3. CRITTOANALISI

La ***crittoanalisi*** è lo studio della sicurezza dei sistemi senza avere accesso all'informazione segreta; per i cifrari, essa è finalizzata ad avere accesso sia alla chiave segreta sia al messaggio in chiaro. Questa tecnica, in genere, è usata oggi sui cifrari simmetrici.

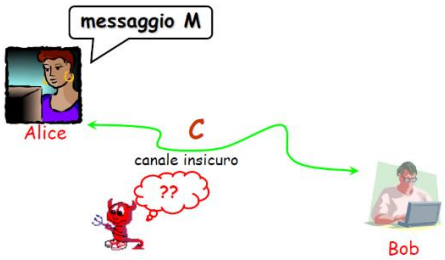
Il ***principio di Kerckhoffs*** afferma che la sicurezza di un crittosistema deve dipendere solo dalla segretezza della chiave e non dalla segretezza dell'algoritmo usato. Infatti, i sistemi crittografici odierni sono contraddistinti da implementazioni open-source, e la sicurezza che un loro impiego porta ad un sistema informatico non dipende da questo aspetto.

Si possono utilizzare diverse tecniche di attacco:

- con il ***Known Ciphertext Attack*** (letteralmente "attacco con testo cifrato conosciuto", COA) l'attaccante ha accesso solo ad un insieme di testo cifrato, ed ha comunque minima conoscenza del plain text per la cifratura. Spesso, questo tipo di attacco è basato su analisi di eventuali ripetizioni nel messaggio, per cui è particolarmente indicato per cifrari a sostituzione;

L'avversario conosce solo il testo cifrato

- con il ***Known Plaintext Attack*** (letteralmente "attacco con testo piano conosciuto", KPA) l'attaccante ha accesso sia al plain text sia alla sua versione crittata;

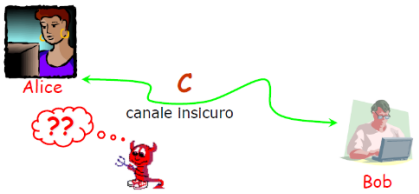


L'avversario conosce anche il testo in chiaro

- con il ***Chosen Plaintext Attack*** (letteralmente "attacco con testo piano scelto", CPA) l'attaccante può scegliere un testo piano da crittografare in modo casuale ed ottenere il testo cifrato corrispondente. Nel caso peggiore, un tale attacco potrebbe esporre informazioni segrete dopo il calcolo della chiave segreta;

L'avversario può ottenere la cifratura di testi in chiaro di sua scelta

- con il ***Chosen Ciphertext Attack*** (letteralmente "attacco con testo cifrato scelto", CCA) l'attaccante raccoglie informazioni su un sistema crittografico scegliendo un testo cifrato ed ottenendo la sua versione decifrata con una chiave non nota. L'attaccante conosce sia il testo in chiaro che il testo cifrato.



L'avversario può ottenere la decifratura di testi cifrati di sua scelta

Per attaccare il cifrario di Hill, si suppone di utilizzare il ***Known Plaintext Attack***. Supponiamo di conoscere: (P_1, C_1) dove $C_1 = K \times P_1$, …, (P_m, C_m) dove $C_m = K \times P_m$. La chiave K è una matrice m·m.

Sia "PQCFKU" la ***cifratura Hill*** di "FRIDAY" per m=2: "FR" = (5, 17) → "PQ" = (15, 16), mentre "ID" = (8, 3) → "CF" = (2, 5); in particolare, abbiamo che $\begin{pmatrix}15\\16\end{pmatrix} = K \begin{pmatrix}5\\17\end{pmatrix} \bmod 26$, e $\begin{pmatrix}2\\5\end{pmatrix} = K \begin{pmatrix}8\\3\end{pmatrix} \bmod 26$. Siccome la chiave K è una matrice m·m, si considerino le matrici $X = p_{ij}$, dove ogni riga ha uno dei testi in chiaro, e $Y = c_{ij}$, dove ogni riga ha uno dei testi cifrati. Si ha che $Y = K \cdot X$. Di conseguenza, $K = Y \cdot X^{-1}$.

Per i testi in precedenza, si ha che $Y = \begin{pmatrix}15 & 2\\16 & 5\end{pmatrix} = K \cdot X \bmod 26 = K \begin{pmatrix}5 & 8\\17 & 3\end{pmatrix} \bmod 26$; quindi:

$X^{-1} = \begin{pmatrix}9 & 2\\1 & 15\end{pmatrix}$ implica che $K = Y \cdot X^{-1} = \begin{pmatrix}7 & 8\\19 & 3\end{pmatrix}$. Se X non è invertibile, allora occorrono altre coppie (P_i, C_i) fino ad avere X invertibile.

Per attaccare il ***cifrario di Vigenère***, si suppone di utilizzare il ***Known Ciphertext Attack***. Si vuole determinare la lunghezza t della chiave, con il ***Tesk di Kasiski*** basato sullo studio delle ripetizioni, sviluppato da Friedrich Kasiski (1863). Si può dividere il testo cifrato in t sottotesti, dove ogni sottotesto corrisponde ad un cifrario con shift. Di conseguenza, si effettua l'analisi delle frequenze per ognuno dei sottotesti.
Ad esempio, dato il testo cifrato "…WPI**XFG**HDAFNVTV…KL**XFG**LQ", il crittoanalista notò che ci sono più occorrenze di "XFG", per cui ebbe l'idea secondo cui questa sottostringa potrebbe cifrare lo stesso testo in chiaro. A tal proposito, siano $d_1, d_2, \ldots, d_h$ le distanze tra le "X" di "XFG"; allora, il $\gcd(d_1, d_2, \ldots, d_h)$ è un multiplo di t. Su questa base, sviluppò questa tecnica e riuscì a rompere il sistema.