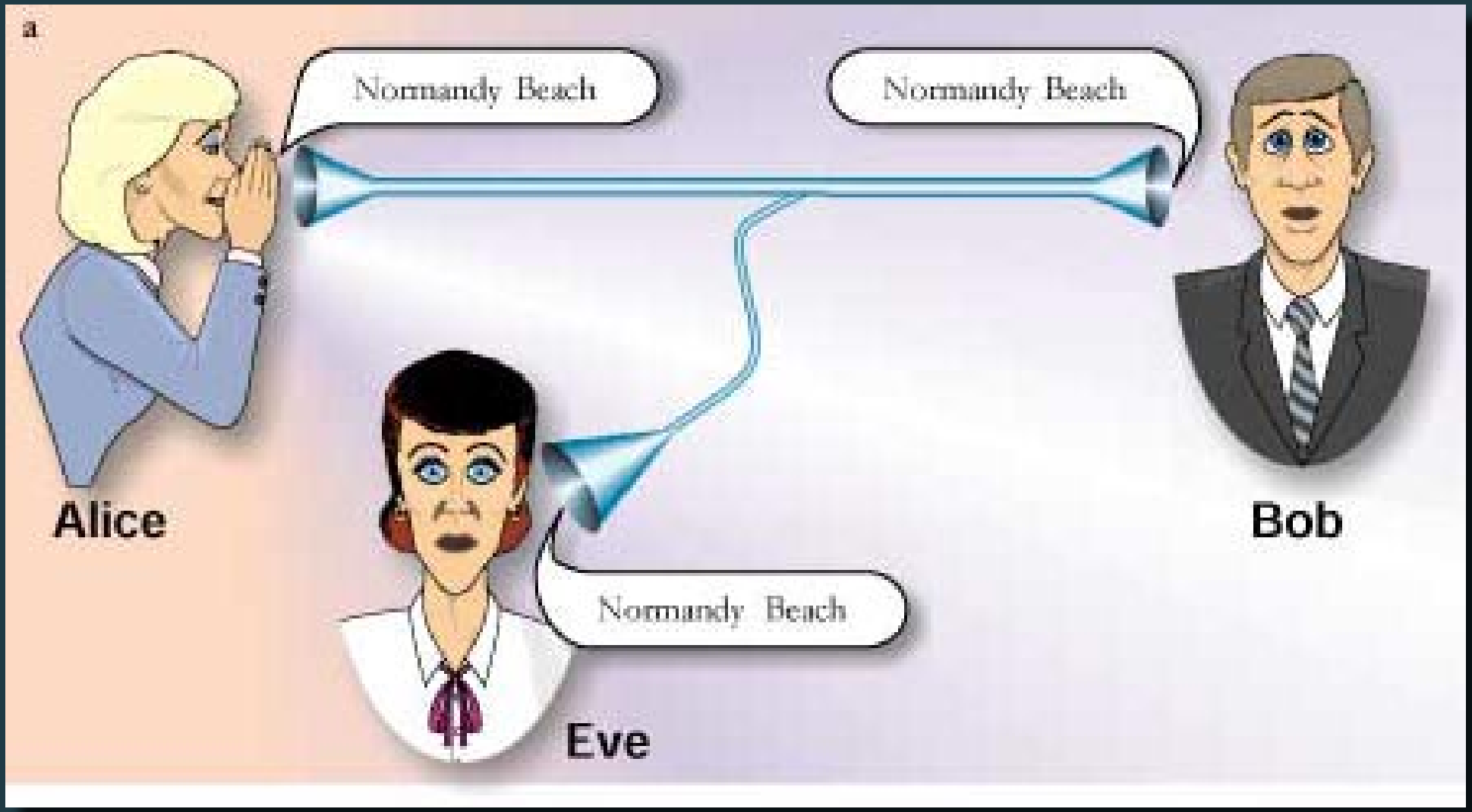
- **1. Grundlagen** ~ 15 Minuten
  - **1a** Crashkurs: »Wozu Kryptographie?«
  - **1b** Wie funktioniert Verschlüsselung?
  - **1c** Historische Beispiele

- **2. Moderne Anwendung** ~ 15 Minuten
  - **2a** Symmetrisch, asymmetrisch?
  - **2b** Elektronische Signatur
  - **2c** Zertifikate
  - **2d** Hybride Systeme

- **3. Fragen, Diskussionsrunde** ~ ? Minuten

1. Grundlagen

Crashkurs: »Wozu Kryptographie?«


a
Normandy Beach
Normandy Beach
Alice
Bob
Normandy Beach
Eve

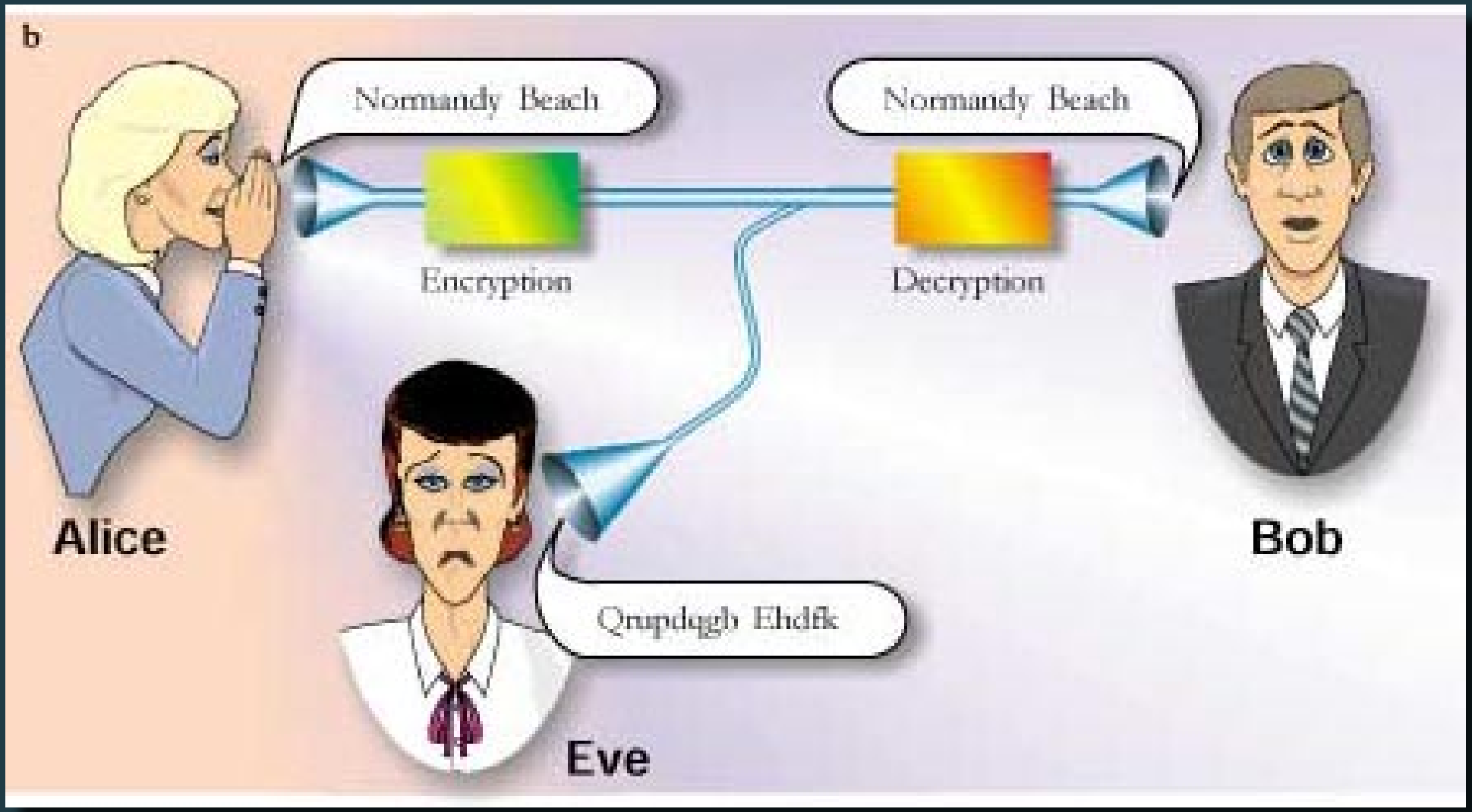
Crashkurs: »Wozu Kryptographie?«

- **Bedrohungsszenarien**

  - Unbefugtes Einsehen von Nachrichten
  - Unbefugtes Ändern von Nachrichten
  - Fälschen von Absenderangaben

Crashkurs: »Wozu Kryptographie?«

- **Was können kryptographische Systeme leisten?**
  - Geheimhaltung → *Abhörsicherheit vor »unbefugten Dritten«*
  - Integrität → *Unversehrtheit der Nachricht garantiert*
  - Authentizität → *Identität von Sender und Empfänger prüfbar*


b
Normandy Beach
Normandy Beach
Encryption
Decryption
Alice
Bob
Qrupdqgb Ehdfk
Eve

Crashkurs: »Wozu Kryptographie?«

- **Dschungel der Fachbegriffe**
  - Verschlüsselung → *Nachrichten wiederruflich unlesbar machen*
  - Verschl.-Algorithmus → *Bes. Ablauf, der Nachrichten verschlüsselt*
  - Kryptographie → *Wissenschaft vom Verschlüsseln*
  - Kryptoanalyse → *Verschlüsselung brechen*

  - Steganographie → *Existenz von Nachrichten verbergen*

Wie funktioniert Verschlüsselung?

Wie funktioniert Verschlüsselung?

Definition

Verschlüsselung nennt man den Vorgang, bei dem ein **Klartext** mit Hilf eines **Verschlüsselungsverfahrens** (Algorithmus) in einen **Geheimtext** umgewandelt wird.

Als Parameter des **Verschlüsselungsverfahrens** werden ein oder mehrere **Schlüssel** verwendet. […]

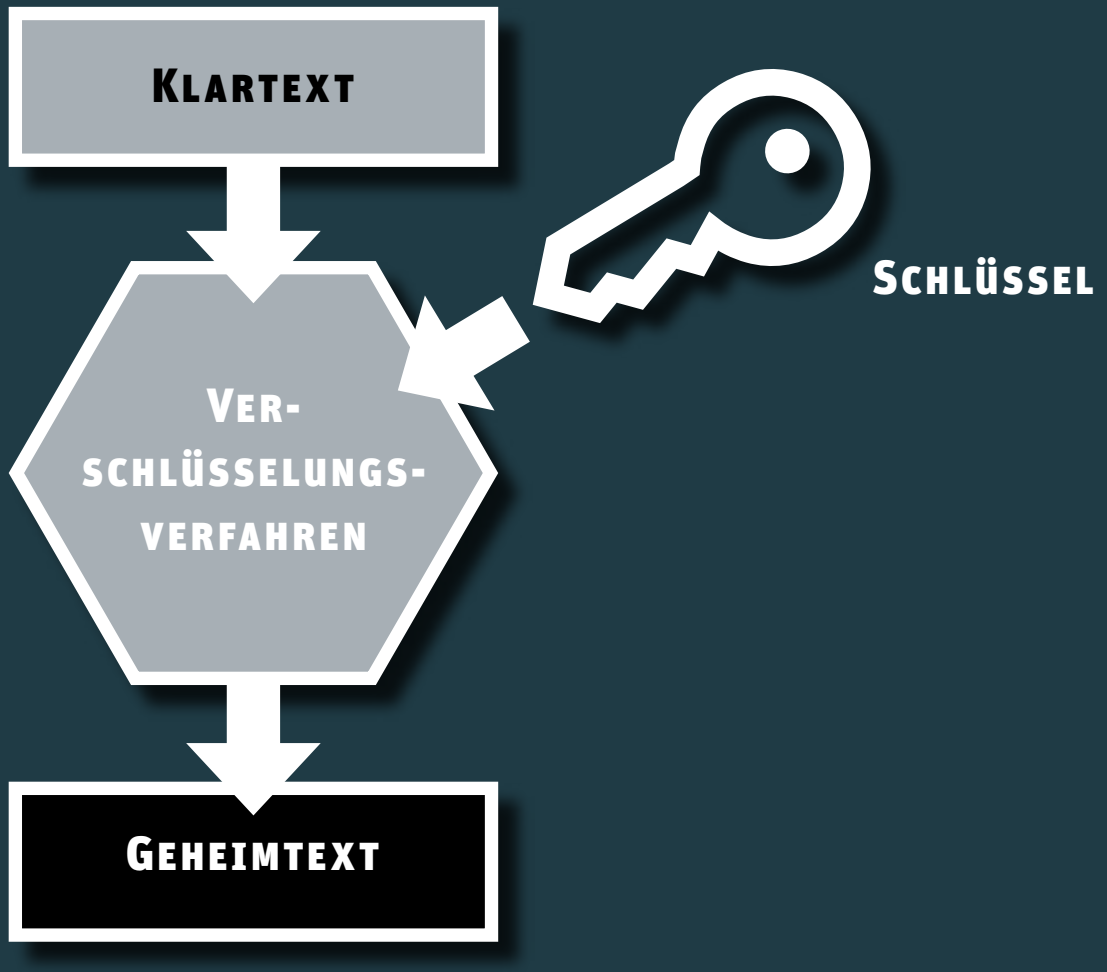
Den umgekehrten Vorgang, also die Verwandlung des **Geheimtextes** zurück in den Klartext, nennt man Entschlüsselung.

Wie funktioniert Verschlüsselung?

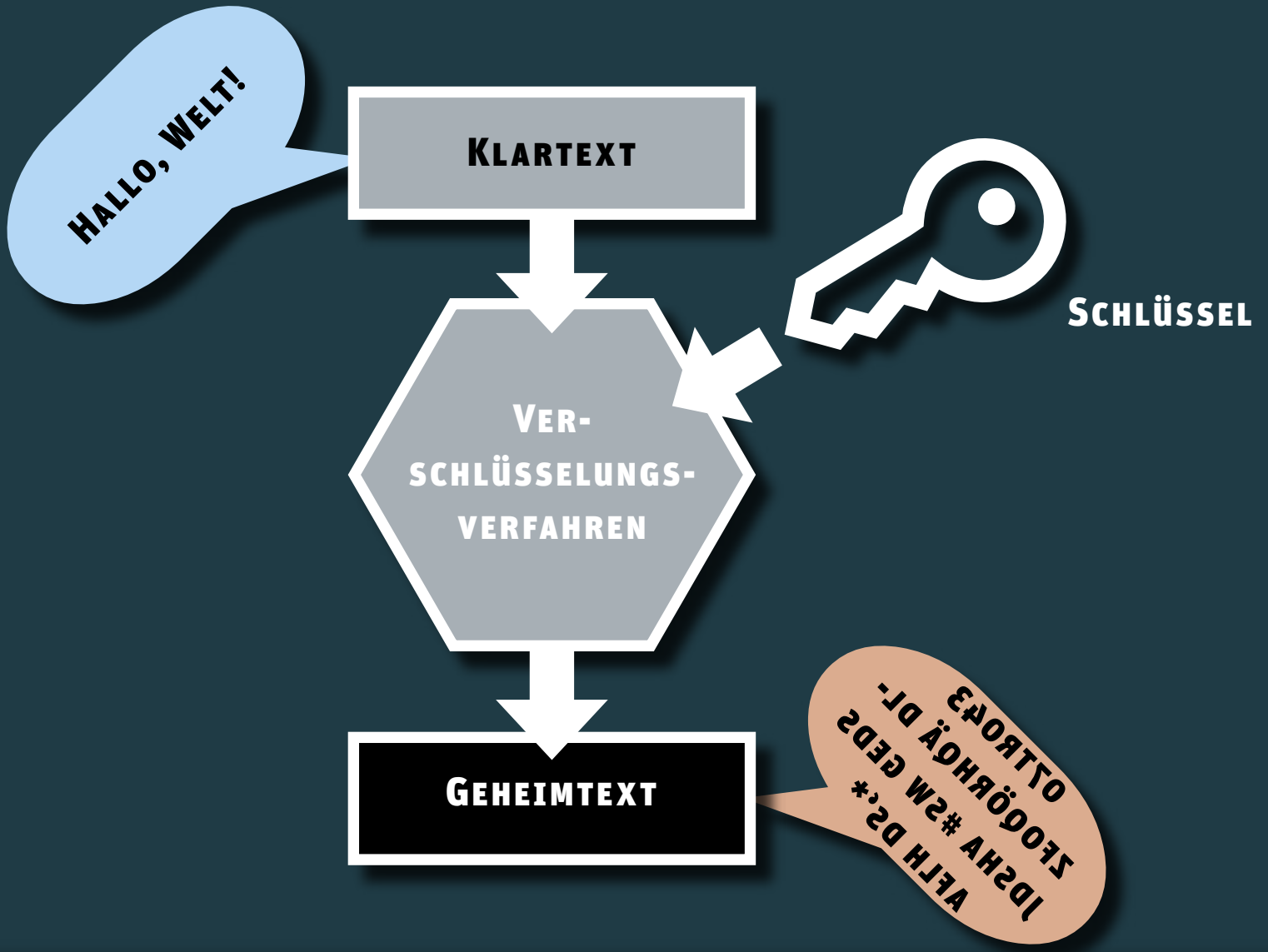
Wie funktioniert Verschlüsselung?

Wie funktioniert Verschlüsselung?

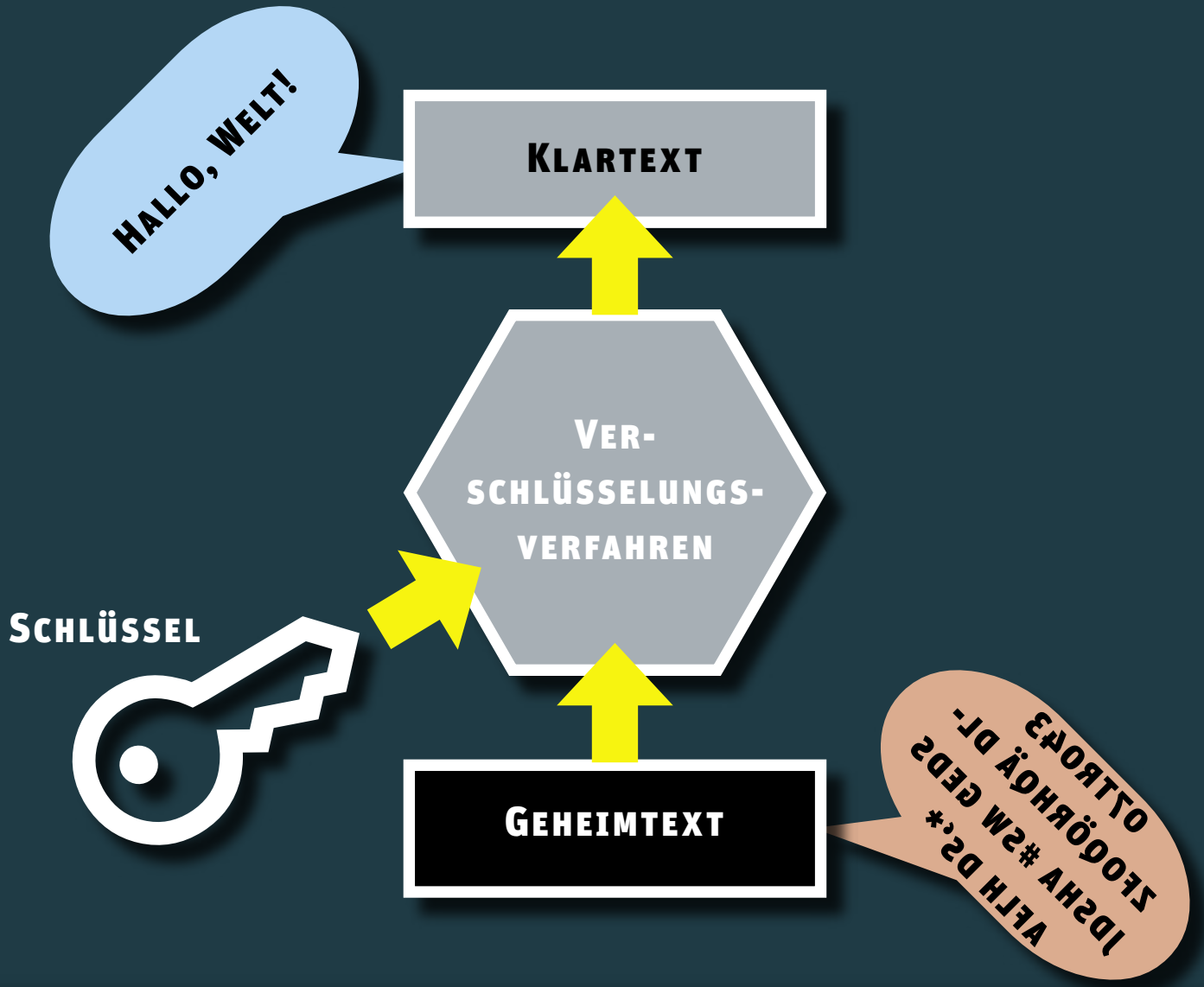
Wie funktioniert Verschlüsselung?



Wie funktioniert Verschlüsselung?



Wie funktioniert Entschlüsselung?



Wie funktioniert Verschlüsselung?

- **Verschlüsselungsoperationen**

- **Transposition & Substitution**

Wie funktioniert Verschlüsselung?

- **Verschlüsselungsoperationen**
  - **Transposition**
    - Bei einer Transposition werden die Zeichen untereinander vertauscht
    - LIES MICH → *HCIM SEIL*
    - LIES MICH → *SIEL HICM*

Wie funktioniert Verschlüsselung?

- **Verschlüsselungsoperationen**
  - **Substitution**
    - Bei einer Substitution werden Zeichen durch andere Zeichen ersetzt
    - A B C D E F → *C D E F G H*
    - A B C D E F → *1 2 3 4 5 6*

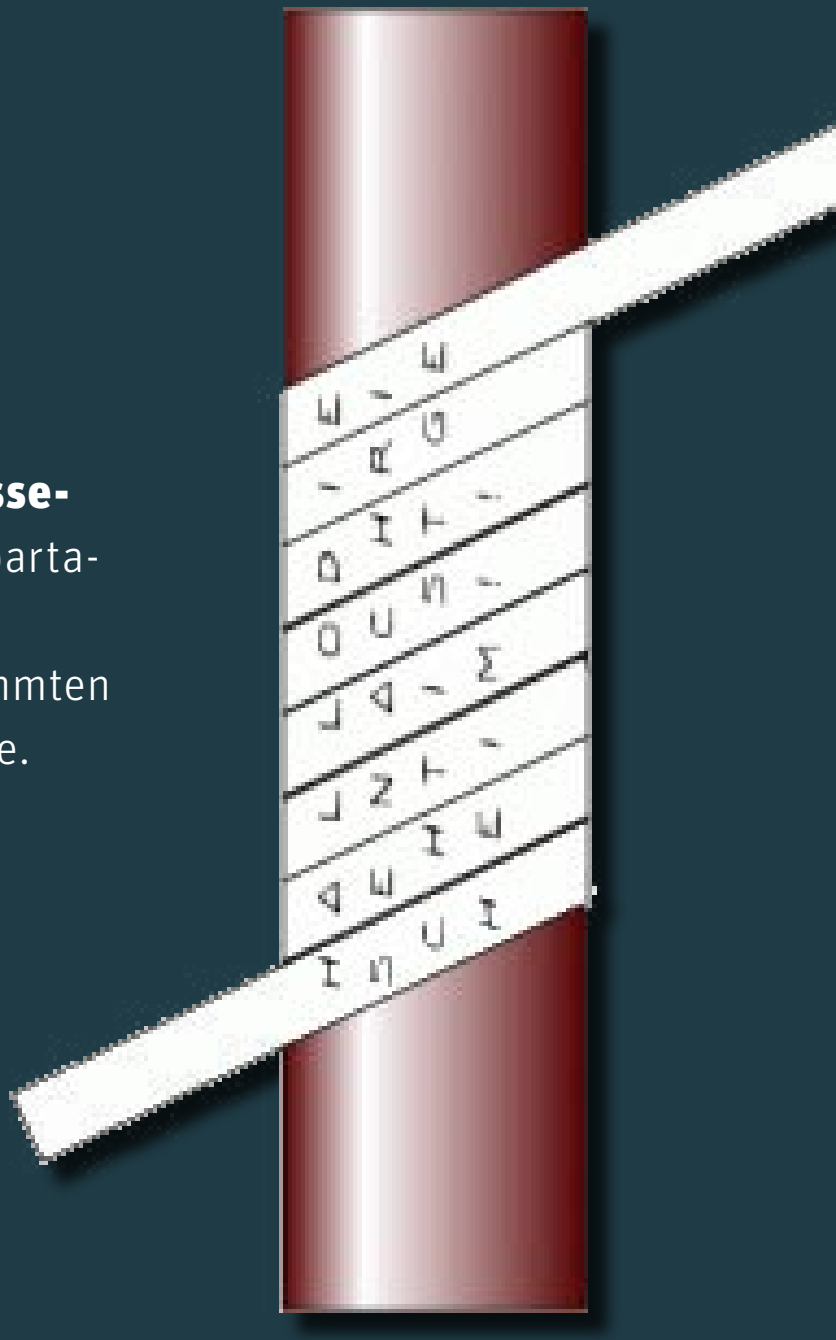
Wie funktioniert Verschlüsselung?

- **Verschlüsselungsoperationen**
  - **Transposition & Substitution**
  - … bilden die einzigen zwei Möglichkeiten für Verschlüsselungsverfahren
  - … können beliebig kombiniert werden

Historische Beispiele

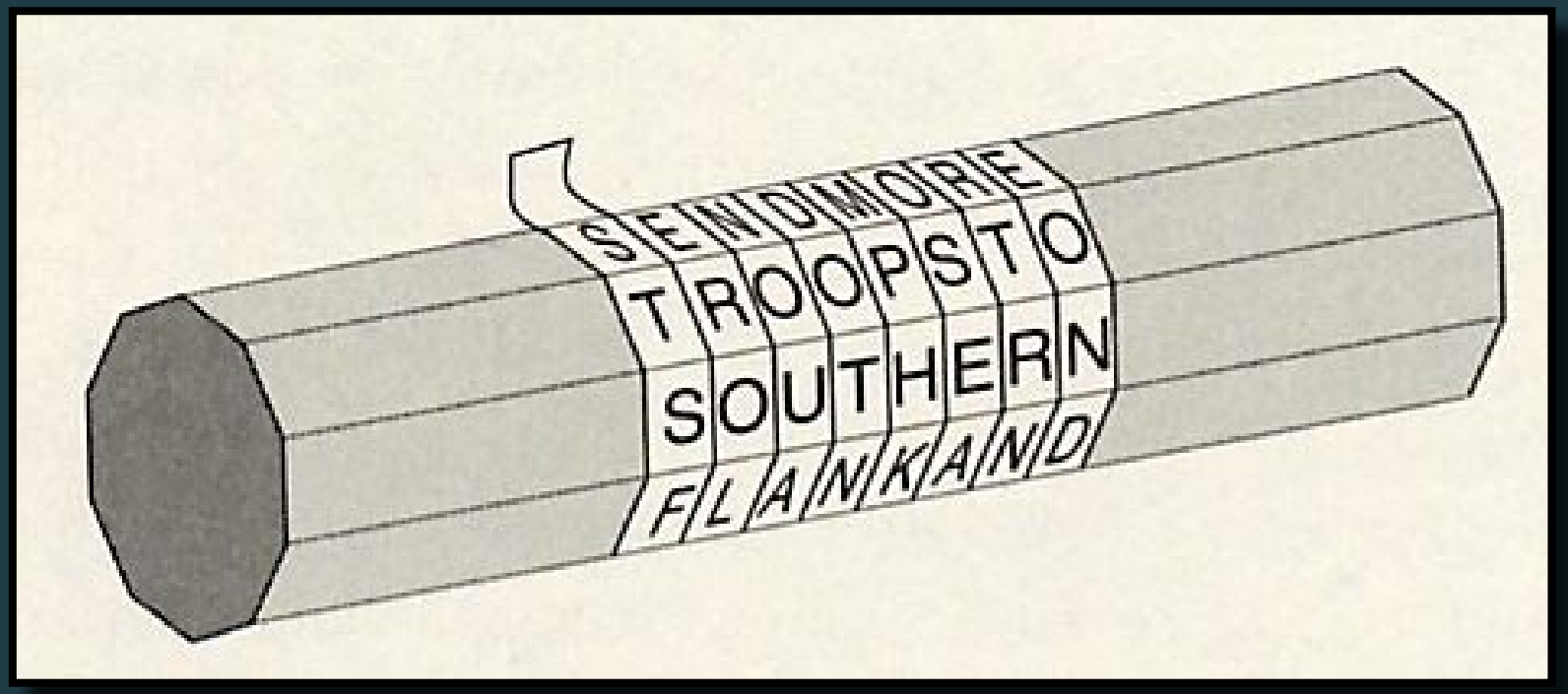
Skytale

Die älteste bekannte **Transpositionsverschlüsselung** wurde schon vor 2500 Jahren von den Spartanern zu militärischen Zwecken angewandt.
Als Schlüssel diente ein Stab mit einem bestimmten Durchmesser, der als Skytale bezeichnet wurde.



Historische Beispiele

Skytale

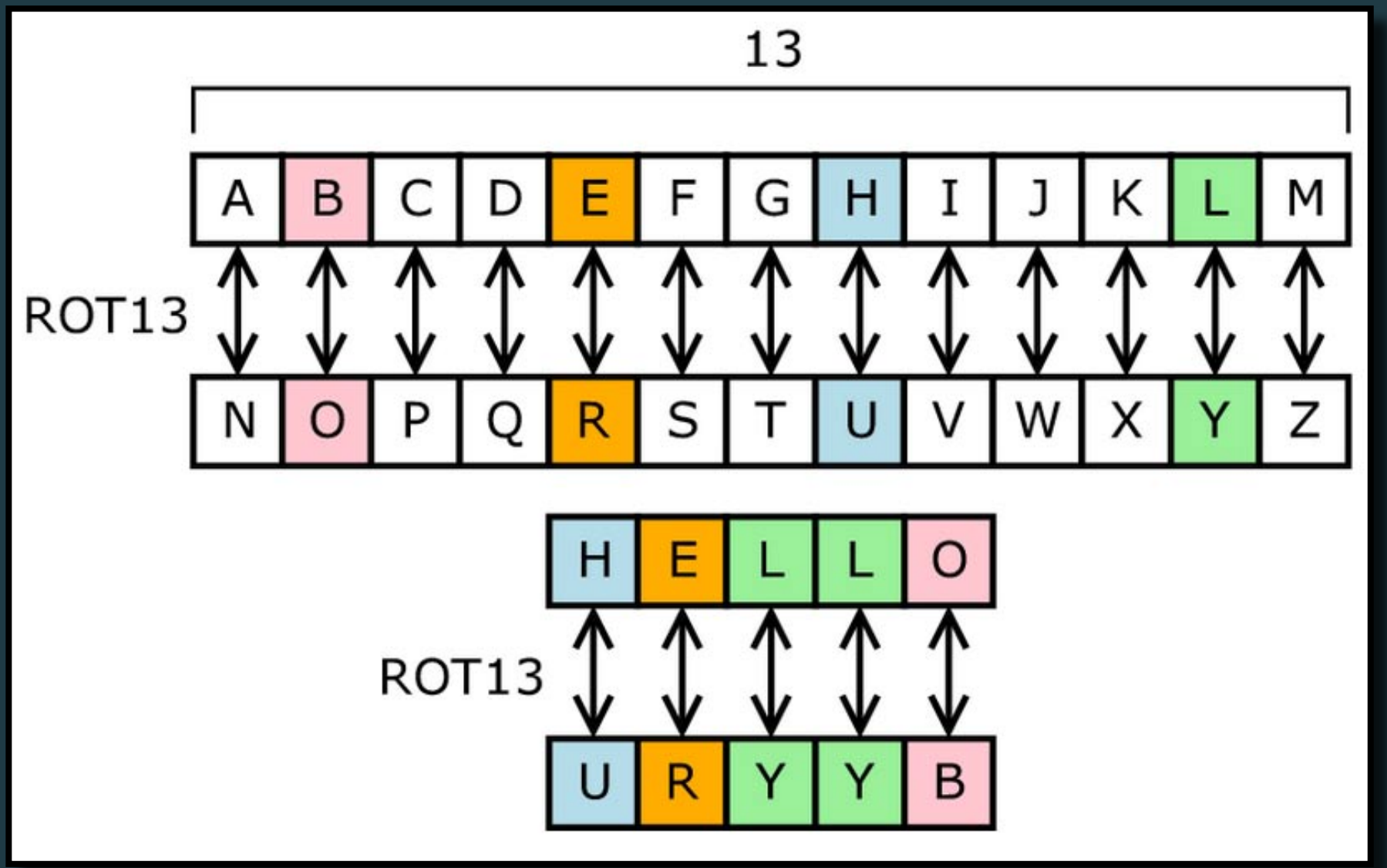


Historische Beispiele

Cäsar-Chiffre / ROT13

Ein sehr bekanntes Beispiel für **Substitutionsverschlüsselung** ist der sogenannte ROT13-Algorithmus, auch Cäsar-Chiffre genannt.
Dabei wird von einem lateinischen Alphabet mit 26 Buchstaben ausgegangen, welches um 13 Stellen verschoben (rotiert) wird.

Historische Beispiele



Uvfgbevfpur Orvfcvryr

Päfne-Puvsser / EBG13

Rva frue orxnaagrf Orvfcvry süe **Fhofgvghgvbafirefpuyüffryhat** vfg qre fbtranaagr EBG13-Nytbevguzhf, nhpu Päfne-Puvsser tranaag.
Qnorv jveq iba rvarz yngrvavfpura Nycunorg zvg 26 Ohpufgnora nhftrtnatra, jrypurf hz 13 Fgryyra irefpubora (ebgvreg) jveq.

Historische Beispiele

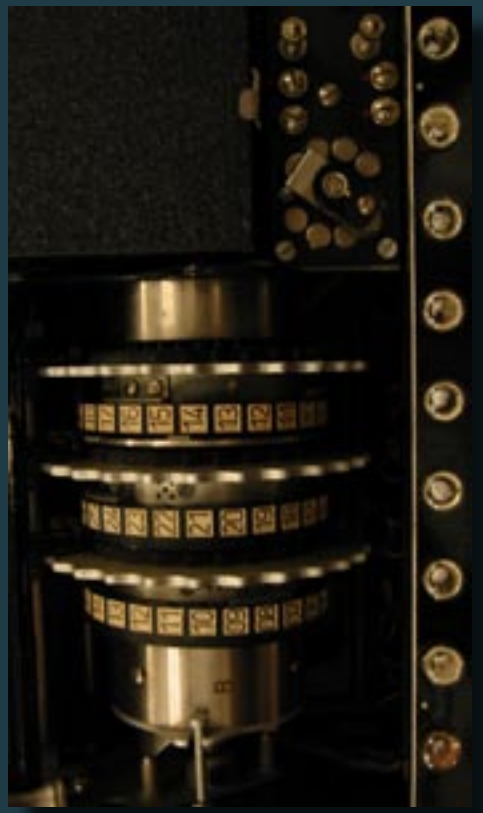
Enigma

Ein weiteres sehr bekanntes Beispiel für **Verschlüsselung** durch **Substitution** ist die deutsche Rotor-Verschlüsselungsmaschine Enigma, die sehr häufig im zweiten Weltkrieg von den Deutschen verwendet wurde.
Wichtigste Eigenschaft der Enigma ist die polyalphabetische Rotorverschlüsselung, welche die automatisierte Verwendung mehrerer Geheimalphabete ermöglicht. Ferner werden dabei für fast jeden einzelnen Klartext-Buchstaben eigene Schlüssel verwendet.

Historische Beispiele

Enigma

Das Herzstück der Enigma sind **drei Walzen und zwei Umkehrwalzen**, die man beliebig anordnen kann. Die Walzen verfügen über ein eigenes 26-Stelliges Geheimalphabet, wwelches sich über eine Ringeinstellung verschieben lässt. Alle Walzen sind untereinander über unterschiedlich einstellbare Steckverbindungen gekoppelt.



Historische Beispiele

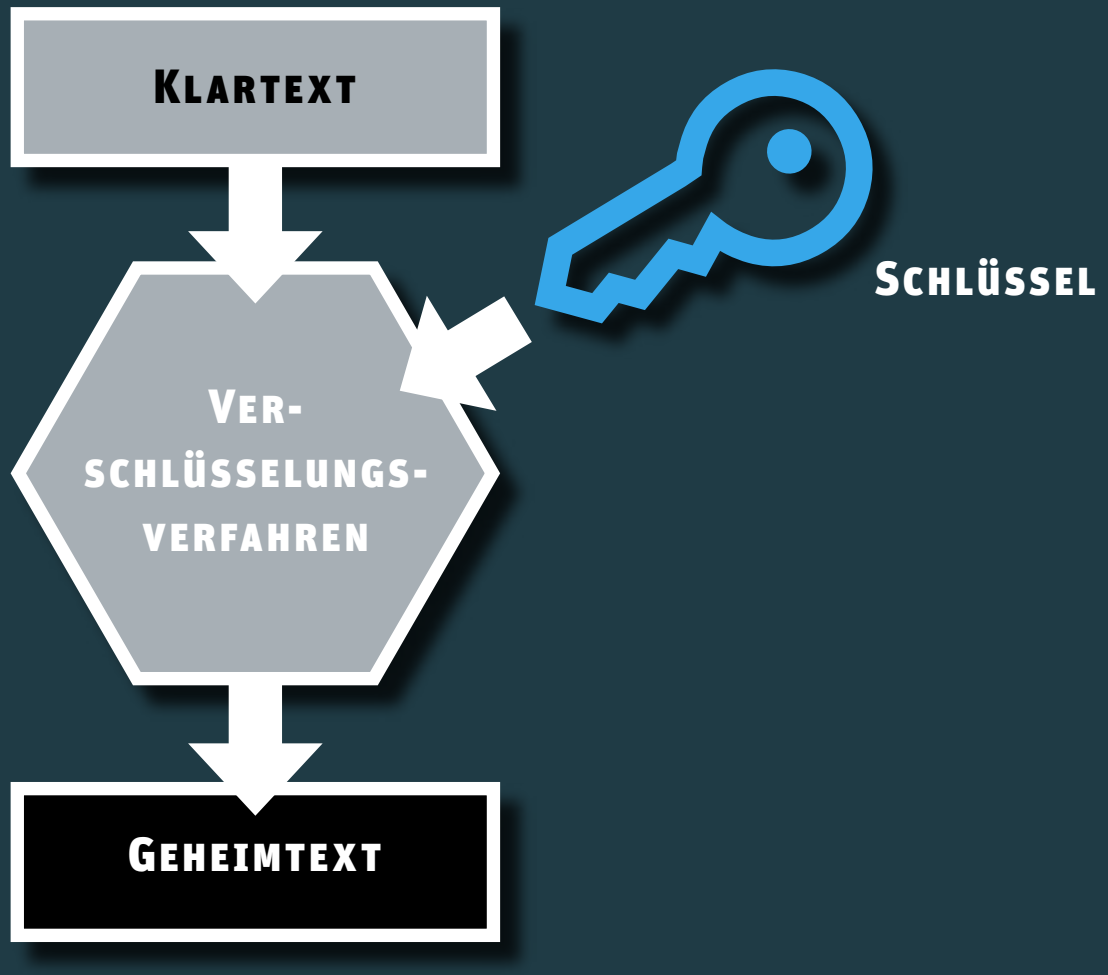
- **Enigma**
  - Die Enigma bietet vier Parameter zur Einstellung:
    1. 120 verschiedene Walzenlagen
    2. 676 Einstellungen der Ringe
    3. 17.576 Grundstellungen der Walzen
    4. 150.738.274.937.250 (~ 150 Bio.) Steckerverbindungen aller Walzen
  - Schlüsselraum circa $2 \cdot 10^{23}$ verschiedenen Möglichkeiten (~ 77 Bit)
  - Durch Sicherheits-Schwächen aber nur ca. 2 Mio. benutzbare Schlüssel

2. Moderne Anwendung

Symmetrisch, asymmetrisch?

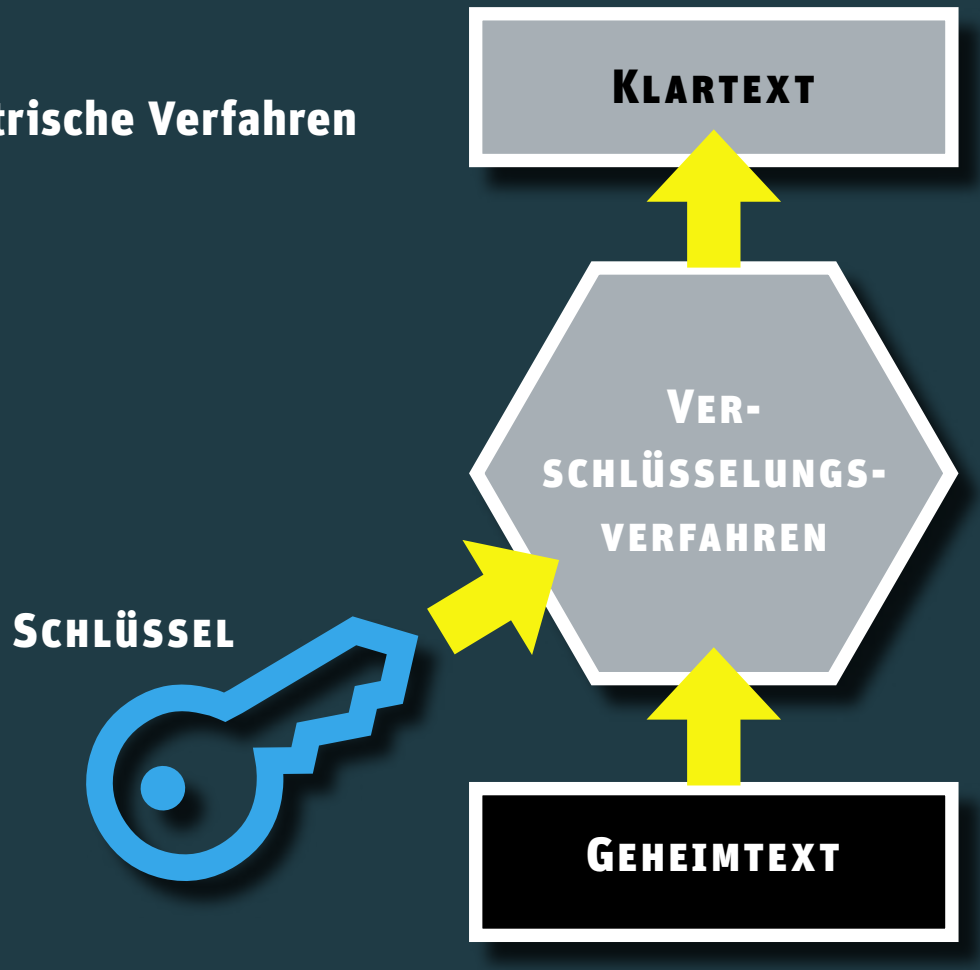
Symmetrisch, asymmetrisch?

- Symmetrische Verfahren



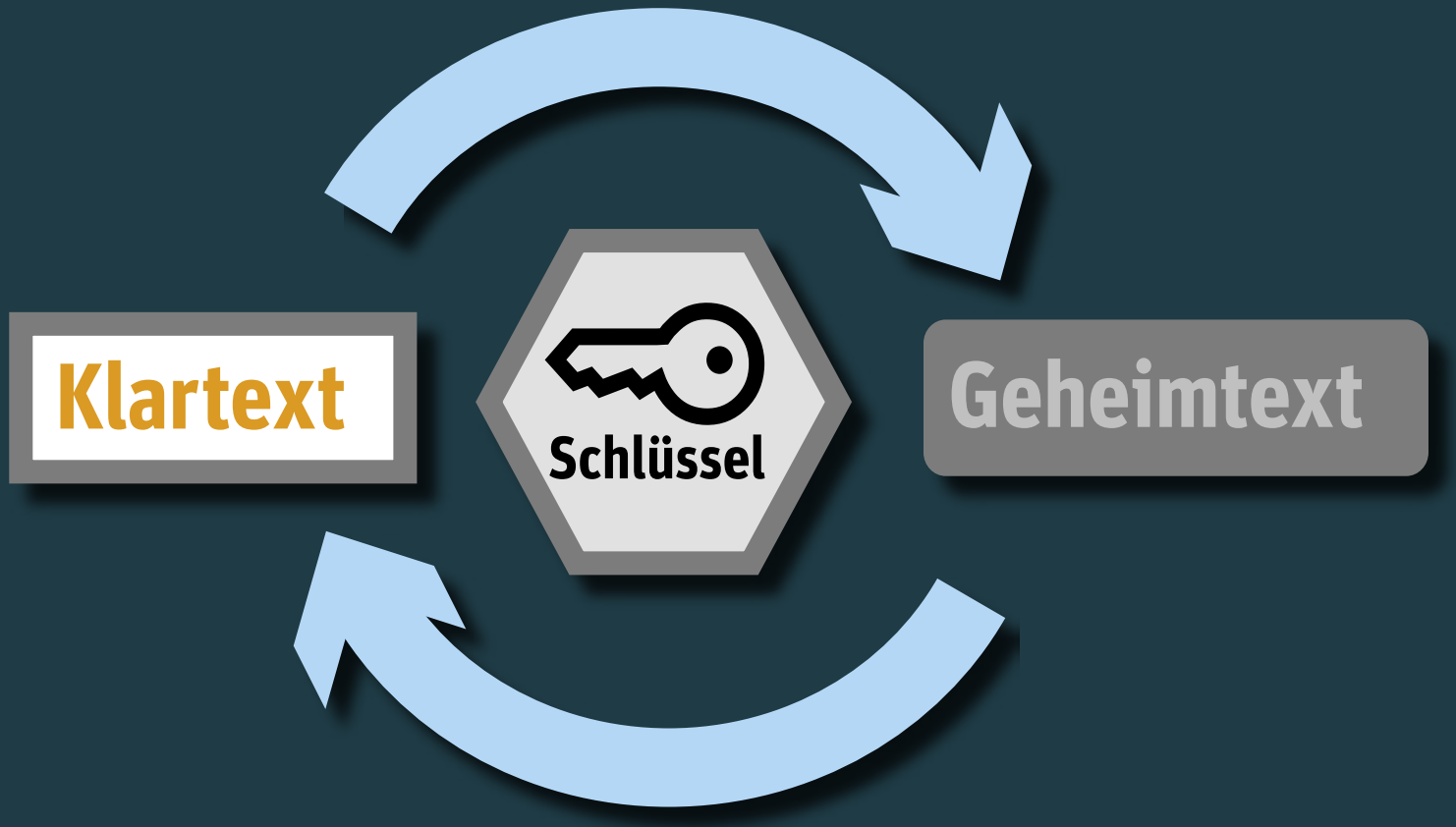
Symmetrisch, asymmetrisch?

- Symmetrische Verfahren



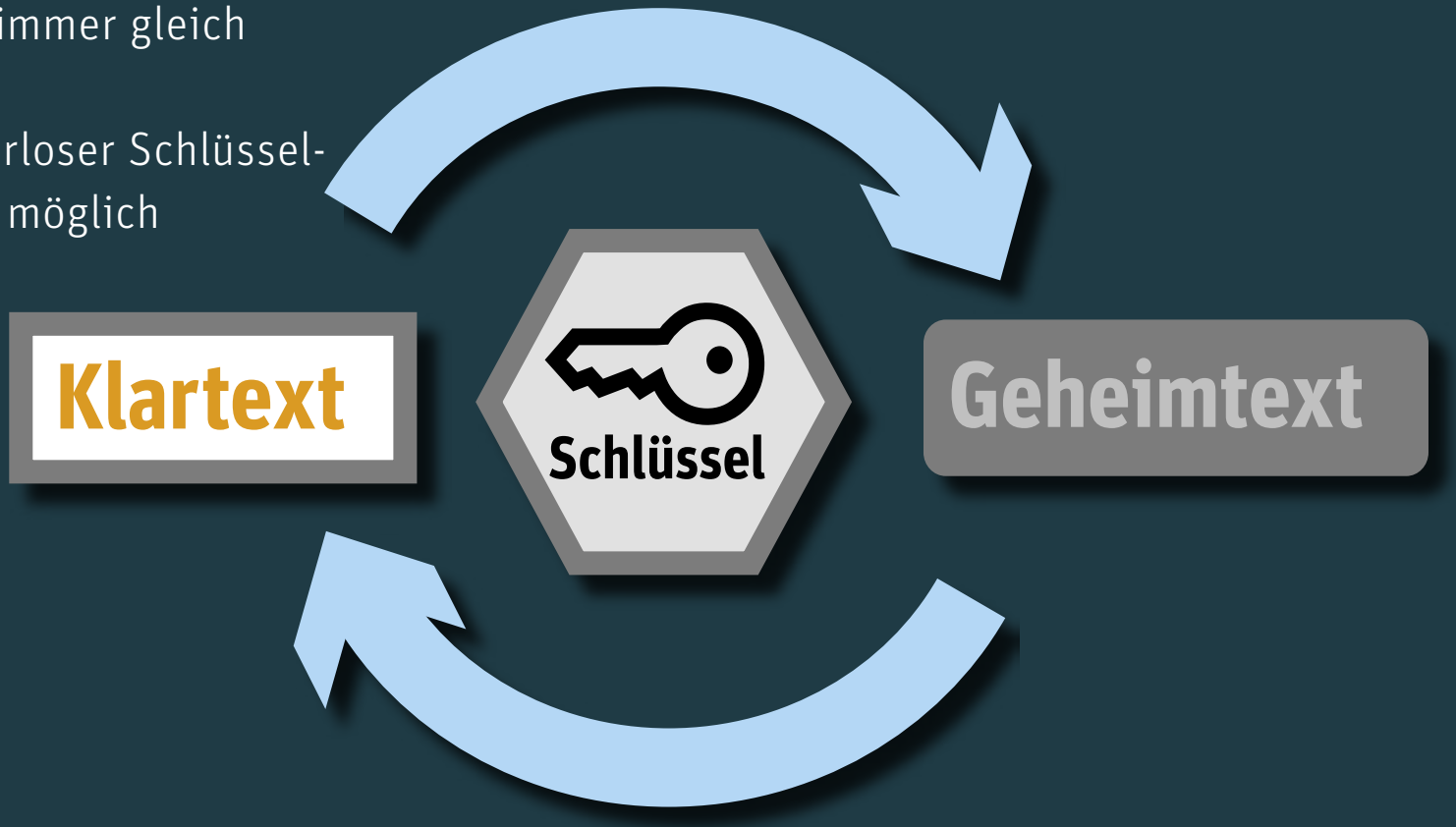
Symmetrisch, asymmetrisch?

- **Symmetrische Verfahren**



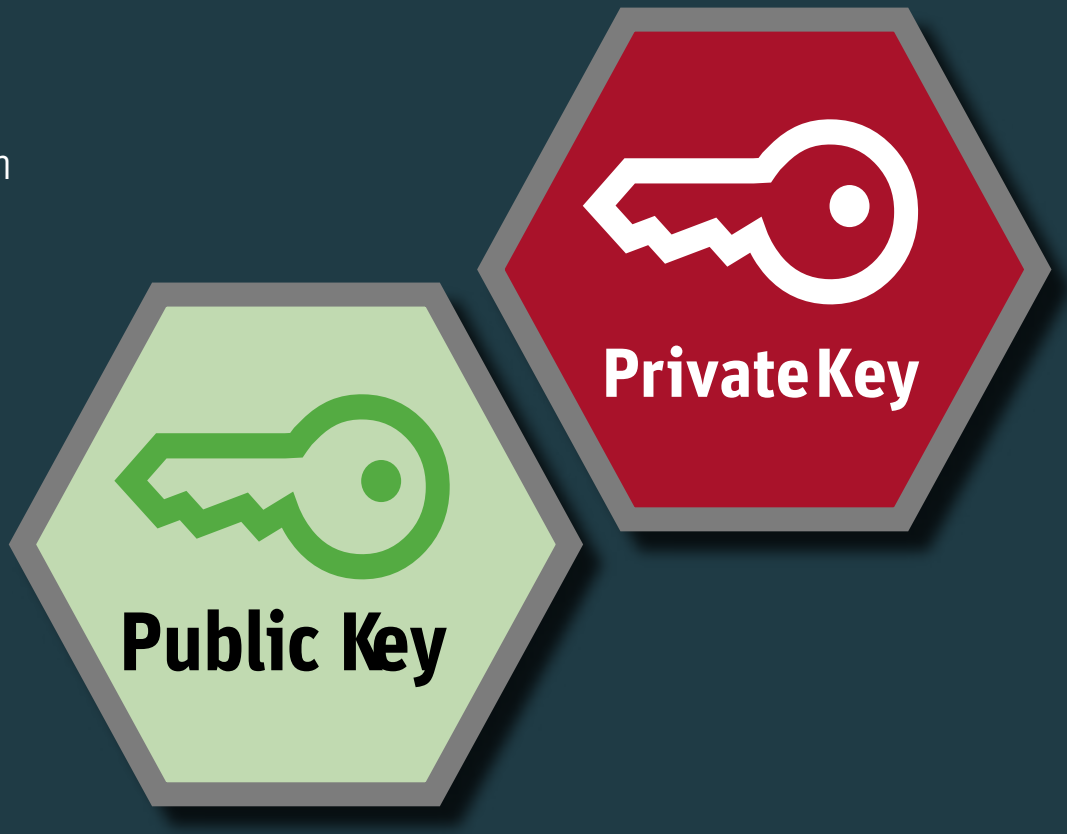
Symmetrisch, asymmetrisch?

- **Symmetrische Verfahren**
- Schlüssel immer gleich
- Kein gefahrloser Schlüsselaustausch möglich



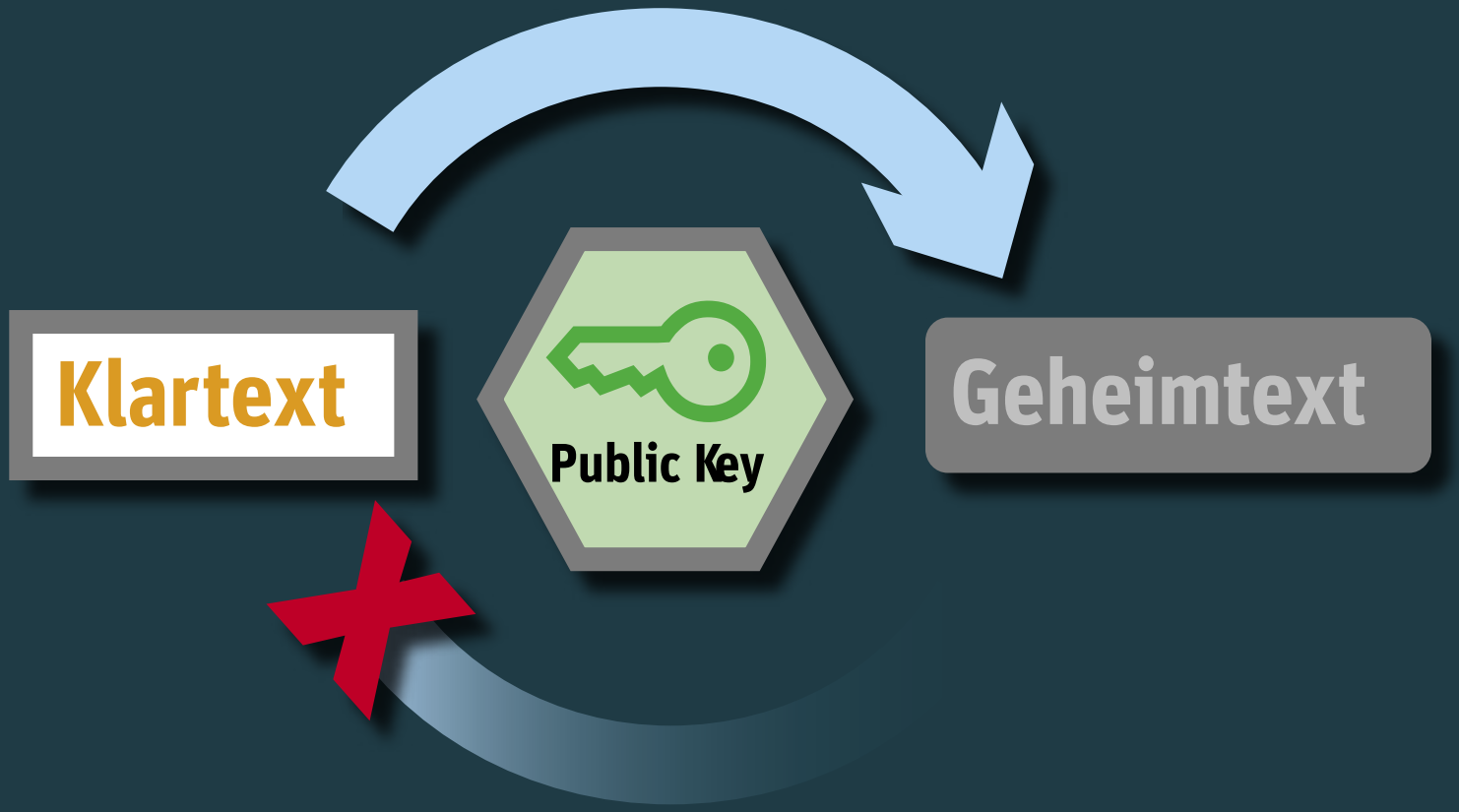
Symmetrisch, asymmetrisch?

- **Asymmetrische Verfahren:**
  - Geheimschlüssel wird durch **Schlüsselpaar** ersetzt
  - Private Key ist nur für den Besitzer zugänglich
  - Public Key ist für jeden Teilnehmer zugänglich



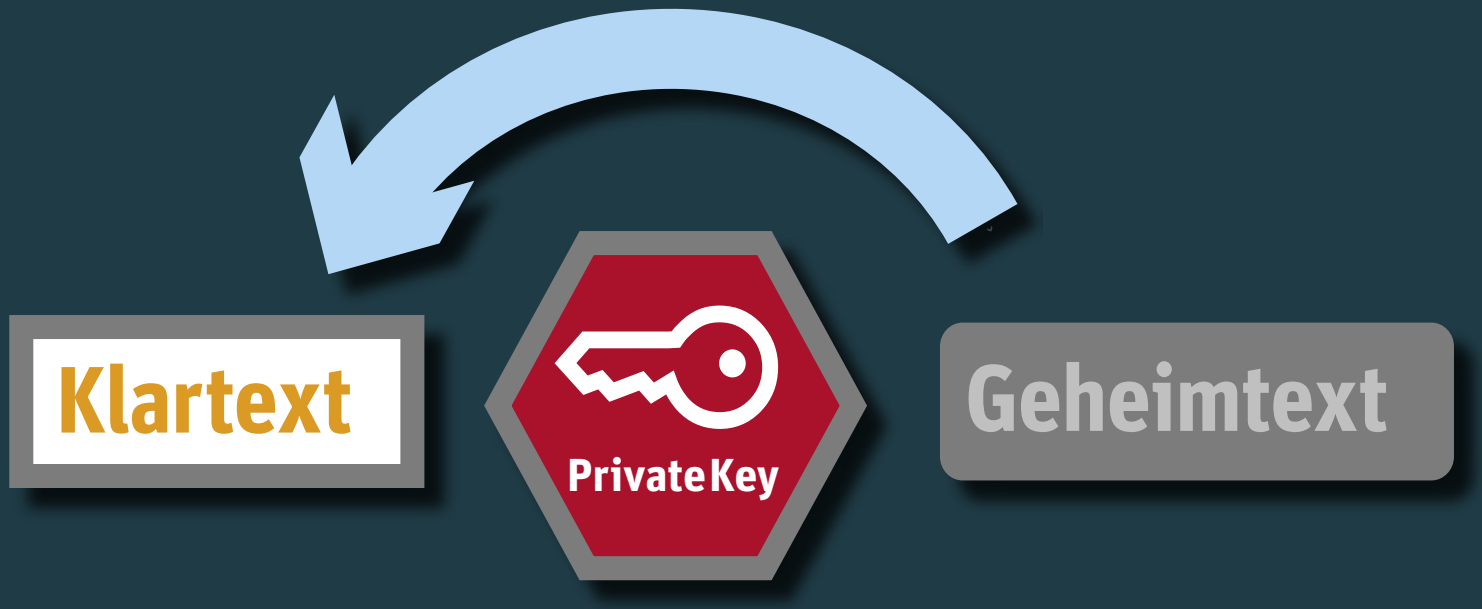
Symmetrisch, asymmetrisch?

- **Asymmetrische Verfahren:**
  Public Key



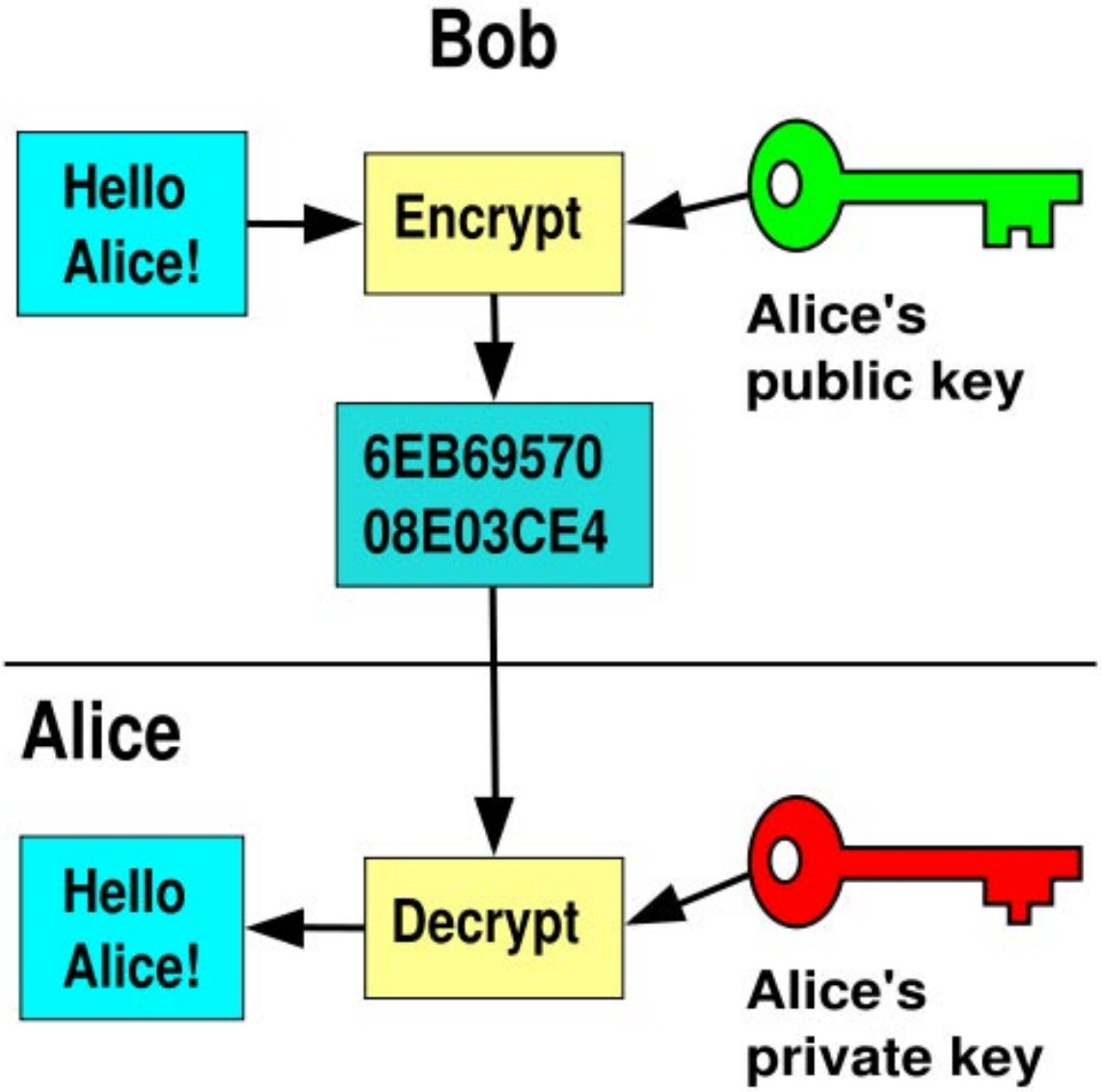
Symmetrisch, asymmetrisch?

- **Asymmetrische Verfahren:**
  Private Key



Symmetrisch, asymmetrisch?

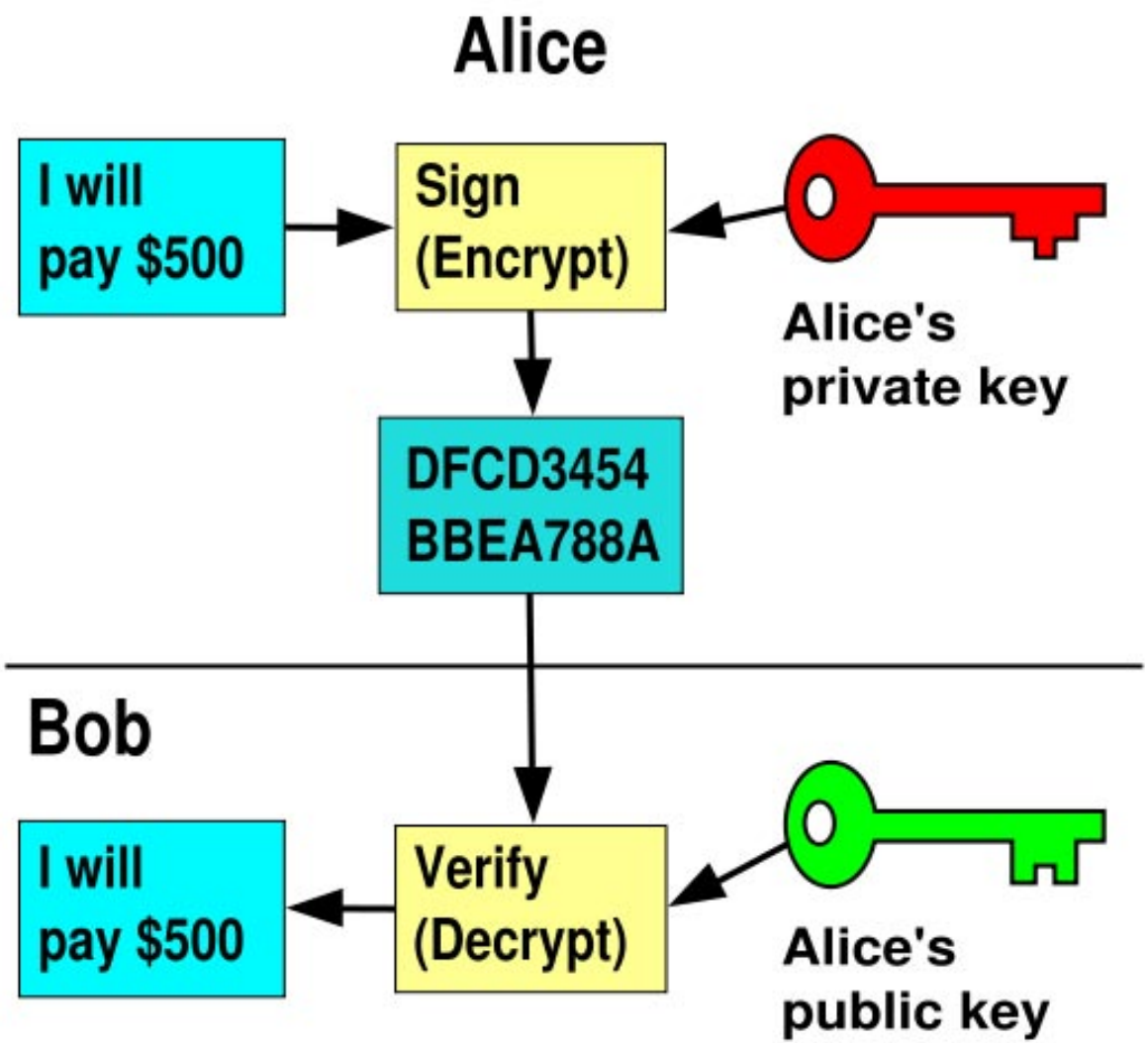
- **Asymmetrische Verfahren**
  - Gedankliches Konzept
    - Public Key verschlüsselt Nachrichten
    - Private Key entschlüsselt Nachrichten
    - Public Key kann mit dem Public Key verschlüsselte Nachrichten **nicht** entschlüsseln (»Asymmetrie«)
    - »Gefährlicher Schlüsselaustausch« entfällt (Public Key kann durch unsichere Kanäle verbreitet werden)

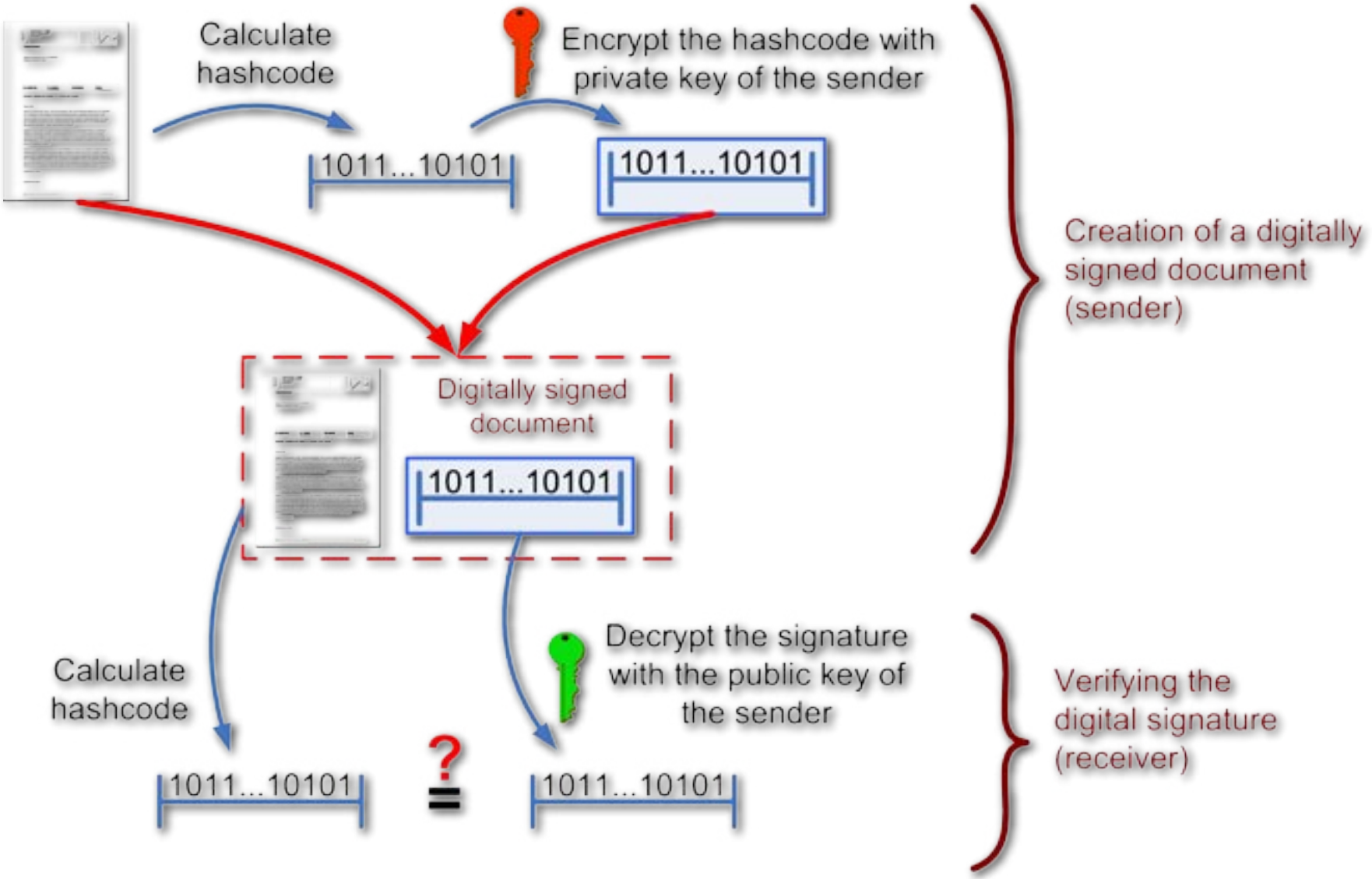

Bob
Hello Alice!
Encrypt
Alice's public key
6EB69570 08E03CE4
Alice
Hello Alice!
Decrypt
Alice's private key

Elektronische Signatur

Elektronische Signatur

- Mit **Schlüsselpaaren** kann nachgewiesen werden, dass eine Person ein bestimmtes Dokument digital signiert hat
- Durch einen speziellen Signier-Algorithmus kann der Besitzer eines privaten Schlüssels für ein bestimmtes Dokument eine digitale Signatur erstellen lassen
- Die generierte digitale Signatur ist ausschließlich für das eine signierte Dokument gültig. Möchte man ein anderes Dokument signieren, muss der Vorgang wiederholt werden.
- Anschließend kann über den öffentlichen Schlüssel der Person nachgewiesen werden, ob die Signatur authentisch ist oder nicht


Alice
I will pay $500
Sign (Encrypt)
Alice's private key
DFCD3454 BBEA788A
Bob
I will pay $500
Verify (Decrypt)
Alice's public key


Calculate hashcode
Encrypt the hashcode with private key of the sender
1011...10101
1011...10101
Creation of a digitally signed document (sender)
Digitally signed document
1011...10101
Calculate hashcode
Decrypt the signature with the public key of the sender
Verifying the digital signature (receiver)
1011...10101
?
=
1011...10101

Zertifikate

Zertifikate

- Zertifkate dienen zur Sicherstellung der Echtheit von öffentlichen Schlüsseln und weren von sog. Zertifizierungsstellen ausgestellt
- Ein Zertifikat enthält Informationen über den Namen des Inhabers, dessen öffentlichen Schlüssel, eine Seriennummer, eine Gültigkeitsdauer und den Namen der Zertifizierungsstelle
- Um die Echtheit des Zertifikates zu garantieren, wird dem Zertifikat eine digitale Signatur einer vertrauenswürdigen Organisation oder Instanz (z. B. eine Behörde) aufgeprägt. Durch dessen Signatur kann die Integrität und Echtheit des Zertifikates nachgewiesen werden.
- In Deutschland übernimmt die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen die Rolle der höchsten Zertifizierungsinstanz

Hybride Systeme

Hybride Systeme

- Hybride Systeme arbeiten gemischt mit asymmetrischen und symmetrischen Verschlüsselungsverfahren, was einen großen Geschwindigkeitsvoteil bringt
- Ein typisches Anwendungsbeispiel ist der Austausch des **»Session-Keys«** bei sicherheitskritischen Internet-Anwendungen (z. B. Onlinebanking)
  - Hierbei einigen sich beide Gegenstellen zuerst anhand von Zertifikaten und asymmetrischer Kryptographie auf einen Sitzungsschlüssel, welcher dann für eine symmetrische (und ressourcensparende) Verschlüsselung genutzt wird.
  - Bei vertrauenswürdigen Zertifikaten eine sichere Methode um den Geheimschlüssel für symmetrische Kryptographie zu übertragen

Hybride Systeme

Wie wird ein **Session-Key** generiert? (stark vereinfacht)

1. Dienstleister (Server) und Kunde (Client) bauen eine Verbindung auf
2. Server sendet seinen Public Key und ein Zertifikat, das die Echtheit des Public Keys bestätigt, an den Client
3. Client überprüft Zertifikat
4. Wenn Zertifikat vertrauenswürdig, generiert Client einen symmetrischen Schlüssel, welcher asymmetrisch mit dem Public Key des Servers verschlüsselt wird
5. Server erhält den Schlüssel und leitet eine symmetrisch verschlüsselte Verbindung zwischen sich und Client ein

ENDE.

3. Fragen, Diskussion

Danke für eure Aufmerksamkeit