Leibniz Gemeinschaft

IPN
Leibniz-Institut für die Pädagogik der Naturwissenschaften und Mathematik

Rückblick & Zusammenfassung

Die bisherigen Verfahren

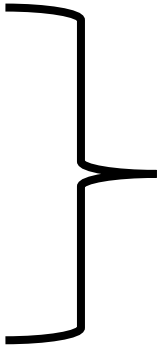
- Cäsar

- Vigenère

- Skytale

Die bisherigen Verfahren

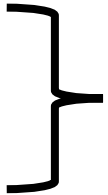
- Cäsar
- Vigenère
- Skytale



Austauschen von Buchstaben

Die bisherigen Verfahren

- Cäsar
- Vigenère
- Skytale



Vertauschen von Buchstaben

Die bisherigen Verfahren

- Austauschen von Buchstaben = „**Substitution**“
- Vertauschen von Buchstaben = „**Permutation**“

Sicherheit der Verfahren

- Cäsar 
- Vigenère 
- Skytale 

Sicherheit der Verfahren

- „Angriffe“:
  - Alle Schlüssel ausprobieren (**Brute-Force**)
  - Häufigkeitsanalyse
- **Häufigkeitsanalyse**: Wir analysieren die Chiffre.

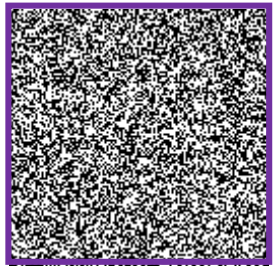
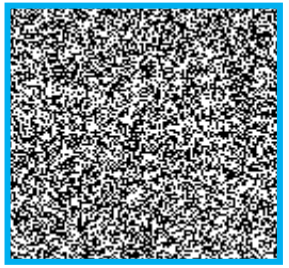
Sicherheit der Verfahren

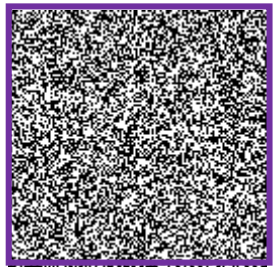
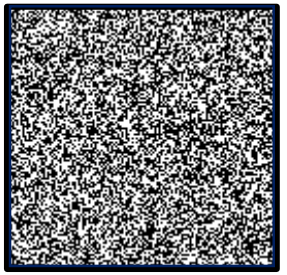
- Bestes Verfahren: Vigenère
- Brute-Force: dauert zu lange bei langen Schlüsselworten
- Häufigkeitsanalyse: nicht möglich, wenn Schlüssel lang ist, im Verhältnis zur Nachricht!

Probleme bei Vigenère?

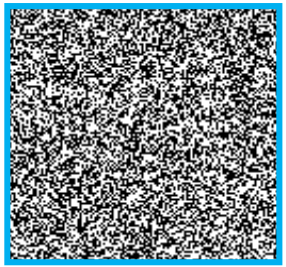
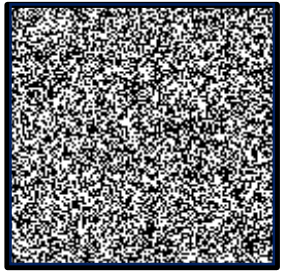
Der Schlüssel kann immer nur einmal verwendet werden.

Gleichen Schlüssel mehrmals verwenden

+

=



+

=


Probleme bei Vigenère?


Probleme bei Vigenère?

- Schlüssel: 5
- Position Buchstabe 1: 20
- Position Buchstabe 2: 17
- Position Chiffre 1: 25
- Position Chiffre 2: 22

Probleme bei Vigenère?

- Position Chiffre 1: 25
- Position Chiffre 2: 22

- Differenz von Chiffre 1 und 2: (`schiebe_zurück()`)
  25 - 22 = 3

Probleme bei Vigenère?

- Position Buchstabe 1: 20
- Position Buchstabe 2: 17

- Differenz von Buchstabe 1 und 2:

  20 – 17 = 3

Probleme bei Vigenère?

- $25 = 20 + 5$
- $22 = 17 + 5$

- $25 - 22 = (20 + 5) - (17 + 5) = 20 - 17 + 5 - 5 = 20 - 17$

Probleme bei Vigenère?

- Differenz von Chiffre 1 und 2 = Differenz von Buchstabe 1 und 2
- Die Chiffre liefert Informationen über den Klartext, ohne dass wir diesen kennen
- Diese können statistisch analysiert werden

Wann ist das Vigenère-Verfahren sicher?

- Schlüssel so lang wie die Nachricht
- Schlüssel wird nur einmal verwendet
- ‚One-Time-Pad‘
- **Aber**: Wenn man den Schlüssel sicher tauschen kann, dann auch die Nachricht!

Lösung unserer Probleme

- **Ziel**: einen Schlüssel mehrfach benutzen
- **Lösung**:
  - Teile Nachricht in gleich lange Blöcke auf
  - Benutzen besondere Verschlüsselung: **Blockchiffre**
  - Ein Nachrichten-Block wird mit dem vorherigen Chiffre-Block verschlüsselt

Beispiel für Blockchiffren

- Verwendung in (fast) allen modernen Verschlüsselungen
- Am weitesten verbreitet: **AES**, (DES)
- Feste Nachrichten-/ und Schlüssellänge

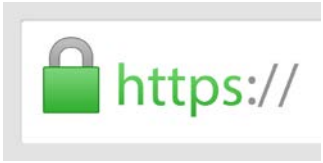
AES

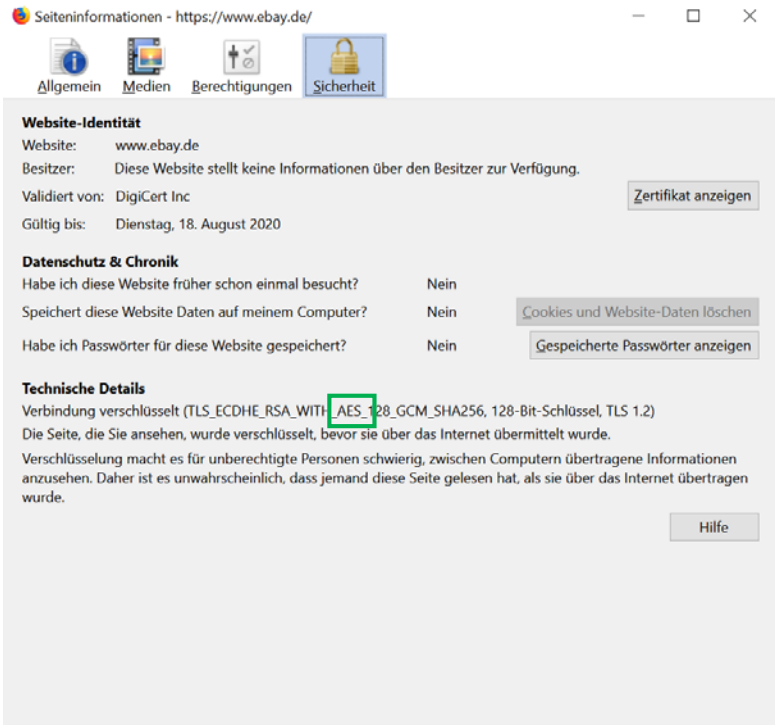
Substitutions-Permutations-Netzwerk

- W-Lan
- WhatsApp
- Skype
- E-Mail (PGP)

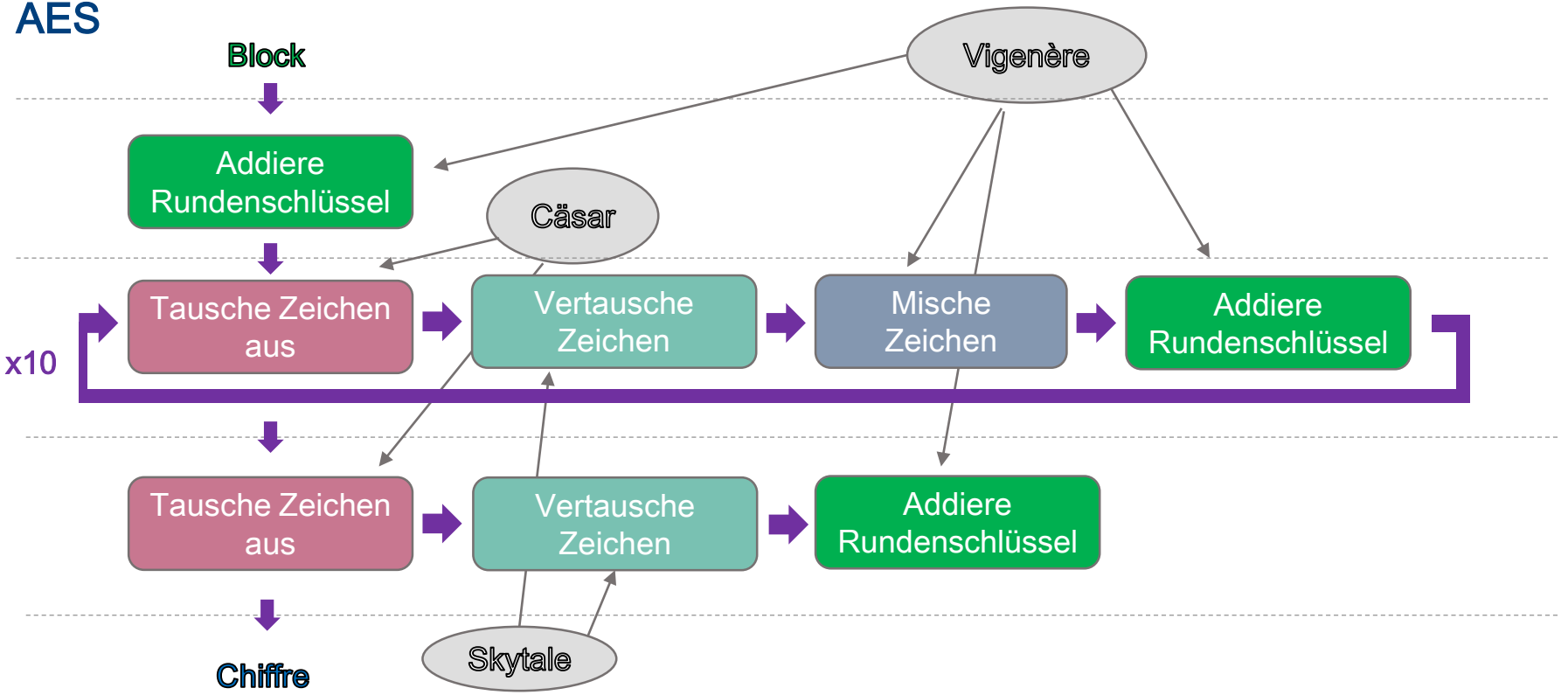
https://

Beispiel Browser

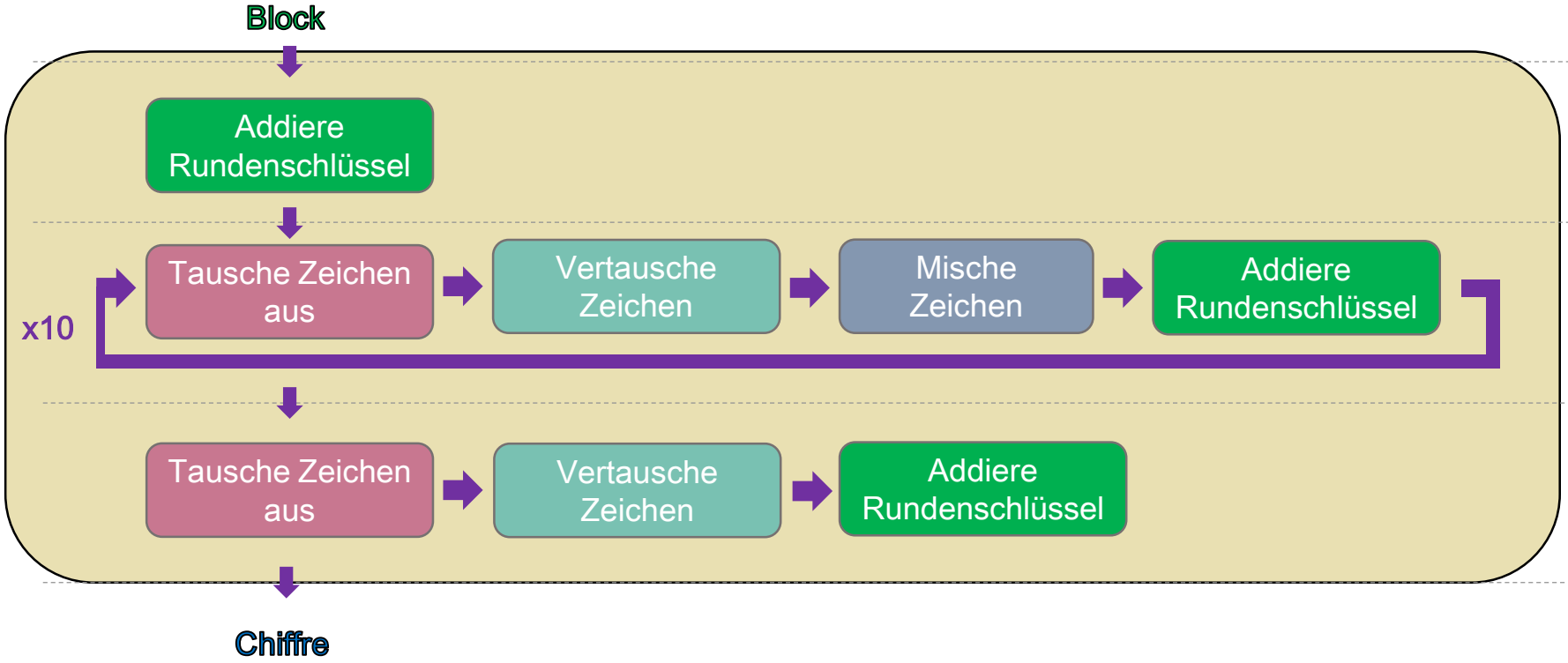




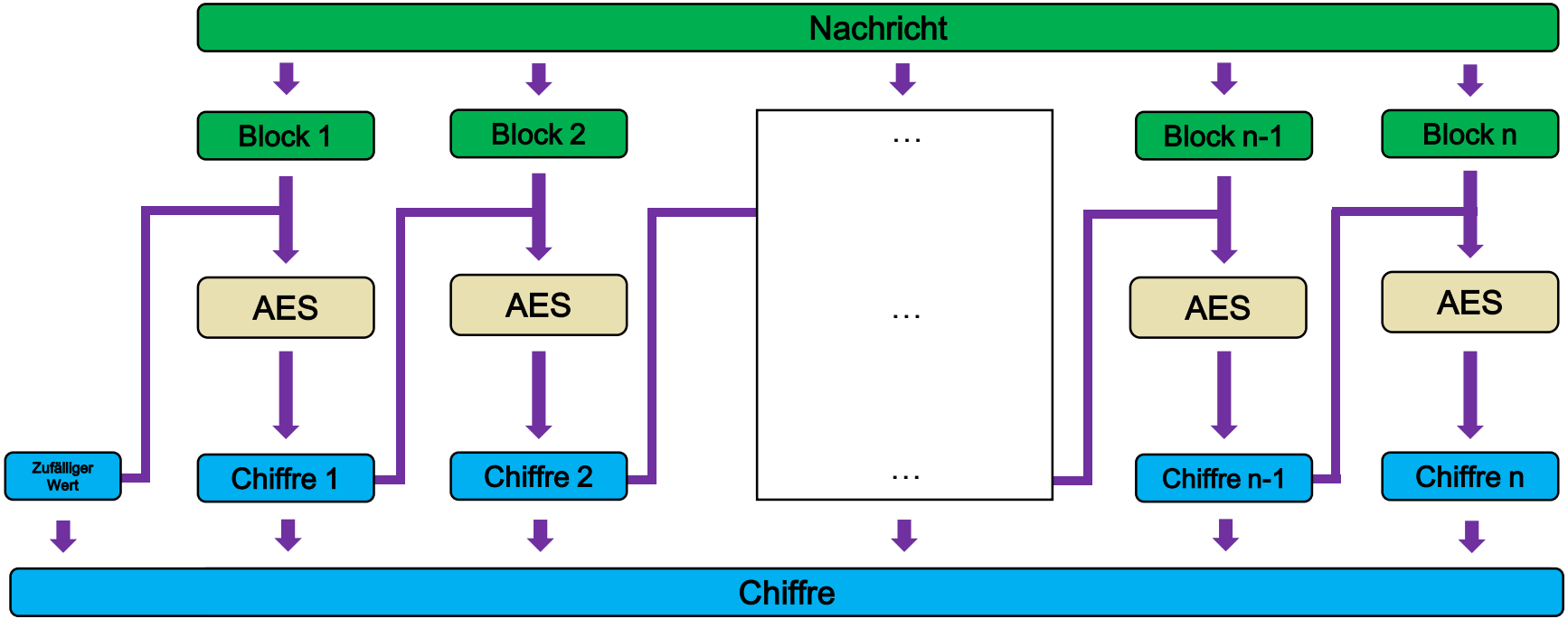
AES


Block
Vigenère
Addiere Rundenschlüssel
Cäsar
Tausche Zeichen aus
Vertausche Zeichen
Mische Zeichen
Addiere Rundenschlüssel
x10
Tausche Zeichen aus
Vertausche Zeichen
Addiere Rundenschlüssel
Skytale
Chiffre

AES


Block
Addiere Rundenschlüssel
x10
Tausche Zeichen aus
Vertausche Zeichen
Mische Zeichen
Addiere Rundenschlüssel
Tausche Zeichen aus
Vertausche Zeichen
Addiere Rundenschlüssel
Chiffre

AES


Nachricht
Block 1
Block 2
…
Block n-1
Block n
AES
AES
…
AES
AES
Zufälliger Wert
Chiffre 1
Chiffre 2
…
Chiffre n-1
Chiffre n
Chiffre

Schüsseltausch-Problem

- Alle bisherigen Verfahren: gemeinsamer Schlüssel benötigt
- Wenn wir den Schlüssel sicher tauschen können, brauchen wir ihn nicht!

Schüsseltausch-Problem

- Lösung:
  - Verfahren, das keinen Schlüsseltausch braucht
  - Verfahren, das mit einem Schlüssel verschlüsselt, mit einem anderen entschlüsselt
  - Verfahren, bei dem nur Teilinformationen übermittelt werden und Sender und Empfänger durch geheime Informationen ergänzen

Zusammenfassung

- Cäsar / Vigenère : Substitutionsverfahren
- Skytale : Permutationsverfahren
- Alle : Schlüssel muss zwischen Sender und Empfänger übertragen werden & Schlüssel nur einmal verwendbar

- Blockcodes machen Schlüssel mehrfach verwendbar
- Schlüsseltauschproblem bleibt bestehen → weiteres / anderes Verfahren nutzen

Hast du eine Frage, einen Fehler gefunden oder sonstige Anregungen? Melde dich bei uns!

Unter karrasch@leibniz-ipn.de oder info@panama-project.eu