Test JCrypTool 1.0.0. unter Windows am 13.07.2020

Nils Kopal

1. Download und Installation

   Auf der Webseite steht Version 0.9

   https://www.cryptool.org/en/jct-downloads

   Downgeloaded habe ich aber 1.0 ☺

   Entpacken und starten klappt ohne Probleme.

2. Obwohl ich eine neue Installation runtergeladen, entpackt und gestartet habe, erhalte ich, als ich JCT öffne, RC4, welches ich zuletzt mit der alten Version offen hatte. Gibt es kein Einstiegsfenster, welches nach einer Neuinstallation kommt?

3. Ich schließe RC4.

4. Doppelkick auf ADFGVX im rechten Menü (Crypto Explorer). Es kommt eine Meldung, dass ich erst einen neuen Editor öffnen soll. Wo ich das tun soll, wird nicht angezeigt. Das wäre hilfreich, da vermutlich nicht jeder sich mit Eclipse auskennt ☺

5. Ich öffne einen neuen Editor oben links in der Ecke mit dem Icon. Jetzt geht auch die ADFGVX ☺. Ich verstehe, dass JCT sich wie CrypTool 1 bedienen lässt (Neuer Text (Editor), Auswahl des Verfahrens, Verfahren konfigurieren, danach erhalte ich einen neuen Text (z.B. Geheimtext) in neuem Editor). ADFGVX verschlüsselt. Es gefällt mir, wie der Key sich immer anpasst, wenn ich da verschiedene Keywords eingebe.

6. Nun probiere ich mal den Grille Analyzer aus. Da ich weiß, dass es sich wie CT1 bedient suche ich die Analysen unter „Analysis“ in der Dropdown-Leiste am oberen Rand. OK – habe gerade gesehen, dass es auch rechts einen Tab für Analysen (und weitere) gibt. Kann man den Tabs auch Symbole geben, damit ich diese „besser sehe“? Noch eine generelle Frage: Warum haben die einzelnen Verfahren alle das gleiche Symbol rechts?

   Zur Grille Analyse:

   a. Zunächst brauche ich einen verschlüsselten Text mit der Grille… daher suche ich mir einen Text und verschlüssele den mit der Grille Chiffre. Problem: Es gibt keine Grille-Chiffre im rechten Menü… Ok. Die Chiffre finde ich jetzt bei der Analyse – das find ich inkonsistent ☺ aber ok. Der vorgegebene Geheimtext ist übrigens Deutsch, obwohl ich JCrypTool in Englisch benutze. Ok, ich sehe wieder das ich da vorgegebene Texte auswählen kann und einstellbar ist, dass ich einen eigenen eingeben kann.
   b. Verschlüsseln, Entschlüsseln klappt gut… mir fällt nur auf, das Zahlen, die im Klartext stehen, an falschen Stellen im Geheimtext landen
   c. Analyse… ich analysiere einen Geheimtext mit 7x7 matrix. Analyse ist fix.
   d. Auch eine 11x11 Matrix funktioniert ohne Probleme. Dauert etwas länger. Coole Analyse

e. Mir fehlt ein Progress-Bar (oder eine Anzeige), wie weit die Analyse ist, damit man ungefähr weiß, wie lange es noch dauert. Auch möchte ich die Analyse stoppen können
f. Auch blockiert die Analyse offensichtlich die UI, was bedeutet, dass JCrypTool bei sehr großen Keys (ich teste gerade 20x20) einfriert.
g. 20x20 dauert knapp 45 Sekunden, liefert aber kein Ergebnis mehr (hier sind 800 Zeichen wohl zu wenig). Aber die Analyse gefällt mir trotzdem ☺
h. Ich teste das Ganze einmal mit mehr Buchstaben (diesmal mit 2800 Buchstaben). Nach 11 Minuten und 15 Sekunden ist die Analyse vorbei (so lange war JCT eingefroren) Aber es kommt nicht das richtige Ergebnis. Ich hatte die Restarts auf 10 gestellt. Trotzdem finde ich die Analyse gut so wie sie ist. 20x20 ist auch schwer.

7. Nun teste ich den Vigenère-Autokey. Mir fällt auf, dass wenn ich da doppelt in der Classic/Autokey-Vigenère draufklicke und die ADFGX-Analyse noch offen ist, nur die Hilfe unten links aufgeht.
   a. Entschlüsseln/Verschlüsseln klappt ☺
   b. Ich würde nicht Uppercase/Lowercase als Default-Einstellung für das Alphabet wählen. Der Vigenère-Autokey arbeitet normalerweise nur auf einem Alphabet ohne Beachtung der Groß-Klein-Schreibung.
   c. Zum Spaß probiere ich noch den „puren" Vigenère aus. Der sieht ja quasi 1:1 wie der Autokey aus. Da frag ich mich, warum man dafür zwei Komponenten pflegt. Idee: Ich würde diese mergen und einfach einen Schalter beim Vigenère für den Autokey-Mode machen.

8. Ich spiele ein wenig mit Double-Box. Frage: Warum gibt es hier ein Dropdown für die Alphabete welches gesperrt ist?

Für die folgenden Tests habe ich folgenden ASCII-encodierten Text genutzt:

„**F**ranz jagt im komplett verwahrlosten Taxi quer durch Bayern"
(ohne die Anführungszeichen)

9. Ich teste SHA
   a. Ich wunder mich, warum da keine 160bit sondern 256bit (32 byte) rauskommen. Ich hatte erwartet, dass das SHA-1 ist ☺
   b. Nach Testen mit CT2 verifiziere ich, dass das SHA256 ist… ☺
   c. Es sollte irgendwo stehen, dass mit „SHA" eben SHA256 gemeint ist. Es gibt SHA-1, SHA-224, SHA-256, SHA-384 und SHA-512. Da das vermutlich alles Aufrufe von BouncyCastle sind, würde ich in dem bisher ungenutzten Fenster des Plugins, welches auch darauf hinweist, dass es ungenutzt ist, ggfs die SHA-Version auswählbar machen.

10. Ich teste AES
    a. Ich verschlüssele mit dem Key = 0,0,0,…,0 und ohne Padding
    b. Ich würde gerne den Text als Hex-Array rauskopieren um dann mit CT2 zu entschlüsseln. Dafür markiere ich im „Hex-Editor" die entsprechenden Hex-Zellen und wähle Kopieren. Leider geht das nicht.

c. Frage: Wie soll ich den Text aus JCrypTool „einfach“ rausbekommen? Auch den UTF-8 Text in der ganz rechten Spalte geht leider nicht zu kopieren. Und selbst wenn, das könnte man niemandem geben, da der Text quasi „kaputt“ ist. Ich würde mir eine einfache Möglichkeit wünschen, die markierten Bytes als „Hex-Werte“ zu kopieren

11. Absturz mitten im Testen. Ich bin zurück zu JCrypTool gewechselt (Alt-Tab) in Windows und habe in den Hex-Editor geklickt. JCrypTool ist ohne irgendeine Meldung „einfach verschwunden“. Also restarte ich das jetzt.
    (Ich sehe, dass es einen Crashreport im JCT-Verzeichnis gibt – keine Ahnung ob der davon ist. Den schicke ich nach dem Testen mit)

12. Ich finde es gut, dass alle meine offenen Tabs wiederhergestellt werden (also auch die Hex-Editoren mit meinen AES-Tests).

13. Ich teste jetzt Visuals – da finde ich auch die Grille-Chiffre

    a. Ich bringe diese direkt zum Absturz (JCT friert ein) indem ich zwei Löcher manuell wähle und (weil ich faul bin) dann den Rest random verteilen möchte. JCT friert ein und ich kann es nur noch beenden. Neustart JCT.
    b. Ich teste, ob ich das reproduzieren kann. Nein, jetzt klappts :D
    c. OK… ich gebe einen Text in den Plaintext ein und klicke dann wieder auf „Put random holes“ -> JCT friert ein
    d. Ich versuche das noch mal zu reproduzieren: (was übrigens „nervt“ – wenn ich die Grille unter Visuals anwähle, öffnet JCT mir das nicht „in der Mitte“ sondern rechts – ersetzt quasi den Crypto-Explorer. Ich muss es dann quasi jedes Mal manuell in die Mitte ziehen. Es sollte direkt in der Mitte aufgehen). Und ich kriege den Fehler gerade wieder nicht reproduziert.
    e. Fakt ist: Ich habe es zweimal beim Klicken auf „Put holes randomly“ zum Einfrieren gebracht :-D – und vorher in der Grille selbst „rumgeklickt“. Dann müsst Ihr den Fehler wohl selbst suchen ;-)

14. Ich schaue mir nun noch den „Number Shark“ an… auch hier öffnet der sich wieder Rechts über dem „Crypto Explorer“ und ich muss ihn manuell in die Mitte ziehen.
    a. Shark gewinnt… :D
    b. Ok, ich will nochmal spielen. Wie resette ich das jetzt… ?
    c. Ok, ich finde die kleinen Icons im Titel… die sind nicht sofort ersichtlich ☺
    d. Ich verstehe das Spiel nicht… was muss ich hier tun? Ich wähle Zahlen aus und dann werden „vom Hai“ irgendwelche anderen markiert… es wäre schön, wenn da irgendwo die Spielregeln stehen würden bzw was der Hai genau macht. Ok. Durch ein wenig Geklicke schaffe ich es, die Hilfe zu finden ☺ - der eine Satz oben über dem Spiel hilft nicht weiter. Ich verstehe, dass der Hai alle Teiler der Zahl bekommt, die ich auswähle… also ab zu den Primzahlen. Ok, habe das Spiel jetzt verstanden.
15. Ich probiere „Zudo-Ku“ aus… Das ist so träge und langsam, und ich habe null Ahnung was ich hier machen soll, das ich es wieder schließe ☹
16. Ich probiere noch den Vigenere-Breaker aus.
    a. Ich wähle Automated Analysis und bekomme ein leeres Fenster
    b. Manual Analysis friert JCT ein (und ich muss es wieder hart beenden)

Alles in Allem muss ich sagen, dass JCT ein krasses Qualitätsgefälle hat. Es gefällt mir aber dennoch sehr gut ☺

Es gibt viele coole Sachen, aber ich habe es geschafft, das Ganze innerhalb von 2h mindestens fünf Mal zum Totalabsturz zu bringen.

So ein Qualitätsgefälle haben wir in CT2 ja auch – insbesondere Komponenten und Templates die ich „langweilig“ finde, sind nicht so ausgereift, weil ich da natürlicherweise weniger Zeit reinstecke, als in meine „Lieblinge“. Ähnlich wird es vermutlich mit JCT sein, denke ich. Aber das macht den Gesamteindruck für einen externen Tester schlecht. Auch sind nicht immer alle Entwickler gut oder sehr gut, die eine Komponente für CT2 oder JCT bauen. Die Abstürze sollte und muss dann aber die Architektur drum-herum abfangen.

Es sollte wohl noch mal über alle Plugins gegangen werden, und alle Funktionen getestet. Auch würde ich schauen, dass nicht alles im UI-Thread ausgeführt wird, sondern die Komponenten eigene Threads starten. Dann friert das komplette JCT nicht ein, wenn eine Komponente amok läuft. Auch sollte der „Komponententhread“ dann beendet werden, wenn das entsprechende Fenster geschlossen wird (im Notfall den Thread hart killen).