NUMBER STATION
CODICE “VERNAM”
(Domenico IU7OXM)

[SECONDA PARTE]

Il **codice Vernam**, noto anche come “cifratura a chiave univoca” o “one-time pad (OTP)”, è un metodo di crittografia che fornisce la massima sicurezza quando utilizzato correttamente. È stato sviluppato all'inizio del XX secolo e prende il nome da Gilbert Vernam, che lavorò su di esso negli anni 1910. Ecco un'analisi dettagliata del codice Vernam, comprensivo di storia, funzionamento, sicurezza e applicazioni.

Origini:
- Il concetto alla base della cifratura a chiave univoca risale a prima della Prima Guerra Mondiale. Tuttavia, il metodo fu formalmente descritto da Vernam nel 1917.
- La cifratura è stata successivamente sviluppata da militari e agenzie di intelligence per garantire comunicazioni sicure.

Sviluppo:
- L’idea di base si basa sull’uso di una chiave di cifratura che è tanto lunga quanto il messaggio stesso e utilizzata solo una volta.

Generazione della Chiave:
- La chiave utilizzata nel codice Vernam deve essere una serie di lettere o numeri completamente casuali. Per ogni lettera o numero del messaggio originale, si utilizza il corrispondente carattere della chiave per la cifratura.

Processo di Cifratura:
- La cifratura viene eseguita utilizzando l'operazione di somma a modulo. Se utilizziamo l'alfabeto (ad esempio A=0, B=1, ..., Z=25), l'operazione di cifratura per ciascun carattere del messaggio può così essere espressa:
C_i = (P_i + K_i) \mod 26
dove:
- C_i è il carattere cifrato,
- P_i è il carattere del messaggio originale,
- K_i è il carattere della chiave.

Processo di Decifratura:
- La decifratura avviene in modo simile, ma si utilizza la sottrazione:
P_i = (C_i - K_i) \mod 26

Sicurezza
- Se il codice Vernam è utilizzato correttamente – cioè se la chiave è veramente casuale, lunga quanto il messaggio e utilizzata solo una volta – è considerato "inviolabile". Questo perché non ci sono schemi o ripetizioni che l'attaccante possa sfruttare.
Problemi nella Pratica:
- In pratica, la generazione, la distribuzione e la gestione delle chiavi rappresentano sfide significative. Se la chiave viene riutilizzata o se non è casuale, la sicurezza del sistema viene

compromessa.
Attacchi Indiretti:
- Se un attaccante riesce a intercettare sia il messaggio cifrato che la chiave, può facilmente decifrare il messaggio. Pertanto, è essenziale garantire anche la sicurezza della chiave.

Applicazioni
Uso Militare:
- Storicamente, le forze armate e le agenzie di intelligence hanno utilizzato la cifratura a chiave univoca per comunicazioni particolarmente sensibili, dove è necessaria la massima riservatezza.

Telecomunicazioni:
- Il codice Vernam ha avuto un'importanza limitata nelle telecomunicazioni moderne a causa delle sfide nella gestione della chiave. Tuttavia, il concetto di base ha influenzato lo sviluppo di metodi crittografici più complessi e pratici.

Crittografia Quantistica:
- Le idee alla base del codice Vernam sono state incorporate in tecnologie moderne come la crittografia quantistica, che mira a migliorare ulteriormente la sicurezza nella comunicazione.

Conclusione
Il codice Vernam rappresenta uno dei metodi di cifratura più sicuri mai concepiti, sebbene sia difficile da implementare in modo pratico. La sua importanza nella storia della crittografia e nel campo della sicurezza informatica resta significativa. La conoscenza del codice Vernam è fondamentale per comprendere i fondamenti della crittografia moderna e l'evoluzione dei sistemi di sicurezza delle informazioni.