Im Rahmen der Fortbildung für Agenten sollen Sie die eben gelernten Methoden über maschinelle und moderne Verschlüsselung selbst anwenden. Sie müssen wieder eine Reihe von Aufgaben absolvieren, und – wie in der Grundausbildung – gibt es in jeder Aufgabe ein Codewort, welches Sie sich notieren sollten. Sobald Sie alle Aufgaben bearbeitet haben, fügen Sie auf einem Zettel alle Codewörter (CW1-CW4) zu einem einzelnen Codewort der Form CW1CW2CW3CW4 zusammen. Dieses zusammengesetzte Codewort nennen Sie einem Ihrer Vorgesetzten. Sie erhalten daraufhin das Passwort für Ihren dritten Auftrag.

Aufgabe 1 – Enigma anwenden

Verwenden Sie CrypTool 2, um folgenden Text zu entschlüsseln:

HYNLJ CMAMT LSHNZ YJLQZ ACDDV HZYTE BYLUB EKHVX XMAMS VVPUN RIKXE ITZKW UXJNT YEONQ AXHNS MRDTX ONITO WXIOT UHMFV SRSIA VMCWI OJGEX OYBLL DXOPY XCFII OINXU AAGPO ZPMKM DGUCZ HZJGH TZRAK YLMTM XXQJV GMB

Die verwendeten Einstellungen sind:

```
UKW |  Walzen | Ringstellung |    == Steckerverbindungen ==
=============================================================
 C  | VI I V  |   11 18 5    |    AN EF GV HI LZ
```

Als Startposition wurde **WAR** verwendet. Achten Sie bitte insbesondere auf die Reihenfolge der Walzenlage: In CrypTool 2 befindet sich die schnellste Walze (hier **V**) ganz oben (Rotor 1). Die gleiche Anordnung gilt für die Ringeinstellung. Beim Steckerbrett müssen die voreingestellten Steckerverbindungen zunächst entfernt werden, bevor die oben angegebenen verwendet werden können.

Der verschlüsselte Text enthält das Codewort. Bitte notieren Sie dieses.

Aufgabe 2 – AES anwenden

Verwenden Sie CrypTool 1.4, um folgendes Chiffrat zu entschlüsseln:

v1mmJIrEKdy4lHP9z7MMSZ4+vy7SPyUlKSV1pdSuhW2AsTrztIfvTy65Aznjh3rC4E466tjAlpW/KDKMeP5zZfQc3QOWiiZpHhmYjPwcLrVcJxSxylrSdSJ/hJjPqKM1NK0mycKxnECgrnz67VPHISB1uT8qyPH+lOux1umhrRTv6+hYbB6Hkn3GdmXC14VpXzCSBECjJ6IflTsS28yIovLghWMPZC/9RTqU1UbgRTnmbIIYLOB67U9dg/HDk+cJxe6wff+7uQErSvjFbE4EWsE0C2hv59Ctriz6cAbmZn+SQkPEsCGNsFM1OtcFeZft1ipHu6Ri3dTq964P8IWAfMV6c9D1yqsQrIVB22/1GuPm4tjxaccwoj6aO9XI4U5V4ItAxBfYBHxiLfa9/Zqx0e+eqD5vdWvxerAbE7PEICRWcxiTHIm/sJ+4SuYcQGg3+seQqQC+keeYUD2w1YsoqDs/m8q8S4Q5308hdW9J6m9M+8fwpuI6KwzuJ+3buYeqctrTjrash+/GBgnkSa2qdA==

Um die binären Daten hier darstellen zu können, wurden diese zusätzlich Base64 kodiert. D.h. um den gegebenen Text zu entschlüsseln, müssen Sie zunächst die Base64-Kodierung umkehren und danach mit AES entschlüsseln. Beides kann in CrypTool sehr einfach durchgeführt werden. Klicken Sie in CrypTool 1.4 zunächst auf „Neu“, um ein neues Fenster zu erzeugen. Kopieren Sie nun obigen Text in dieses Fenster. Wählen Sie aus dem Menu ***Einzelverfahren → Tools → Codierungen → Base64-Codierung/Decodierung → Base64 decodieren***. Es öffnet sich ein neues Fenster mit vielen unleserlichen Zeichen – dies ist normal, da nicht alle Bytewerte druckbare Zeichen sind. Sie können

dieses Fenster optional nun auf Hexadezimalansicht umstellen, um die Bytewerte zu sehen. Das geht unter ***Ansicht → Als HexDump anzeigen***. Wählen Sie nun ***Ver-/Entschlüsseln → Symmetrisch (modern) → Rijndael (AES)***. In der sich öffnenden Dialogbox geben Sie den Schlüssel **C736688FB928E55660ABBF6AED1A8972** ein und klicken anschließend auf „Entschlüsseln".

Es öffnet sich nun ein weiteres Fenster mit dem Klartext. Notieren Sie sich das gefundene Codewort.

Aufgabe 3 – AES-Schlüssel suchen

Bei den modernen Verfahren, zu denen es keine bekannten Angriffe gibt, bleibt nur die vollständige Schlüsselsuche, d.h. jeden möglichen Schlüssel zu probieren und jedes Mal berechnen, ob das Ergebnis Sinn macht (Entropie). Moderne Computer können den Bereich bis zu 40 Bit problemlos durchsuchen – wobei 40 Bit schon eine Weile (von Tagen bis zu Wochen, abhängig vom Rechner) dauern kann. Alles über ca. 70 Bit gilt heute noch als sicher, da es selbst für viele parallel arbeitende Computer noch zu lange dauern würde, alle Schlüssel zu durchsuchen. Um auf der ganz sicheren Seite zu sein, verwendet man heute Schlüssellängen von mindestens 128 Bit.

Gegeben seien nun folgende verschlüsselte Daten – wieder wie in Aufgabe 2 zusätzlich in Base64 kodiert.

TLy16Z4cj55jJc+l0cr/vW/1nHAs71j+9tk/AynjdDdW0L/PnYWvfR88Bq2RwMduqVccD3016nNx/Vqh9yr4Tn2clQGxB05niE7DK4hJkMOv26QTtiaRh4n7X8vxMitOM84buR5VJtOgQ6bd5UI9XiaaBf9+tcSY04PrHhvUWZo995WZ2xfNCgFI0KJZ/NOtKeId+CHBVPBx7fMHUkYgvvymWu8ssKAD6PB3KPxDxjq06av7LBrQTbMCbu6O12wP8yzCHfMkhCtgakmIFbt8J6IStYSkaz2Meg1dHEn59d07udODmLfZqJbi5Q98FWrdHq5ECRXQ5D1PD8DeRjDLLpeMKs4O1gw7lDmrQfxaBLFxo5M/JV7NtgsWrHwdrkYehodu5oveq3I3U5HgQ1vmsf25nd1Nbd1/hW3OEa6aU388VLxO2xeFKUfvXsa/FlKbJhV/XQgyHmhnT/16pEF8zNUlxfTcW9S+X6rR1Q5iq8ULJ9v2djQ8T9UdqBdEvcnlGDNVLsQ5Arkc0gcAPhhEtSOv3xjDiBn12NTEyztsn/x4vPISSbIJwUqQh5uy68s7QKBmD3oU6R0wYDEAwu2+BfnApIU2Lf5rXu4yZpksjv+BLKXtPZ+emMgifxtT0hiazvIziYJwo4y/xhZ4PdRBFbaU0FzBZTEgvyH2wQO/YZPHtY7lrK31PM7zNRucD6V9c+64I0WAx6l2LmkRjQHWMuEsC2I3d2fh8jK9PLmPziqIZw1UlsHXOZI/ABRuUlrff3mkyld++pFwpvUx9FV+hmYPNcA391dEsL64bgE/gJRJRd55NAxJ0N5BFKIkBQJRikANw8dXItQS8rKAPUmeY9SUPrwIVVqSCEyhKRajlhc=

Gehen Sie nun genauso wie in Aufgabe 2 vor, um die Base64-Kodierung rückgängig zu machen. Zum AES entschlüsseln verwenden Sie diesmal allerdings die Analysefunktion von CrypTool 1. Wählen Sie dafür im Menü von CrypTool die Funktion ***Analyse → Symmetrische Verfahren (modern) → Rijndael (AES)***. Es öffnet sich eine Dialogbox, in der zunächst alle Stellen des Schlüssel mit einem * gekennzeichnet sind. Geben Sie nun folgenden Teilschlüssel ein: **CD8B52A56EF58B38E5648174B9E**. Die letzten 20 Bit bleiben mit einem Stern (*) markiert, d.h. diese werden durchprobiert. Nach einem Klick auf „Starten" können Sie den Fortschrittsbalken verfolgen, wie Ihr Rechner nun die 2^{20} = 1048576 Möglichkeiten durchprobiert. Als Ergebnis sehen Sie eine Liste mit möglichen Entschlüsselungen – meist steht ganz oben der Richtige. Durch einen weiteren Klick auf „Auswahl übernehmen" können Sie den Klartext vollständig lesen.

Bitte notieren Sie sich wieder das gefundene Codewort.

Aufgabe 4 – RSA knacken

Sie haben die Nachricht **c=225332300289110864632549682024917334712049638752 15** abgehört und wissen, dass dies eine mittels RSA verschlüsselte Nachricht ist. Der öffentliche Schlüssel des Empfängers ist **(e,n)=(65537,380524036095333262332887725740536951817936705032 69)**. Da die Zahlen (im kryptographischen Sinn) nicht besonders groß sind, bietet diese Verschlüsselung keinen guten Schutz. Öffnen Sie CrypTool 1 und wählen Sie im Menü ***Einzelverfahren → RSA Kryptosystem → Faktorisieren einer Zahl***. Kopieren Sie sich den Wert für n in das Feld für die zu faktorisierende Zahl und klicken Sie auf „Weiter“. Nun beginnt CrypTool mit der Faktorisierung dieser Zahl, indem verschiedene Algorithmen verwendet werden. Nach ca. einer Minute sollte das Ergebnis bereit stehen. Beachten Sie, welcher Algorithmus zum Erfolg führte. Kopieren Sie sich die beiden gefundenen Faktoren in eine Textdatei zur späteren Weiterverwendung. Nun können Sie die Dialogbox fürs Faktorisieren schließen. Wählen Sie als nächstes im Menu ***Einzelverfahren → RSA Kryptosystem → RSA Demo***. Kopieren Sie nun die beiden gefundenen Faktoren in die Felder für die Primzahlen p und q. Stellen Sie sicher, dass beim öffentlichen Schlüssel der Wert 2^16+1 (oder 65537) eingetragen ist. Um aus den beiden Primzahlen alle für das RSA-Verfahren notwendigen Zahlen zu berechnen, klicken Sie nun auf „Parameter aktualisieren“. Selektieren Sie im unteren Bereich die Eingabe als Zahl und kopieren Sie den Wert für c in das Feld „Eingabe der Nachricht…“. Klicken Sie nun auf „Entschlüsseln“ und notieren Sie sich die drei Buchstaben, die im Klartextfeld auftauchen – das ist Ihr Codewort für diese Aufgabe.

Abschluss der Fortbildung

Schreiben Sie die vier gefundenen Codewörter auf einen Zettel in der Form CW1CW2CW3CW4 und kontaktieren Sie damit Ihren Vorgesetzten (Hinweis: Lesen sie das gesamte Codewort rückwärts). Sie erhalten dann das Passwort für Ihren dritten Auftrag.