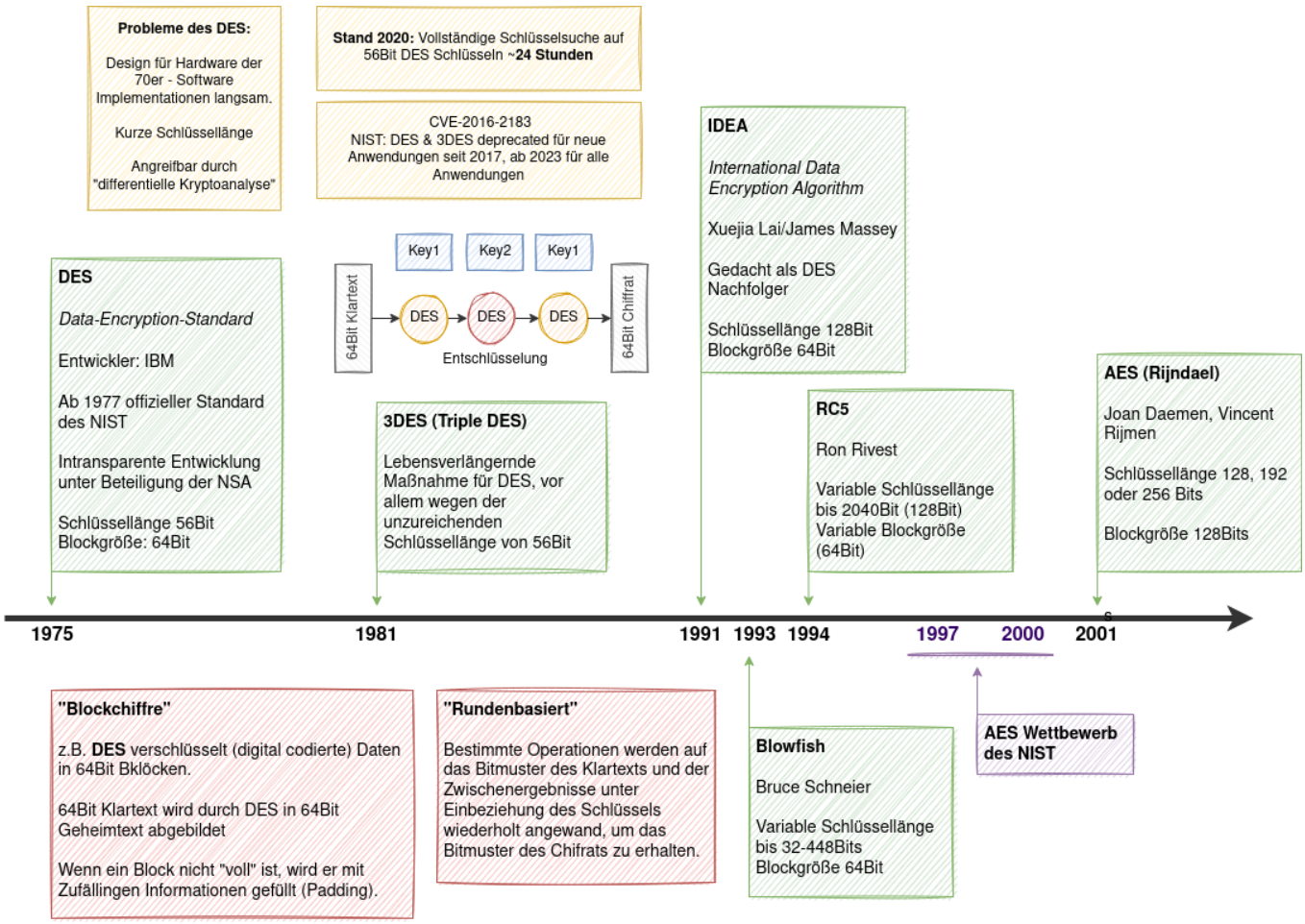
Moderne symmetrische Verschlüsselungsverfahren

Überblick



Rechercheaufträge

- Führe eine Recherche über die drei Verschlüsselungsverfahren **DES**, **IDEA** und **AES** durch. Beantworte die genannten Fragen. Achte darauf, dass deine Antworten auch Verweise zu den Quellen enthalten, aus denen du deine Informationen bezogen hast.
- Du kannst dich an der Zeitleiste im Überblick orientieren
- Erstelle eigene Notizen zu den Teilbereichen, in denen du wichtige Begriffe angemessen hervorhebst.

(A1) DES

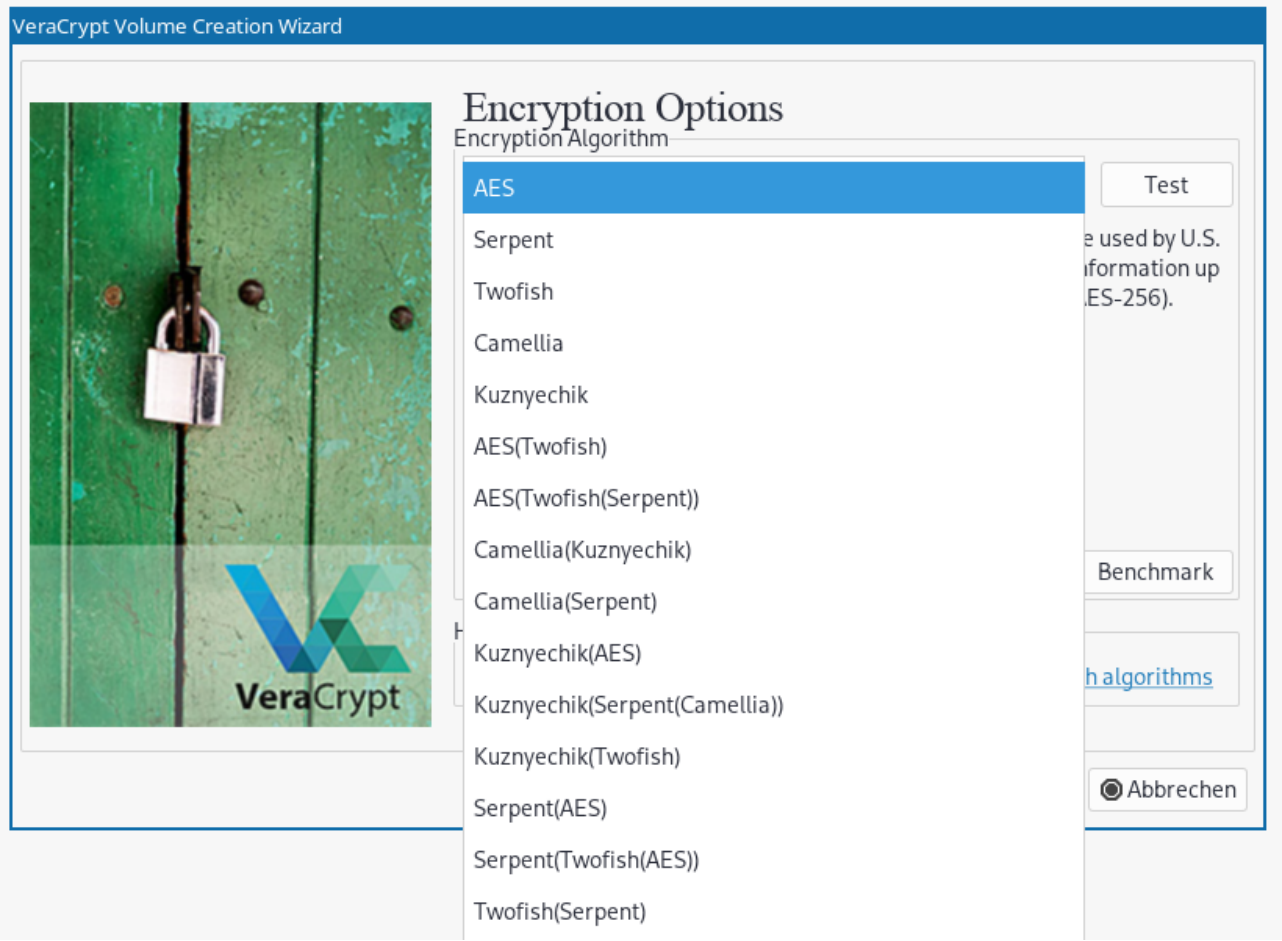
1. Wofür steht die Abkürzung "DES"? Wann und durch wen wurde dieses Verschlüsselungsverfahren veröffentlicht?
2. Wann war die erste erfolgreiche Kryptoanalyse von DES? Von welcher Art war der Angriff?
3. Wie groß ist die *Blockgröße* bei DES? Wie groß ist ein Schlüssel (Schlüssellänge)? Wie viele verschiedene Schlüssel gibt es?
4. Was ist *Triple-DES*? Wie wird es durchgeführt, warum wird es verwendet? Was ist die effektive Schlüssellänge von 3DES?
5. Ist DES/3DES heutzutage (2020er Jahre) noch sicher?

(2) IDEA & Co

1. Wer hat das IDEA-Verfahren entwickelt? In welchem Jahr wurde es vorgestellt? Warum wurde es etwickelt?
2. Wie lang kann ein ein IDEA-Schlüssel sein?
3. Finde weitere symmerische Blockchiffren, die in den 1990er Jahren entwickelt wurden.

(3) AES

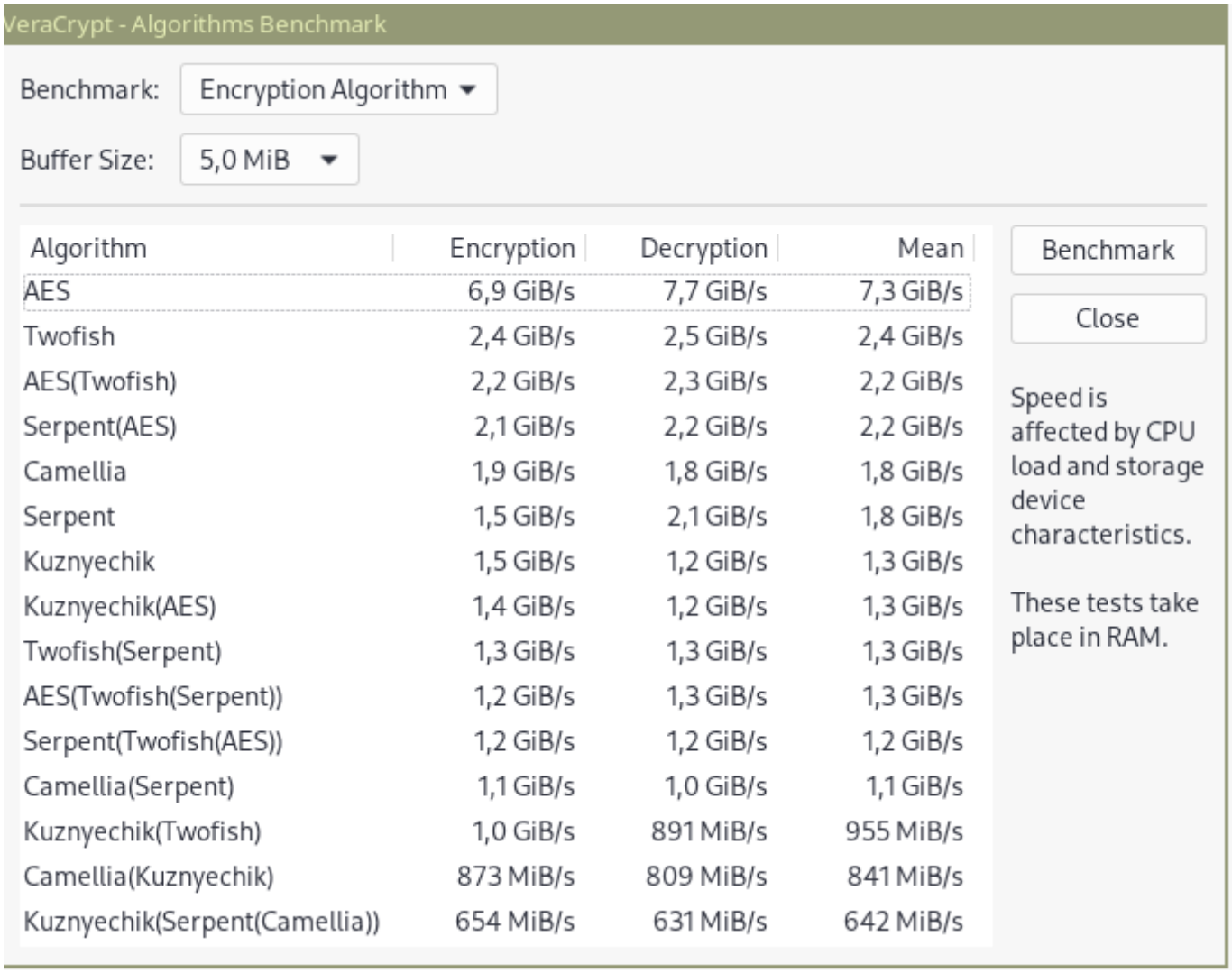
1. Beschreibe kurz die Entstehungsgeschichte von AES. Was ist das NIST und welche Rolle spielt es bei der Entwicklung von AES?
2. Was sind die wesentlichen Unterschiede zwischen AES und DES? Vergleiche Schlüssellängen und Blockgrößen.
3. Wie lange dauert eine vollständige Schlüsselsuche derzeit (2020er Jahre) bei DES, wie lange bei der längsten Schlüssellänge für AES?
4. Die freie Verschlüsselungssoftware Veracrypt bietet zahlreiche Verschlüsselungsalgorithmen an, die alle als weitgehend sicher anzusehen sind:



Was spricht heutzutage vor allem dafür, AES zu wählen?[1)]

Tipp zur letzten Frage

Ergebnisse des kryptographischen Benchmarks von Veracrypt - warum fällt das so aus?



Algorithm	Encryption	Decryption	Mean
AES	6,9 GiB/s	7,7 GiB/s	7,3 GiB/s
Twofish	2,4 GiB/s	2,5 GiB/s	2,4 GiB/s
AES(Twofish)	2,2 GiB/s	2,3 GiB/s	2,2 GiB/s
Serpent(AES)	2,1 GiB/s	2,2 GiB/s	2,2 GiB/s
Camellia	1,9 GiB/s	1,8 GiB/s	1,8 GiB/s
Serpent	1,5 GiB/s	2,1 GiB/s	1,8 GiB/s
Kuznyechik	1,5 GiB/s	1,2 GiB/s	1,3 GiB/s
Kuznyechik(AES)	1,4 GiB/s	1,2 GiB/s	1,3 GiB/s
Twofish(Serpent)	1,3 GiB/s	1,3 GiB/s	1,3 GiB/s
AES(Twofish(Serpent))	1,2 GiB/s	1,3 GiB/s	1,3 GiB/s
Serpent(Twofish(AES))	1,2 GiB/s	1,2 GiB/s	1,2 GiB/s
Camellia(Serpent)	1,1 GiB/s	1,0 GiB/s	1,1 GiB/s
Kuznyechik(Twofish)	1,0 GiB/s	891 MiB/s	955 MiB/s
Camellia(Kuznyechik)	873 MiB/s	809 MiB/s	841 MiB/s
Kuznyechik(Serpent(Camellia))	654 MiB/s	631 MiB/s	642 MiB/s

(4) Allgemeines

1. Erinnerung: Was ist ein *symmetrisches* Verschlüsselungsverfahren?
2. Was versteht man unter einer *Blockschiffre* (Blockverschlüsselung)? Was bedeutet in diesem Zusammenhang z.B. die Angabe "64 Bit" Blockgröße, Was versteht man unter "Padding"?
3. Was ist ein *rundenbasiertes* Verschlüsselungsverfahren? Was ist ein Rundenschlüssel?

[1)]

Recherchieren, nicht raten...