EXCEL – VERSCHLÜSSELUNG – PRO MEMORIA

Die Verschlüsselung von Buchstaben und Ziffern erfolgt in mehreren Schritten:

Die ins Textfeld eingegebenen Zeichen werden für den Versand einzeln in vier – und fünfstellige Zahlen transformiert. Die «offen» zu versendende Zahlentabelle enthält dabei stets 1000 Zahlen, wovon aber höchstens deren 500 den realen Text verschleiern. Die übrigen Zahlen (1000 minus Anzahl eingegebener Zeichen) sind – teilweise identische – Zufallszahlen.

Eine erste Zahlenzuordnung der realen Zeichen des zu verschlüsselnden Textes erfolgt nach einem definierten Algorithmus, nach welchem ein bestimmter Buchstabe oder eine bestimmte Ziffer in eine «erste Zahl» transformiert wird. Diese «ersten Zahlen» bilden in der Folge je das Argument zu einer komplexen mathematischen Funktion, aus welcher die zur Übermittlung vorgesehenen vier – bis fünfstelligen Zahlen berechnet werden.

Im Umkehrverfahren wird der an den Empfänger übermittelte Zahlenschlüssel in analoger Weise «zurückgerechnet» und kommt in einer speziellen Entschlüsselungstabelle unmittelbar als ursprünglicher Text zurück. Will der Empfänger dem Absender oder einer mitbeteiligten Workgroup antworten, verschlüsselt er seinerseits seine Meldung im EXCEL – Verschlüsselungsprogramm, kopiert die Verschlüsselungstabelle (das heisst die 1000 vier – bis fünfstelligen Zahlen) und versendet diese als separate Exceltabelle (als Anhang per E – Mail, per SMS, per WhatsApp...oder per Briefpost, etc.) an den Adressaten.

Erwägungen zur Sicherheit:

Dank dem Umstand, dass im versendeten Schlüssel stets 1000 Zahlen «ohne Zwischenräume» enthalten sind, ist bei einem allfälligen «Fishing» der Daten für den Aussenstehenden nicht erkennbar, wie viele Worte und Zahlen die Meldung enthält. Ausserdem verhält es sich so, dass bei z.B. 100 Mal neu geschriebenem identischen Text daraus 100 Verschlüsselungstabellen mit unterschiedlichen Zahlenmustern generiert werden – welche bei der Entschlüsselung trotzdem immer den gleichen Ursprungstext liefern.[1)] Damit würde es auch bei tausenden von «gefischten» Verschlüsselungstabellen wohl unmöglich, Rückschlüsse auf einzelne Buchstaben anhand der Zahlenmuster zu schliessen. Zudem ist nicht rekonstruierbar, bei welchen der vier – oder fünfstelligen Zahlen es sich jeweils um echte Zeichen, und bei welchen es sich um Zufallszahlen handelt – zumal vereinzelte dieser Zufallszahlen gezielt mehrfach vorkommen.

[1)] Dies ist schon im Programm DEMO – VERSCHLUESSELUNG ersichtlich: Immer wenn dieses neu geöffnet wird, erscheint im Register ALS MAIL VERSENDEN ein anderes Zahlenbild. Wird dieses direkt kopiert und – statt des MUSTERTEXTES – unter MAIL – EMPFANG EINSETZEN eingefügt, erscheint in ENTSCHLÜSSELUNG trotzdem stets der gleiche, schreibgeschützte Text: Also lediglich ein «W». Wird jedoch der zur Verfügung gestelllte MUSTERTEXT in MAIL – EMPFANG EINSETZEN eingefügt, folgt in ENTSCHLÜSSELUNG die anschauungshalber versandte Meldung.

Weitere praktische, das heisst, vom Programm – Algorithmus unabhängige Erschwernisse gegen eine Entschlüsselung können darin bestehen, dass der zu verschlüsselnde Text nicht am Anfang, sondern irgendwo im Textfeld abgesetzt wird. Oder, dass die zu versendende Excel - Verschlüsselungstabelle mit unverfänglichem Text erweitert, der Zahlenschlüssel dagegen mittels «weisser Zahlen» unsichtbar gemacht wird.

Unter all diesen Gesichtspunkten ist eine sehr hohe Sicherheit vor unerlaubter Entschlüsselung gewährleistet!

14. Juni 2018 / Ba