19. Landestagung der Fachgruppe GI-HRPI

Workshop: CrypTool

Dr. Doris Behrendt
25.09.2023
Sportschule und Bildungsstätte, Landessportbund Hessen e.V.

Entwurf

FI CODE Forschungsinstitut Cyber Defence Universität der Bundeswehr München

Dat Com Professur Datenschutz und Compliance Universität der Bundeswehr München

Was ist CrypTool und was hat es mit der Bundeswehr zu tun?

- Steht im Abstract zu *dieser* Veranstaltung ;-)

Bildnachweis: Forschungsinstitut CODE / Bellgrau

Links, von links nach rechts: Prof. Arno Wacker, Prof. Bernhard Esslinger, Prof. Michaela Geierhos (Technische Direktorin des Forschungsinstituts CODE) bei der Urkundenübergabe des CrypTool-Projektes.

- Software Downloads von `https://www.cryptool.org`
  - CrypTool-Online (CTO) –> derzeit in Überarbeitung
  - CrypTool 2 (CT2)
    - Nils Kopal `https://www.kopaldev.de`
    - YouTube `https://www.youtube.com/@CryptographyForEverybody/featured`
    - Discord channel Cryptography for everybody
  - CrypTool 1 (CT1), z. B. Spiel Zahlenhai
  - JCrypTool (Java-CrypTool, JCT)
  - CrypTool Transcriber and Solver (CTTS) –> DECRYPT Projekt `https://de-crypt.org`; Github `https://github.com/CrypToolProject/CTTS`

- Webseite
  - Landing Pange CrypTool-Portal (CTP) https://www.cryptool.org/de/
  - MysteryTwister (MTW) https://mysterytwister.org/home/welcome/ –> derzeit in Überarbeitung; Bitte Account anlegen!
  - CRYPTO TOUR
  - Materialien, u. a. CrypTool-Buch; momentan nur deutsche Version von 2018 verfügbar: https://cryptool.org/download/ctb/CT-Book-de.pdf; viele SageMath-Beispiele
  - Edu-Bereich, z. B. https://www.cryptool.org/en/education/history; teils nicht up to date;
  - Handyoptimiert: Das Chinesische Labyrinth https://www.cryptool.org/de/education/CTTC CTTC CrypTool TwitterCampus –> verworfen
  - Thematische Suche ... gut versteckt: www.cryptool.org –> Dokumentation –> CT-Funktionsumfang https://www.cryptool.org/de/documentation/functionvolume

Entwurf

Lehrpläne? –> Lehrplanrecherche

1. Caesar
2. Substitution
3. Transposition
4. DH
5. RSA
6. Signaturen
7. Hashfunktionen

Recherche zum Auftreten von *Kryptografie*, *Verschlüsselung*, *Kodierung* in deutschen Lehrplänen für das Fach Informatik

Stand: 2023-04-11

Wie gelangt man am besten zu den Lehrplänen? ⟶ Mühsame Handarbeit aufgrund föderalen Wildwuchses.

KMK sammelt Links, aber die führen lediglich zum Internetauftritt des jeweiligen Bundeslandes und von dort aus kann es immer noch lange dauern, bis man fündig wird: https://www.kmk.org/dokumentation-statistik/rechtsvorschriften-lehrplaene/uebersicht-lehrplaene.html

Es gibt auch noch den Bildungsserver vom Leibniz-Institut, aber der hat genau dieselbe Liste, nur mit weniger Informationen als bei der KMK: https://www.bildungsserver.de/lehrplaene-400-de.html

Schwerpunkt der Recherche: Sekundarstufe 2, Gymnasium; Sekundarstufe 2 entspricht grob den Jahrgangsstufen 10 bis 13 und damit dem Alter von 16 bis 19 Jahren

Probleme: Nur manchmal wird ein zeitlicher Umfang genannt, oft ist Kryptografie nur als ein mögliches Beispiel für eine Projektarbeitsphase genannt, viele Lehrpläne sind veraltet (<2010) und werden momentan überarbeitet (oder auch nicht); moderne Lehrpläne enthalten weniger konkret-fachliche Inhalte, sondern sind *kompetenzorientiert* formuliert derart „die SuS *vergleichen* symmetrische und asymmetrische Verschlüsselung“ oder „die SuS *bewerten* oder *untersuchen* Algorithmen, z. B. . . . “;

Persönliche Meinung: Der Lehrplan vom Saarland hat mir am besten gefallen.

Aufgabe 1: Erste Schritte mit Caesar, CTO und CT2

- Gehen Sie zur CT-Funktionsumfang-Suche `https://www.cryptool.org/de/documentation/functionvolume` und suchen Sie Caesar!
- Hier: `https://www.cryptool.org/en/cto/caesar`
- Dort ist auch ein Link zu `next-cto`.
- Schauen Sie sich das Video von Nils Kopal hierzu an:

  `https://youtu.be/IuasEqanRAM?si=JBV33HlR_E8XzT49`

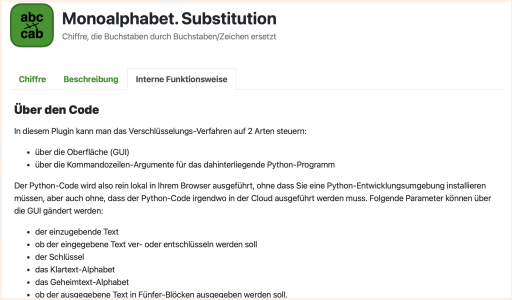
  (Dauer: knapp 8 Minuten)

  Findet man auch, wenn man auf seinem YouTube-Channel nach *Caesar* sucht.
- Wenn man auf dem YouTube-Channel ist und auf *Videos* und dann auf *Popular* klickt, findet man insbesondere *Short Introduction to CrypTool 2* (Dauer: knapp 22 Minuten)

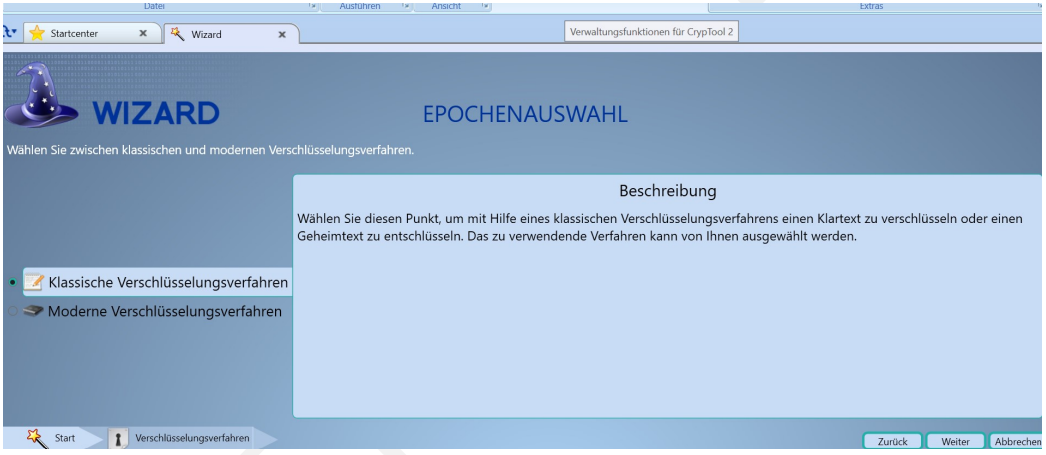
Entwurf

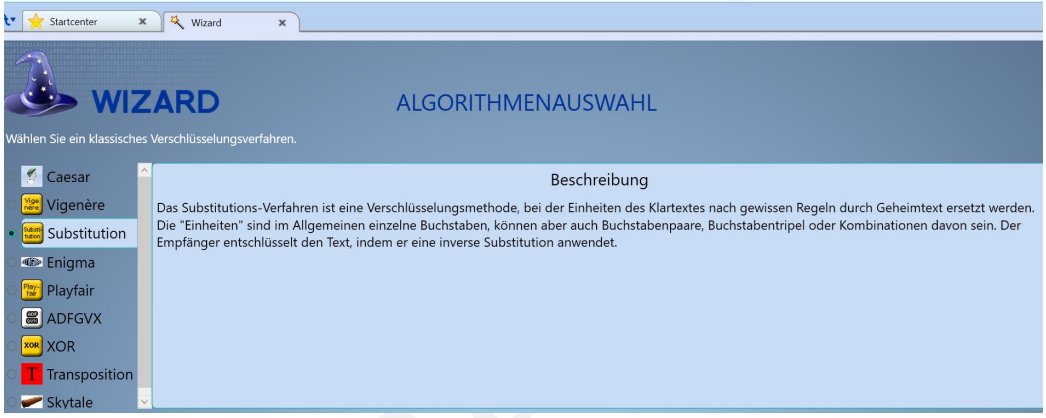
Aufgabe 2: Erkunden Sie nun selbst die klassischen Verfahren (Substitution, Transposition)

Beachten Sie auch die READMEs von CTO:

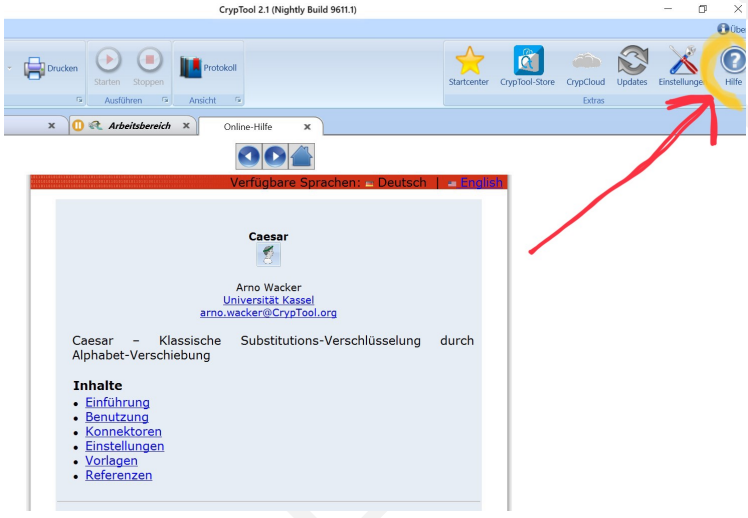


Probieren Sie den WIZARD von CT2:




Startcenter
Wizard
WIZARD
ALGORITHMENAUSWAHL
Wählen Sie ein klassisches Verschlüsselungsverfahren.
Caesar
Vigenère
Substitution
Enigma
Playfair
ADFGVX
XOR
Transposition
Skytale
Beschreibung
Das Substitutions-Verfahren ist eine Verschlüsselungsmethode, bei der Einheiten des Klartextes nach gewissen Regeln durch Geheimtext ersetzt werden. Die "Einheiten" sind im Allgemeinen einzelne Buchstaben, können aber auch Buchstabenpaare, Buchstabentripel oder Kombinationen davon sein. Der Empfänger entschlüsselt den Text, indem er eine inverse Substitution anwendet.

CT2 hat auch detaillierte Hilfeseiten:



Aufgabe 3: DH

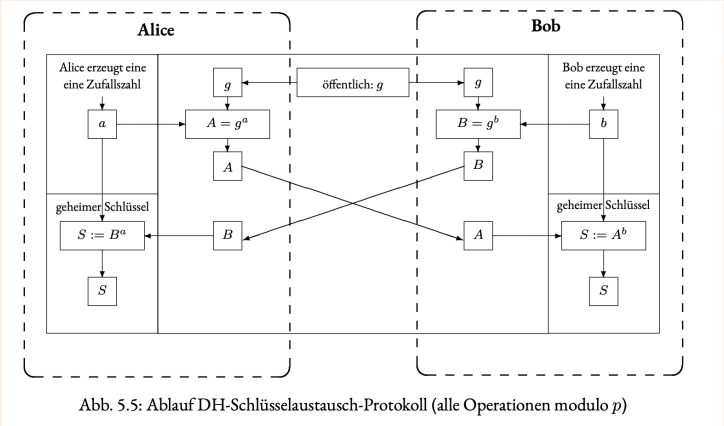


Abb. 5.5: Ablauf DH-Schlüsselaustausch-Protokoll (alle Operationen modulo p)

Situation:

- p Primzahl $\Rightarrow$ $\mathbb{Z}_p^*$ ist zyklische Gruppe der Ordnung $p - 1$
- g Primitivwurzel mod n
- $g^a = A \bmod p$ schnell berechenbar („square and multiply“)
- $a = \log_g(A) \bmod p$ diskreter Logarithmus; mit nicht-Quantencomputern derzeit keine schnelle Berechnungsmöglichkeit bekannt

Suchfilter: diffie — Case sensitive

Kryptografische Kategorie: Kein Filter angewendet

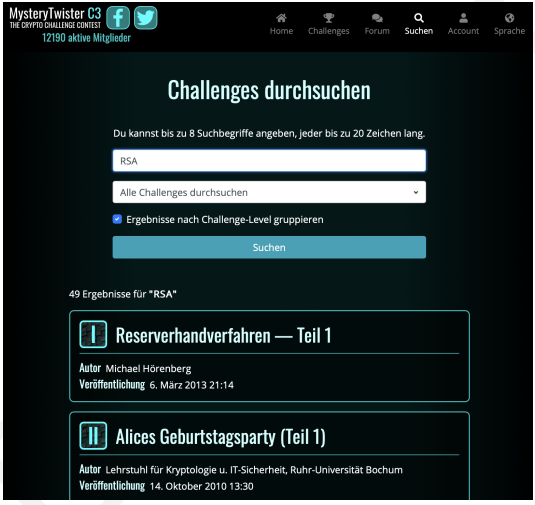
CrypTool 1 (CT1) — CrypTool 2 (CT2) — JCrypTool (JCT) — CrypTool-Online (CTO)

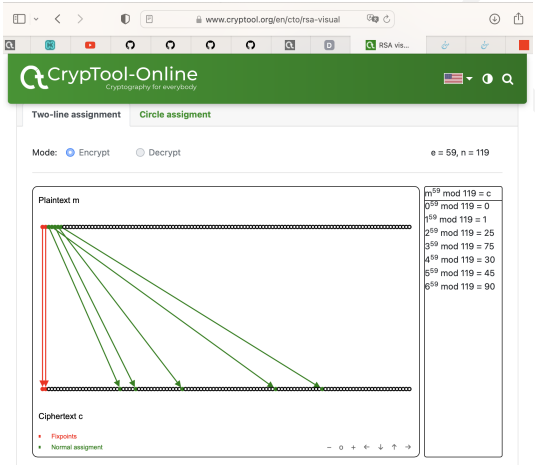
3 von insgesamt 345 Funktionsgruppen entsprechen dem Auswahlkriterium.

Funktionen	CT1	CT2	JCT	CTO	Pfad in CT1	Pfad in CT2	Pfad in JCT	Pfad in CTO
Diffie-Hellman-Schlüsselaustausch (Perfect Forward Secrecy) [Visualisierung]	X				Einzelverfahren \ Protokolle \ Diffie-Hellman-Demo...			
Schlüsselaustausch (Diffie-Hellman DH)		T	D			[T] \ Protokolle \ Diffie-Hellman-Schlüsselaustausch [T] \ Protokolle \ Diffie-Hellman-Schlüsselaustausch über Netzwerk	[D] \ Visualisierungen \ Diffie-Hellman Schlüsselaustausch (EC)	
Sicherer Chat – Angewandte Kryptografie		T				[T] \ Werkzeuge \ Einfacher Video-Audio-Chat mit AES-Verschlüsselung [T] \ Werkzeuge \ Diffie-Hellman AES-Video-Audio-Chat [T] \ Werkzeuge \ Einfacher AES-Chat		

Video von Nils Kopal: https://www.youtube.com/watch?v=2Uz9hdhcFv8

Aufgabe 4: RSA, Signaturen, Hashfunktionen




www.cryptool.org/en/cto/rsa-visual
RSA vis...
CrypTool-Online
Cryptography for everybody
Two-line assignment
Circle assigment
Mode:
Encrypt
Decrypt
e = 59, n = 119
Plaintext m
Ciphertext c
Fixpoints
Normal assigment
m^59 mod 119 = c
0^59 mod 119 = 0
1^59 mod 119 = 1
2^59 mod 119 = 25
3^59 mod 119 = 75
4^59 mod 119 = 30
5^59 mod 119 = 45
6^59 mod 119 = 90

Signaturen: Suchen Sie im CT-Funktionsumfang, es gibt viele Treffer bei JCT, aber auch bei CT2

Entwurf

Hashfunktionen:

Hash-Algorithmen [Visualisierung]	X		D	Einzelverfahren \ Hashverfahren \ Hashwert einer Datei...		[D] \ Visualisierungen \ Hash-Sensitivität	
Hash-Kollisionen	X			Analyse \ Hashverfahren \ Angriff auf den Hashwert der digitalen Signatur...			
Hashwert einer Datei	X			Einzelverfahren \ Hashverfahren \ Hashwert einer Datei...			
HMAC	X	T/K		Einzelverfahren \ Hashverfahren \ Generieren von HMACs...	[T] \ Hash-Funktionen \ HMAC [K] \ Hash-Funktionen \ HMAC		
ImageHash		K/T			[K] \ Hash-Funktionen \ BildHash [T] \ Hash-Funktionen \ BildHash [T] \ Hash-Funktionen \ BildHash – Weichzeichnungs-Vergleich		

Show 10 entries

Previous 1 2 3 Next