IS ZA

Kryptologie:

* Kunst und Wissenschaft Nachrichten sicher zu behalten => von Kryptographen praktiziert

Kryptoanalyse:

* Kunst und Wissenschaft Cipertexte zu knacken => Kryptoanalysten

Ziele der Kryptographie:

* Vertraulichkeit
  + Eine Nachricht kann nur von den vertrauten Parteien gelesen werden (Sender und Empfänger)
* Authentizierung
  + Empfänger kann die Herkunft bestätigen. Angreifer kann nicht als jemander anderss sich ausgeben.
* Integrierung
  + Empfänger kann verifizieren, dass die Nachricht nicht verändert wurde als Transit
* Non-Repudiation (Nicht-Zurückweisung)
  + Der Sender einer Nachricht kann nicht fälschlicherweise sagen, dass er die Nachricht nicht gesendet hatte

Mögliche Schlüssel => keyspace

Information-theoretically secure:

* Unknackbar
* Bsp. One-Time-Pad

Computationally secure

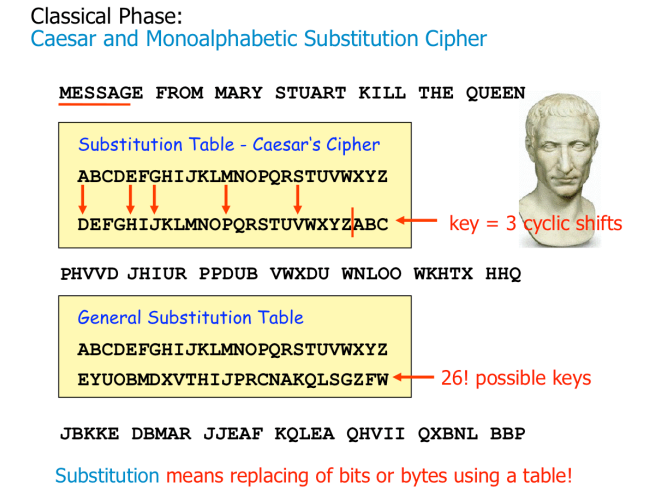
* Es gibt keine bessere Methdoe als brute force attack

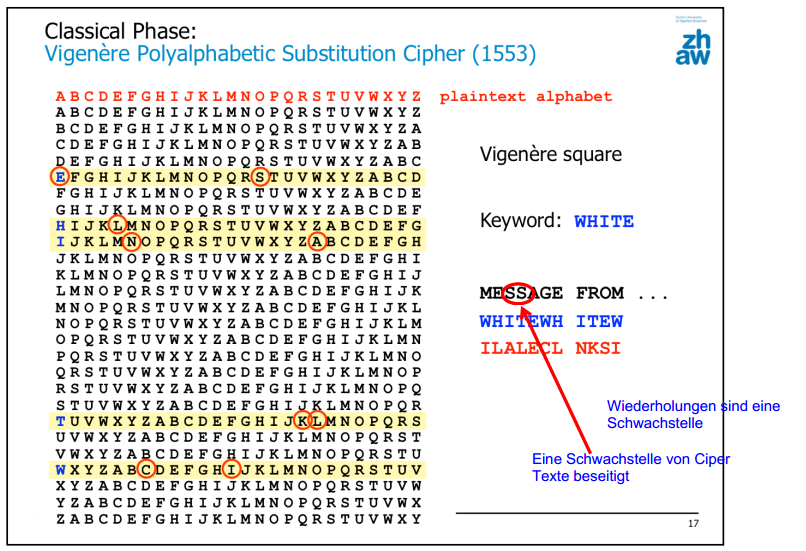
Verschiedene Attacken:

* Ciphertext-only atack
* Known-plaintext attack
* Chosen-plaintext attack
* Chosen-ciphertext attack

Eine starke cipher sollte alle möglichen Attacken aushalten

Vigenere Polyalphabetic Substitution Cipher => Wiederholungen sind keine Schwachstellen mehr.

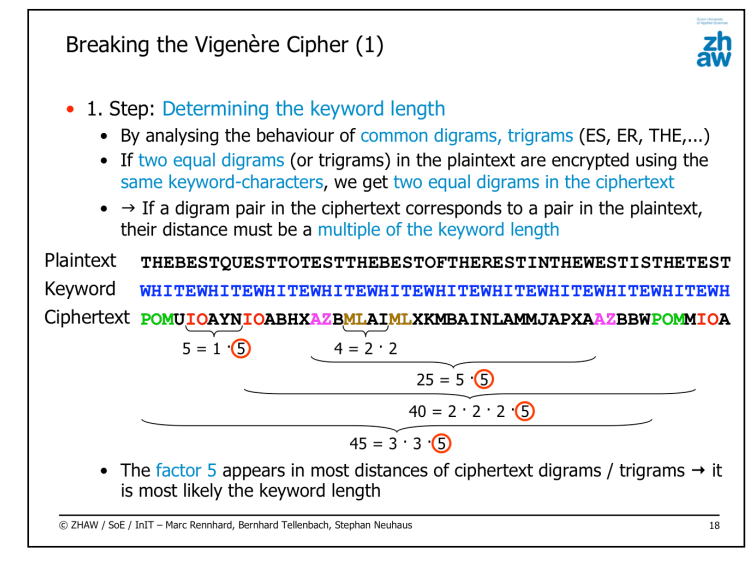


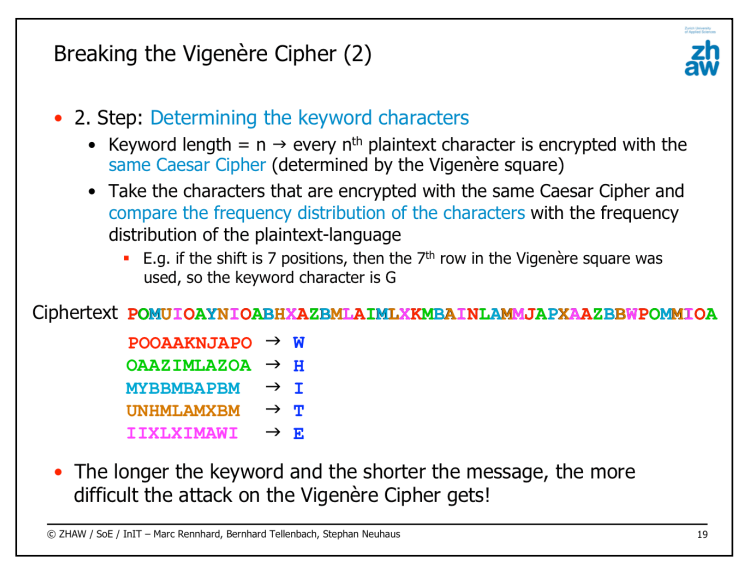


Stärke von Vigenere Cipher:

* 26 verschiedene Cipher Alphabeten werden gebraucht für die Verschlüsselung.
  + Daher wird das Knacken aufgrund der Häufigkeit der Buchstaben, viel schwieriger.

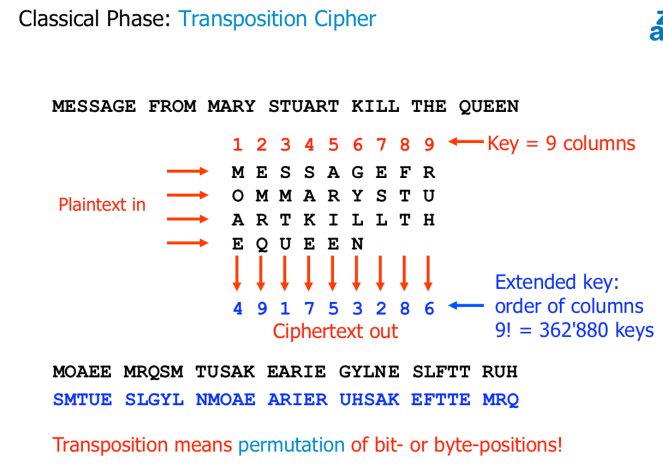
Breaking Vigenere Cipher:

* 

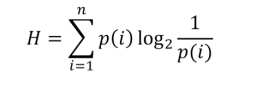


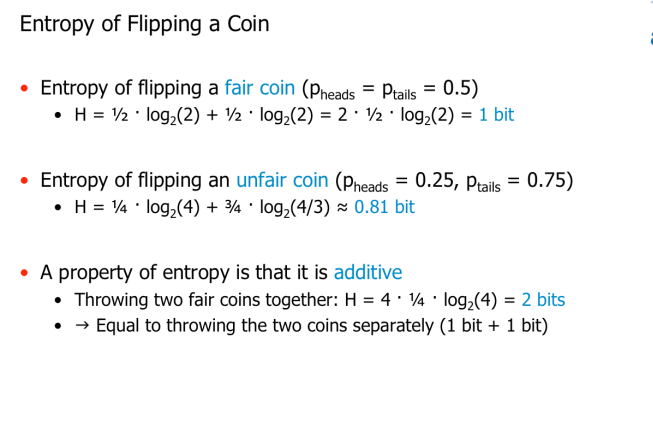
Je länger das Keyword and je kürzer die Nachricht, desto schwieriger wird die Attacke.

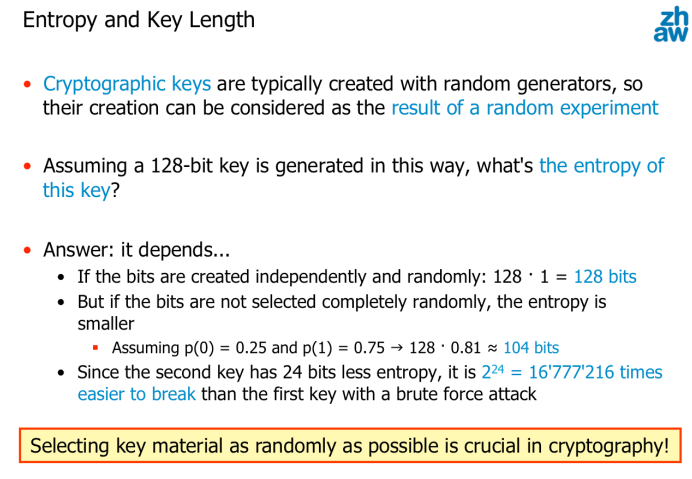
Transposition:



Anzahl Spalten ist Teil des Secret Keys.

Entropie berechnen





Plaintexte:

* Redundanz vermindern, da Redundanz böse ist und das Knacken erleichtert.
* Vor dem Verschlüsseln zuerst komprimieren.
* Gute Datenkompression kann fast alle Redundanzen entfernen.

