7 Chiffriersicherheit

7.1 Chiffrierfehler

- Verwendung unsicherer Kommunikationswege und Kryptographie, wenn sichere Kommunikationswege verfügbar sind ("Funken ist Landesverrat")
- Verschlüsselung der gleichen Nachricht mit verschiedenen Schlüsseln (z.B. für verschiedene Empfänger) $\Rightarrow$ Geheimtext-Geheimtext-Kompromittierung
- zusätzlich unverschlüsselte Übertragung $\Rightarrow$ Klartext-Geheimtext-Kompromittierung, erlaubt Rekonstruktion von Schlüsseln/Verfahren
- Verschlüsselung vom Angreifer gewählter (untergeschobener) Texte $\Rightarrow$ Klartext-Geheimtext-Kompromittierung, Chosen-Plaintext-Attack
- Verwendung von Standardfloskeln und stereotypen Begriffen $\Rightarrow$ Methode des wahrscheinlichen Wortes

7.2 Maximen der Kryptologie

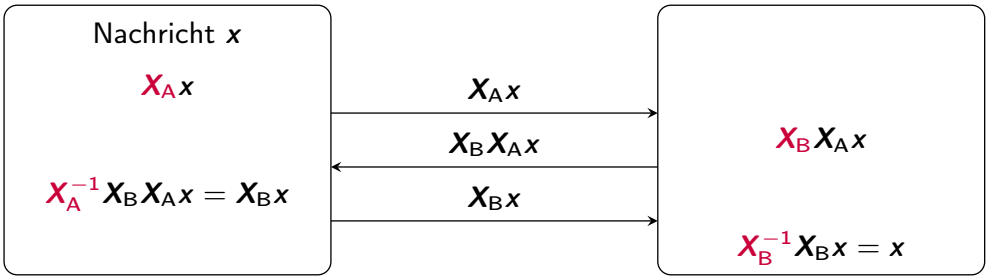
- Man soll den Gegner nicht unterschätzen.
- Nur der Kryptanalytiker, wenn überhaupt jemand, kann die Sicherheit eines Chiffrierverfahrens beurteilen.
- Bei der Beurteilung der kryptanalytischen Sicherheit eines Verfahrens muss man damit rechnen, dass dem Gegner die Verfahrensklasse bekannt ist.
- Äußerliche Komplikationen können illusorisch sein; sie gaukeln dem Kryptologen eine trügerische Sicherheit vor.
- Bei der Beurteilung der kryptanalytischen Sicherheit eines Verfahrens sind Chiffrierfehler und andere Verstöße gegen die Chiffrierdisziplin mit einzubeziehen.

7.3 Unizitätslänge

- ein Chiffrierverfahren sei über Z verschiedene Schlüssel parametrierbar
- also könnte ein Geheimtext zu (höchstens) Z verschiedenen Klartexten entschlüsselt werden – wie viele davon sind sinnvoll?
- bzw. falls Länge des Klartextes k eindeutig: wie groß muss k werden, damit Entschlüsselung eindeutig? $\Rightarrow$ Unizitätslänge U
- Anzahl sinnvoller Texte der Länge k ungefähr $2{,}3^k$
- Wahrscheinlichkeit, dass zufälliger Text der Länge k sinnvoll: $\frac{2{,}3^k}{26^k} = \left(\frac{2{,}3}{26}\right)^k$
- Anzahl falscher, aber sinnvoller Texte der Länge k, die durch Entschlüsselung eines Geheimtextes mit Z verschiedenen Schlüsseln zu erwarten sind: $\left(\frac{2{,}3}{26}\right)^k \cdot (Z-1) \approx \left(\frac{2{,}3}{26}\right)^k \cdot Z$
- Entschlüsselung vermutlich eindeutig, wenn $\left(\frac{2{,}3}{26}\right)^k \cdot Z < 1$, also $k > \frac{\operatorname{ld} Z}{\operatorname{ld} 26 - \operatorname{ld} 2{,}3} \approx 0{,}29 \operatorname{ld} Z$
- Für VIGENÈRE der Periode d: $\operatorname{ld} Z = \operatorname{ld} 26^d = d \operatorname{ld} 26$, also $U \approx 1{,}34 \cdot d \Rightarrow$ ist der Schlüssel kürzer als $\frac{1}{1{,}34} \approx 74\,\%$ des Textes eindeutig entschlüsselbar!?
  - Betrachtung zu sehr vereinfacht: Textteil mit nicht-wiederholtem Schlüssel vermutlich uneindeutig, Textteil mit wiederholtem Schlüssel überbestimmt
  - aber spätestens ab $k = 2 \cdot d$ eindeutig

8 Schlüsselaustausch und öffentliche Schlüssel

- Chiffriersicherheit erfordert lange, häufig wechselnde Schlüssel
- Schlüsselverteilung ist gravierendes praktisches Problem
- es geht auch ohne vorherigen sicheren Schlüsselaustausch!
- naiver Ansatz: seien $\boldsymbol{X}_\mathrm{A}, \boldsymbol{X}_\mathrm{B}$ kommutative Verschlüsselungsverfahren, d.h. $\boldsymbol{X}_\mathrm{A}\boldsymbol{X}_\mathrm{B} = \boldsymbol{X}_\mathrm{B}\boldsymbol{X}_\mathrm{A}$



Problem: Klartext-Geheimtext-Kompromittierung von $\boldsymbol{X}_\mathrm{A}$ und $\boldsymbol{X}_\mathrm{B}$
Beispiel VIGENÈRE $\boldsymbol{X}_\mathrm{A}x = x + \boldsymbol{t}_\mathrm{A}, \boldsymbol{X}_\mathrm{B}x = x + \boldsymbol{t}_\mathrm{B}$:

$$\boldsymbol{X}_\mathrm{B}^{-1}\boldsymbol{X}_\mathrm{A}^{-1}\boldsymbol{X}_\mathrm{B}\boldsymbol{X}_\mathrm{A}x = x$$

aber auch

$$\boldsymbol{X}_\mathrm{A}x - \boldsymbol{X}_\mathrm{B}\boldsymbol{X}_\mathrm{A}x + \boldsymbol{X}_\mathrm{B}x = x$$