# Illustration aktueller kryptografischer Verfahren

Das einzige, absolut sichere Verfahren One Time Pad hat die Nachteile, das Schlüssellänge und Klartextlänge identisch sein müssen, der Schlüssel nur einmal benutzt werden darf und er aus einer zufälligen Buchstabenfolgen bestehen muss. Wenn man aber bei einem Internet-Versandhändler erstmalig bestellt und dort die Bankdaten hinterlegen möchte, sollte dies verschlüsselt geschehen. Ein **gemeinsamer** Schlüssel existiert aber nicht! Gesucht ist also ein Verfahren, das trotzdem eine sichere Kommunikation ermöglicht.

**Versuch mit dem Werkzeug ASYM-Kodierer (aus Gallenbacher: Abenteuer Informatik):**

Behauptung: Mit dem Schlüssel AZS wurde EC-CARD zu JVQFQUH verschlüsselt.

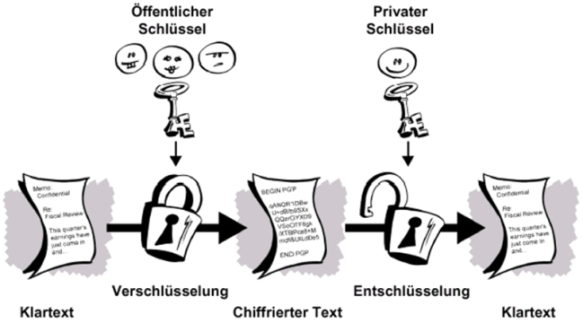
1. Prüfen die Aussage durch Verschlüsseln des Klartextes/Entschlüsseln des Geheimtextes Vergleiche mit dem Partner.

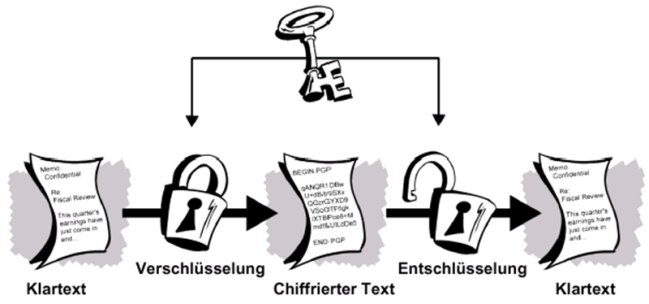
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Verschlüsseln | | | | | | | |  | Entschlüsseln | | | | | | | |
| Schlüssel | A | Z | S | A | Z | S | A |  | Schlüssel | A | Z | S | A | Z | S | A |
| Klartext | E | C | - | C | A | R | D |  | Geheimtext | J | V | Q | F | Q | U | H |
| Geheimtext |  |  |  |  |  |  |  |  | Klartext |  |  |  |  |  |  |  |

1. Nutzen nun den Schlüssel PXB. Prüfe erneut die Aussage und vergleiche mit dem Partner.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Verschlüsseln | | | | | | | |  | Entschlüsseln | | | | | | | |
| Schlüssel | P | C | T | P | C | T | P |  | Schlüssel | P | C | T | P | C | T | P |
| Klartext | E | C | - | C | A | R | D |  | Geheimtext | J | V | Q | F | Q | U | H |
| Geheimtext |  |  |  |  |  |  |  |  | Klartext |  |  |  |  |  |  |  |

1. Beschreibe das Vorgehen zum korrekten Ver- und Entschlüsseln.

Für das Ver- und Entschlüsseln werden **verschiedene** Schlüssel benutzt. Man bezeichnet das Prinzip als asymmetrisches Verfahren oder auch Public-Key-Verfahren, die Schlüssel als privat und öffentlich. Der private Schlüssel ist geheim und nur seinem Besitzer bekannt. Der öffentliche Schlüssel wird vom Besitzer z. B. im Internet bekannt gegeben. Beide Schlüssel werden so berechnet, dass aus einem Teil nicht der andere ermittelt werden kann. Die Regeln zur Schlüsselbestimmung und Anwendung sind komplexe mathematische Verfahren unter Benutzung riesiger Primzahlen und zahlentheoretischer Sätze, die ggf. Schüler abschrecken könnten. Daher werden die Möglichkeiten des Verfahrens weiter mit dem ASYM-Kodierer untersucht.



Quelle: Network Associates Inc. (Hrsg.): Handbuch “Einführung in die Kryptographie“, Bestandteil des Softwarepaketes PGP Ver. 6.5.1. deutsch, Datei „IntroToCrypto.pdf“.

1. Public-Key im Einsatz I: Die Nutzerin Alice möchte bei der Bob AG über das Internet erstmalig eine Bestellung auslösen und dazu ihre Kreditkartennummer 81 verschlüsselt übermitteln.   
   Trage auf den waagerechten Pfeilen die Kommunikationsdaten ein.   
   Ergänze die Ver- und Entschlüsselung.

|  |  |  |
| --- | --- | --- |
| **C:\Users\T.Hempel\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\DIC9QL3S\MC900432626[1].pngAlice** |  | **C:\Users\T.Hempel\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\OM80E61J\MC900339150[1].wmfBob AG**  **public key: BGF**  **private key: FDB** |
| Frage Bob AG nach öffentlichem Schlüssel! | Wie lautet Ihr öffentlicher Schlüssel? | Antworte mit dem public key! |
| public key Bob AG:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Verschlüssle ACHTEINS und übertrage es! |  |
|  | Entschlüssle!  Ergebnis: \_\_\_\_\_\_\_\_\_\_\_\_  Verschlüssle OK mit private key:  Ergebnis: \_\_\_\_\_\_\_\_\_\_\_  Sende OK und verschlüsseltes OK! |
|  |  |
|  |  |
| Entschlüssle zweites Wort  Ergebnis: \_\_\_\_\_\_\_\_\_\_\_\_\_  Prüfe, ob Wort 1 = Wort 2 |  |  |

Die Kommunikation zeigt **zwei grundlegende Prinzipen** des asymmetrischen Verfahrens. Neben der **Ver-/Entschlüsselung** ist es möglich, **Nachrichten** digital zu **unterschreiben**. Dazu wird die Nachricht mit dem eigenen privaten Schlüssel verschlüsselt und dieser Geheimtext zusammen mit der Nachricht übermittelt. Jeder kann nun den verschlüsselten Teil der Nachricht mit dem öffentlichen Schlüssel des Absenders decodieren, mit der Ausgangsnachricht verifizieren und so prüfen, ob die Nachricht auch von ihm stammt.

Das bisherige Verfahren hat aber einen großen Nachteil: die Übermittlung des öffentlichen Schlüssels kann vielfältig manipuliert werden. Gelöst werden kann dies mit Hilfe von Zertifizierungsstellen, sog. Trust Center. Diese geben jedem Kommunikationsteilnehmer den öffentlichen Schlüssel des Trust Centers als Zertifikat in die Hand (z. B. über die Browser des Betriebssystems). Außerdem verwalten sie gegen Gebühr die öffentlichen Schlüssel anderer Teilnehmer. Dazu müssen sich diese persönlich im Trust Center vorstellen und authentifizieren.

1. **C:\Users\T.Hempel\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\C9PXVU82\MC900290706[1].wmf**Public-Key im Einsatz II: Die Nutzerin Alice möchte nun den öffentlichen Schlüssel der Bob AG vom Trust Center erhalten. Ihr Browser/Ihr E-Mail-Programm hat den öffentlichen Schlüssel des Trust Centers fest gespeichert.   
   Vollziehe die Kommunikation nach.   
   Trage auf den waagerechten Pfeilen die Kommunikationsdaten ein.

|  |  |  |
| --- | --- | --- |
| **Alice**  **public key TC: SLDWY** |  | **Trust Center (TC)**  **public key TC: SLDWY**  **private key TC: TEG-V**  **public key Bob AG: BGF** |
| Frage Trust Center nach öffentlichem Schlüssel von Bob AG! | Wie lautet der öffentliche Schlüssel der Bob AG? | Verschlüssle den public key Bob AG mit private key! Ergebnis: \_\_\_\_\_\_\_\_\_\_\_\_\_  Sende „public key Bob AG:“, public key Bob AG und Signatur! |
|  |  |
| Prüfe Signatur!  Extrahiere public key Bob AG!  Ergebnis: \_\_\_\_\_\_\_\_\_\_\_\_\_ |  |  |

Das Trust Center signiert die zu übertragenden Schlüssel stets mit dem eigenen privaten Schlüssel. Außerdem wird mit dem öffentlichen Schlüssel auch der Inhaber genannt. Dadurch ist eine Manipulation kaum noch möglich. Man sieht aber, dass die Kommunikation vom Kunden zum Anbieter stets verschlüsselt aber nicht signiert (authentifiziert), vom Anbieter zum Kunden stets unverschlüsselt, aber signiert verläuft.

Die im Browser gespeicherten öffentlichen Schlüssel (sog. Zertifikate) des Trust Center kann man sich in den Browsereinstellungen übrigens auch anzeigen lassen.

# Lösung

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Verschlüsseln | | | | | | | |  | Entschlüsseln | | | | | | | |
| Geheimtext | J | V | Q | F | Q | U | H | ✔ 🗙 | Klartext | T | Z | O | L | . | J | P |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Verschlüsseln | | | | | | | |  | Entschlüsseln | | | | | | | |
| Geheimtext | Q | G | S | P | L | C | B | 🗙 ✔ | Klartext | E | C | - | C | A | R | D |

1. Beschreibe das Vorgehen zum korrekten Ver- und Entschlüsseln. 🡪 Siehe nachfolgender Text!

|  |  |  |
| --- | --- | --- |
| **C:\Users\T.Hempel\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\DIC9QL3S\MC900432626[1].pngAlice** |  | **C:\Users\T.Hempel\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\OM80E61J\MC900339150[1].wmfBob AG**  **public key: BGF**  **private key: FDB** |
| Frage Bob AG nach öffentlichem Schlüssel! | Wie lautet Ihr öffentlicher Schlüssel? | Antworte mit dem public key! |
| public key Bob AG:  BGF  Verschlüssle ACHTEINS und übertrage es! | BGF lautet der öffentliche Schlüssel! |
| TYLWC.SW | Entschlüssle!  Ergebnis: ACHTEINS  Verschlüssle OK mit private key:  Ergebnis: H.  Sende OK und verschlüsseltes H.! |
| TYLWC.SW |  |
|  | OK H. |
| Entschlüssle zweites Wort  Ergebnis: OK  Prüfe, ob Wort 1 = Wort 2 | ✔ |  |

1. ****

|  |  |  |
| --- | --- | --- |
| **Alice**  **public key TC: SLDWY** |  | **C:\Users\T.Hempel\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\C9PXVU82\MC900290706[1].wmfTrust Center (TC)**  **public key: SLDWY**  **private key: TEG-V**  **public key Bob AG: BGF** |
| Frage Trust Center nach öffentlichem Schlüssel von Bob AG! | Wie lautet der öffentliche Schlüssel der Bob AG? | Verschlüssle den public key Bob AG mit private key! Ergebnis:  Sende „public key Bob-AG.public key Bob AG und Signatur! |
|  | Bob-AG. BGF JMGKKFCGEH |
| Prüfe Signatur!  Extrahiere public key Bob AG!  Ergebnis: BOB-AG.BGF = BOB-AG.BGF | ✔ |  |