Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea Triennale in Matematica

VERNAM E SHANNON LA CRITTOGRAFIA DA ARTE A SCIENZA

Relatore:
Chiar.mo Prof.
DAVIDE ALIFFI

Presentata da:
STEFANO CORNACCHIA

Sessione I
Anno Accademico 2019/2020

"Ai miei genitori, a mio fratello, a mia cognata, alla mia nipotina, a tutti i miei amici, ai miei studenti e a tutti coloro che inseguono i propri sogni."

Indice

Introduzione

La storia della crittografia ha origini remote ed inizia con la crittografia classica, con metodi di cifratura che utilizzavano carta e penna o, al massimo, semplici supporti meccanici.
Il più antico esempio di utilizzo della crittografia è stato rinvenuto in alcuni geroglifici egiziani scolpiti in antichi monumenti dell'Antico Regno, risalenti a più di 4500 anni fa. Anche se non si possono considerare come seri esempi di comunicazioni segrete, sono da considerare come tentativi di scritture misteriose, intriganti o stravaganti fatti da letterati del tempo.
Ci sono anche altri esempi di utilizzo della crittografia: su alcune tavolette di argilla mesopotamiche sono state trovate incisioni cifrate chiaramente fatte con l'intento di proteggere le informazioni riportate, forse ricette con un qualche valore commerciale.
I Romani conoscevano certamente la crittografia: l'esempio più noto è il *cifrario di Cesare*, un cifrario monoalfabetico.
Furono probabilmente motivi religiosi inerenti all'analisi testuale del Corano che portarono all'invenzione della tecnica dell'*analisi delle frequenze* per violare i cifrari a sostituzione monoalfabetica intorno al IX secolo. Questa fu, fino alla seconda guerra mondiale, la più importante tappa della crittanalisi: fino all'avvento del cifrario polialfabetico di Alberti nel 1495 circa, tutti i cifrari erano vulnerabili a questa tecnica crittanalitica.
Anche se il cifrario di Alberti è spesso indicato come il padre dei cifrari polialfabetici, sembra però che già 500 anni prima di lui gli Arabi avessero conoscenze di questo tipo di cifrario, stando ad alcuni manoscritti di Al-Kindi recentemente scoperti.
In Europa la crittografia divenne molto importante come conseguenze della competizione politica e della rivoluzione religiosa. A partire dal Rinascimento, molti matematici e studiosi di diversi stati Italiani furono responsabili di una rapida proliferazione di tecniche crittografiche, alcune delle quali riflettevano la conoscenza e la comprensione degli studi del cifrario di Alberti sulle tecniche di sostituzione polialfabetiche.
"Cifrari avanzati" comparsi dopo quello di Alberti, non erano così avanzati come i loro inventori o utilizzatori volevano far credere: essi venivano regolarmente violati.
Al di fuori dell'Europa, dopo la fine dell'epoca d'oro del mondo arabo, la crittografia rimase senza uno sviluppo costante.
In Giappone la crittografia fa la sua comparsa solo nel 1510, e tecniche avanzate di

crittografia non saranno note fino all'apertura del Paese al mondo occidentale avvenuta nel 1860.
Durante gli anni venti ufficiali polacchi furono chiamati dall'esercito giapponese a fornire conoscenze ed assistenza per lo sviluppo di codici e sistemi cifrati.
Anche se la crittografia ha una storia lunga e complessa, fino al XIX secolo essa non sviluppò niente più che approcci sia alla cifratura sia alla crittanalisi.
La comprensione della crittografia a quel tempo in genere consisteva di piccole conquiste fatte a costo di notevoli sforzi: la crittografia era considerata una vera e propria arte.
Un altro cifrario importante nella storia della crittografia era il *cifrario di Vigenère*, pubblicato nel 1586.
Il cifrario di Vigenère, il più semplice dei cifrari polialfabetici, fu ritenuto per secoli inattaccabile, godendo di una fama in buona parte immeritata essendo molto più debole di altri cifrari polialfabetici precedenti, quali il cifrario di Alberti.
Questa sua fama è durata per molti anni anche dopo la scoperta del primo metodo di crittanalisi da parte di Charles Babbage, e la successiva formalizzazione da parte del colonnello prussiano Friedrich Kasiski: il Metodo Kasiski del 1863.
In quello stesso anno, Kasiski pubblicò un primo metodo di decrittazione; in seguito si sono trovati diversi altri efficienti metodi per forzare questo cifrario. In realtà il cifrario di Vigenère fu già forzato da Charles Babbage, ma i risultati della sua ricerca non furono mai pubblicati.
Il metodo è una generalizzazione del cifrario di Cesare e il vantaggio rispetto ai cifrari monoalfabetici è evidente: il testo è cifrato con n alfabeti cifranti. In questo modo, la stessa lettera viene cifrata, se ripetuta consecutivamente, n volte; ciò rende quindi più complessa la crittoanalisi del testo cifrato. Tuttavia anche il cifrario di Vigenère non era inviolabile.
La debolezza del Vigenère sta nell'essere, di fatto, un insieme di n cifrari di Cesare, dove n è la lunghezza della chiave; se il crittoanalista riesce a determinare la lunghezza della chiave (in questo caso, n) la decrittazione diventa molto semplice.
Fino agli inizi del Novecento nessun cifrario era dunque considerato inviolabile.
Tuttavia Vernam, partendo da una ennesima reinvenzione del cifrario di Vigenère, arrivò poi negli anni venti ad ideare l'ormai noto *cifrario di Vernam* e Claude Shannon nel 1949 portò una dimostrazione matematica, provando che questo cifrario sia teoricamente inattaccabile. Prenderà anche il nome di *cifrario perfetto*.
Ecco che da questo momento la crittografia cessa di essere solo un'arte per diventare una scienza.

Capitolo 1

Vernam e la sua idea

Il seguente capitolo è suddiviso in due paragrafi.
Nel primo verrà raccontata la storia di Vernam, di come ha ideato e realizzato quello che oggi è noto come "Cifrario di Vernam".
Nel secondo verrà descritto il funzionamento tecnico del "Cifrario di Vernam".

1.1 Il cifrario di Vernam

Gilbert Sandford Vernam (1890-1960), laureato al Massachusetts College, fu un ingegnere statunitense delle *American Telephone and Telegraph Company*.

Figura 1.1: Vernam in giovane età

Si unì alla *American Telephone and Telegraph Company* nel 1914, lavorando nella sezione telegrafica del dipartimento di ricerca e sviluppo dell'azienda. Questa sezione, composta da alcuni dei più brillanti ingegneri dell'azienda, si concentrava sui più recenti sviluppi nel campo della telegrafia a stampa diretta.

Lo strumento utilizzato in questa sezione era la telescrivente, un dispositivo elettromeccanico per trasmettere messaggi di testo attraverso la rete telegrafica. I modelli più recenti sono interamente elettronici e visualizzano il testo su un monitor invece di stamparlo.

Figura 1.2: Una telescrivente di quell'epoca

Lavorò così bene nella sezione telegrafica che venne assegnato a uno speciale progetto di segretezza.
Il progetto iniziò durante l'estate del 1917, pochi mesi dopo che era stata dichiarata la guerra. Consisteva nell'indagare sulla sicurezza della comunicazione tramite il metodo della telegrafia a stampa diretta.
Il gruppo di segretezza scoprì che, anche se il nemico non avesse avuto gli stessi loro mezzi, i messaggi sarebbero stati decifrati in ogni caso. Le fluttuazioni della corrente sulla linea telegrafica potevano essere registrate da un oscillografo e i messaggi letti con facilità.
Persino l'invio di più messaggi contemporaneamente in entrambe le direzioni su un singolo filo non offriva alcuna sicurezza reale.
Durante le loro varie prove gli ingegneri riuscirono a risolvere le oscillazioni nelle loro curve costitutive e leggere così i messaggi.
Il gruppo pensò allora di codificare una lettera in un'altra per mezzo di una sostituzione monoalfabetica. Tuttavia gli ingegneri si resero conto che ciò non offriva alcun vero segreto.
A quel punto Vernam si schierò con la sua idea.
Propose la costruzione di una telescrivente a cifre in cui una chiave determinata precedentemente, fornita attraverso un nastro perforato, viene combinata carattere per carattere con un messaggio di riferimento per costruire il corrispondente testo cifrato. Per decifrare il testo cifrato, deve essere utilizzata ancora la chiave combinandola carattere per carattere, in modo da riottenere il testo di riferimento.
Il nastro perforato è un sottile nastro di carta flessibile utilizzato per memorizzare informazioni sotto forma di perforazioni (fori) praticate longitudinalmente in posizioni

predeterminate (piste) ad intervalli regolari.

Figura 1.3: Un rotolo di nastro perforato da una telescrivente

La telescrivente avrebbe utilizzato il codice Baudot, codice che prende il nome dal suo inventore francese Emile Baudot.
Secondo il codice di Baudot, inventato nel 1870, ogni lettera è rappresentata da 5 bit, 0 o 1, che indicano la presenza o assenza di un impulso elettrico.
In totale si hanno $2^5 = 32$ combinazioni possibili, 26 per le lettere dell'alfabeto e le 6 rimanenti per comandi speciali come $\{cr\}$ che sta per *carriage return* (ritorno carrello) o $\{lf\}$ = *line feed* (avanzamento linea).
Diversi cifrari nati tra le due guerre mondiali furono esplicitamente progettati in funzione del codice Baudot e così fu per il cifrario di Vernam.
Quindi Vernam ideò la costruzione di un dispositivo, in grado di leggere, contemporaneamente, due nastri d'ingresso e produrre, a partire da questi, un nastro di uscita, tale che ciascun foro, fosse generato mediante un'operazione XOR, operazione definita meglio nel paragrafo seguente, dei corrispondenti due fori sui nastri d'ingresso. In ciascuna posizione del nastro di uscita, viene praticato un foro se e solo se le corrispondenti posizioni, nei 2 nastri d'ingresso, sono differenti fra loro, ovvero una ha un foro e l'altra no; nessun foro in caso contrario, cioè le posizioni originali sono entrambe forate o entrambe non forate.
Il funzionamento è dunque il seguente.
Si prende un nastro, su cui è perforata una sequenza casuale di caratteri, lunga almeno quanto il testo che si intende cifrare e lo si inserisce sul primo lettore, mentre il nastro, su cui è perforato il testo in chiaro, va nel secondo lettore, attivando la macchina, e si ottiene così un nuovo nastro, completamente inintelligibile, ovvero il messaggio cifrato.
Per decifrare, si utilizzava la stessa macchina, inserendo in input i nastri contenenti, rispettivamente, il cifrato e la chiave.
Effettuando la stessa operazione svolta per la cifratura, con la stessa chiave, si ottiene sul nastro di output, il testo in chiaro.
Grazie all'idea di Vernam non era più necessario crittografare o decifrare un messaggio in una fase separata.
I messaggi venivano crittografati, trasmessi, ricevuti e decifrati in un'unica operazione.

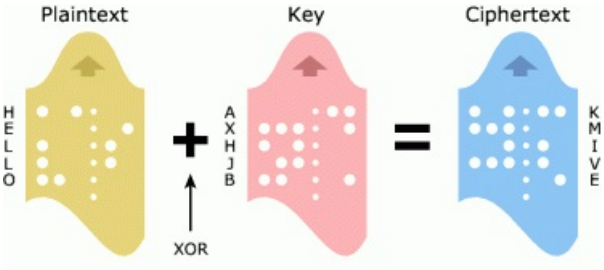

Figura 1.4: Processo di cifratura del nastro perforato

Il testo in chiaro veniva spedito e ricevuto e chiunque avesse intercettato il messaggio, avrebbe raccolto nient'altro che una sequenza incomprensibile di segnali.
Vernam creò quella che fu chiamata "codifica on-line", perché avveniva direttamente sul circuito telegrafico aperto, per distinguerla dalla vecchia "codifica off-line" separata.
Ha eliminato la presenza di una persona in più, l'impiegato della crittografia, dalla catena della comunicazione.
Il suo grande contributo è stato quello di aver automatizzato la crittografia, cosa di cui l'umanità ha beneficiato in tanti settori di attività.
L'idea di Vernam ha rapidamente dato il via a una raffica di attività.
Nel marzo del 1918 la *Western Electric Company*, la filiale di produzione delle *American Telephone and Telegraph Company*, iniziò a costruire un paio di dispositivi Vernam, utilizzando il maggior numero possibile di parti standard. Li collegarono a due telescriventi e, nel laboratorio di Western Electric, eseguirono i primi test di quella che gli ingegneri chiamavano "crittografia automatica". I dispositivi funzionarono.
Rimaneva il problema delle chiavi.
Gli ingegneri, che stavano rapidamente imparando a conoscere la crittografia, probabilmente da un manuale del 1916, scoprirono presto il difetto.
Il sistema di Vernam è polialfabetico. A differenza di un cifrario monoalfabetico che utilizza sostituzioni fisse sull'intero messaggio, quello di Vernam usa differenti schemi di sostituzione ed ogni lettera del testo in chiaro è trattata con un differente alfabeto secondo uno schema stabilito dalla chiave segreta.
Una tabella 32x32 può essere impostata con i 32 caratteri dell'alfabeto Baudot in alto come testo in chiaro e in basso come chiave. Poiché l'alfabeto Baudot è un'informazione pubblica, la composizione degli alfabeti a 32 cifre che riempiono la tabella sarebbe nota. La segretezza nel sistema di Vernam risiede quindi interamente nelle sue chiavi.
Nei primi tempi le chiavi avevano la forma di un ciclo di nastro di carta perforato con sequenze di 0,1 casuali; quindi ogni chiave passava attraverso la macchina ad intervalli regolari, permettendo all'avversario di trovare la chiave con l'analisi delle frequenze del metodo Kasiski.
Gli ingegneri provarono a risolvere questo problema rendendo la chiave estremamente

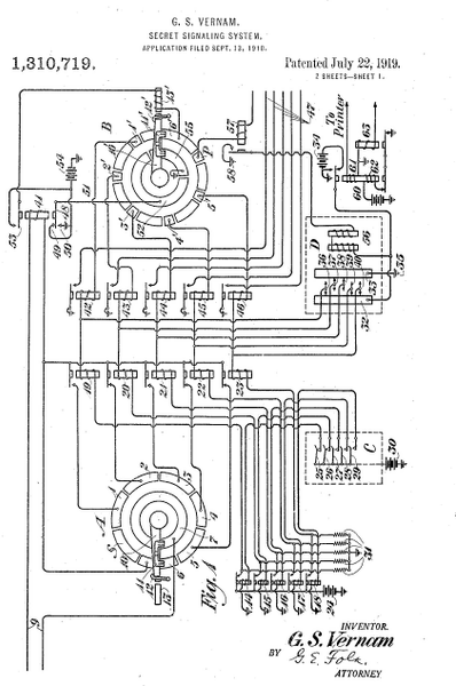

Figura 1.5: La macchina di Vernam

lunga per rendere più complicato il processo di decifrazione per l'avversario. Ma le chiavi diventarono troppo difficili da gestire nelle macchine.
In seguito gli ingegneri si accorsero che qualsiasi ripetizione di un qualunque tipo nelle chiavi dei crittogrammi sotto analisi, avrebbe creato problemi. Non importa se le ripetizioni si fossero trovate all'interno di uno o più messaggi, o fossero derivate dalla semplice ripetizione di una singola chiave lunga. Le ripetizioni nella chiave non potevano essere consentite.
Inoltre, si dimostrò che le chiavi in esecuzione dovevano essere incomprensibili.
La risoluzione di questo problema si deve a Vernam e a Joseph Mauborgne, che a quel tempo era un capitano del Corpo dei trasmettitori dell'esercito statunitense.
I due capirono che, per evitare questi problemi, la chiave doveva essere infinita, senza senso e completamente casuale, e da qui viene il nome *One-Time Pad*.
Quando Vernam e Mauborgne combinarono le due idee, implementarono il One-Time Pad, che consiste in una chiave casuale usata una e una sola volta. Tuttavia nessuno degli inventori a quel tempo usò questo nome. Il One-Time Pad fu brevettato a metà degli anni '20.
Il One-Time Pad fornisce una chiave nuova e casuale per ogni lettera del messaggio in chiaro. E inoltre è un sistema inviolabile.
Alcuni sistemi sono inviolabili solo nella pratica, perché l'avversario potrebbe riuscire a

risolverli se avesse abbastanza testo e abbastanza tempo.
Il One-Time Pad è inviolabile sia in teoria che in pratica.
Non importa quanto testo avesse a disposizione l'avversario o quanto tempo avesse a disposizione per lavorarci: non sarebbe mai stato in grado di risolverlo. Questo straordinario risultato si deve al fatto che la chiave non si ripete, ed è composta da caratteri casuali.
Inoltre se l'avversario, non possedendo la chiave, avesse voluto decifrare il messaggio, avrebbe potuto tentare con ogni possibile chiave. Questa operazione ha un enorme costo computazionale, in quanto il numero di chiavi cresce esponenzialmente al crescere della lunghezza del messaggio.
Seguendo quindi questa strategia, a causa dell'arbitrarietà della chiave, l'avversario avrebbe ottenuto tutti i possibili testi in chiaro della stessa lunghezza del testo cifrato.
Inoltre, per la casualità della chiave, tutti questi testi in chiaro sarebbero ugualmente probabili e dunque sarebbe stato impossibile optare per l'uno o l'altro di questi: l'avversario non sarebbe mai riuscito a capire in alcun modo quale potesse essere quello giusto.
Tuttavia sebbene il dispositivo ebbe un successo ingegneristico, si riscontrarono alcuni problemi pratici non trascurabili.
Il primo consisteva nella generazione delle chiavi. Dovevano essere opportunamente lunghe per consentire lo scambio di messaggi sufficientemente articolati; dovevano essere casuali e, visto che non potevano essere riutilizzate, occorreva produrne tante per aver modo di comunicare frequentemente. La generazione di numeri causali non è un problema banale dal punto di vista dell'Informatica e, a maggior ragione, non lo è la generazione di tante lunghe stringhe di numeri casuali.
Ma il problema principale del cifrario di Vernam era un altro.
La chiave, lunga come il testo, doveva essere preventivamente comunicata al destinatario in modo sicuro, ma non sempre era disponibile un canale sicuro di comunicazione.
I due corrispondenti avrebbero dovuto incontrarsi periodicamente in luogo sicuro e generare una sequenza casuale lunghissima, sufficiente per un gran numero di messaggi, da utilizzare un po' alla volta. Una volta esaurita la chiave avrebbero dovuto incontrarsi di nuovo, rigenerare la chiave e scambiarsi nuovamente dei messaggi.
Perciò società via cavo e imprese commerciali accantonarono l'idea di Vernam, preferendo utilizzare altri metodi che, sebbene non teoricamente inattaccabili, offrivano in pratica un ragionevole grado di sicurezza.
In seguito si pensò, per semplificare le cose, di generare la chiave in modo pseudo-casuale, secondo una qualche regola nota e riproducibile dal destinatario; questa idea diede luogo nel periodo tra le due guerre mondiali a una generazione di macchine cifranti, tra le quali la macchina Lorenz, usata dai tedeschi nella seconda guerra mondiale.
Ma così il cifrario non era più assolutamente sicuro, perché la chiave non era più realmente lunga come il testo, la vera chiave era il seme iniziale utilizzato dall'algoritmo di generazione della chiave. Tanto è vero che la macchina Lorenz fu forzata dagli inglesi sin

dal 1941.
Ma a quel punto Vernam si era già ritirato.
Aveva continuato il suo lavoro presso le *American Telephone and Telegraph Company* per diversi anni.
Migliorò il proprio sistema, inventò un dispositivo per crittografare la scrittura a mano durante la trasmissione di un teleautografo e inventò anche una delle prime forme di crittografia digitale binaria delle immagini.
Il 7 febbraio 1960, dopo un lungo periodo di malattia di Parkinson, l'uomo che aveva automatizzato la crittografia morì nella sua casa, nel New Jersey.
Nonostante le difficoltà pratiche che si erano riscontrate in passato, il cifrario di Vernam fu comunque usato negli anni della guerra fredda dai servizi segreti dell'Est e per il telefono rosso tra Washington e Mosca.
Un cifrario di Vernam era anche quello trovato addosso al Che Guevara dopo la sua uccisione nel 1967.
Tra le macchine cifranti ispirate al sistema Vernam, oltre ai sistemi a rotori che generano sequenze pseudocasuali, come la già citata Lorenz, furono usati sistemi a nastro perforato, che se generati con procedimenti realmente casuali, realizzano un vero cifrario di Vernam, risultando quindi inattaccabili. Un esempio di questo genere è la macchina Hagelin RT con modulo a nastro.

1.2 Il funzionamento del cifrario

In questo paragrafo viene presentata una spiegazione tecnica del funzionamento del cifrario di Vernam, con esempi dove viene mostrato il processo di cifratura.
Ma prima viene data una descrizione del *cifrario di Vernam*.
Questo è un sistema crittografico derivato dal *cifrario di Vigenère*, a cui è stato aggiunto un ulteriore requisito: la chiave di cifratura deve essere lunga quanto il testo e non deve essere riutilizzata. Da questa proprietà il cifrario di Vernam prende il nome di *One-Time Pad (OTP)*, che significa "taccuino monouso".
Quindi il cifrario di Vernam è un'estensione del cifrario di Vigenère, che a sua volta è un'estensione del cifrario di Cesare.
Il cifrario di Vernam permette la cifratura simmetrica di un messaggio: la chiave per cifrare è la stessa per decifrare.
La chiave deve:

(i) essere lunga almeno quanto il messaggio;

(ii) essere una sequenza completamente casuale di caratteri;

(iii) non deve essere riutilizzata. (Monouso)

Ora viene mostrato come cifrare un messaggio in chiaro con una chiave e ottenere così un messaggio cifrato.
Per farlo ci sono due modi diversi, ma che sono equivalenti.
Il primo, il più semplice dei due, è un procedimento che somma il testo in chiaro da cifrare alla chiave. Si associa ad ogni lettera il numero corrispondente nel seguente modo: a=0,b=1,.... z=25.
In questo metodo la somma è una *somma modulo 26.*
La seguente immagine mostra un esempio di questo procedimento.

Figura 1.6: Primo metodo di cifratura con il cifrario di Vernam. In questo esempio mancano le lettere w,x e y quindi alla lettera z non corrisponde il numero 25, ma il 22. In ogni caso il funzionamento è lo stesso e la somma sarà una *somma modulo 22.*

Prima di mostrare il secondo metodo, viene introdotto il concetto di *XOR.*
L'operazione di XOR(exclusive-or) viene indicata con il simbolo $\oplus$, un operatore logico che si applica a due variabili e si comporta nel seguente modo:

(i) restituisce **VERO** se e solo se le variabili sono diverse (una **VERO** e l'altra **FALSO**;

(ii) restituisce **FALSO** se e solo se le due variabili sono entrambe **VERO** o entrambe **FALSO**.

Per non creare fraintendimenti, è opportuno specificare che l'operatore $\oplus$ sarà usato in $\mathbb{Z}_2$.
$\oplus$ indicherà la *somma modulo 2*.
Si avranno i seguenti casi:

(1) $0 \oplus 0 = 0$

(2) $1 \oplus 0 = 1$

(3) $0 \oplus 1 = 1$

(4) $1 \oplus 1 = 0$

Il secondo metodo sfrutta l'operatore $\oplus$.
Per cifrare un messaggio si deve prima convertire il messaggio in codice binario, ovvero una stringa in cui ogni elemento, chiamato *bit*, assume solo i valori 0 e 1.
Questa operazione viene eseguita tramite il codice di Baudot, che faceva corrispondere ad ognuna delle 26 lettere dell'alfabeto inglese una stringa di 5 bit.
Una volta fatto questo, anche per la chiave, si può quindi passare alla cifratura del testo in chiaro.
Si effettua l'operatore $\oplus$ fra le due stringhe di 0,1.

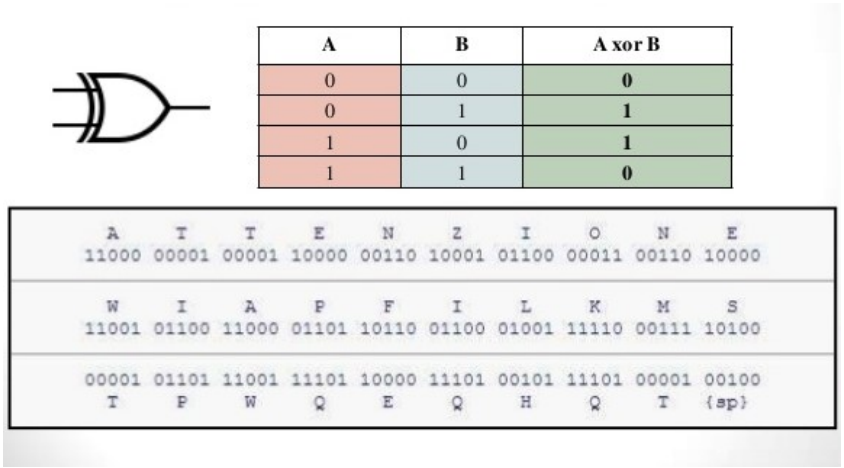

Figura 1.7: Operazione XOR fra due parole converite in stringhe 0,1.

Nella precedente immagine si può notare come l'operatore XOR venga usato su ogni bit

del messaggio in chiaro con il corrispondente bit della chiave per ottenere una stringa del tutto nuova.
Con la seguente immagine viene mostrato l'intero procedimento.

Vernam

Messaggio in chiaro	A T T E N Z I O N E
c (cod. Baudot)	11000 00001 00001 10000 00110 10001 01100 00011 00110 10000
chiave	S G S I F H S L A N
K	10100 01011 10100 01100 10110 00101 10100 01001 11000 00110
c XOR K	01100 01010 10101 11100 10000 10100 11000 01010 11110 10110
Messaggio cifrato	**I R Y U E S A R K F**

Figura 1.8: Secondo metodo di cifratura con il cifrario di Vernam. Essendo la versione binaria del cifrario di Vernam, lo si può chiamare One-Time Pad.

Come mostrato in foto e secondo quanto detto nel precedente paragrafo, la chiave è lunga almeno quanto il testo ed è anche completamente casuale. Allora il testo cifrato non contiene alcuna informazione sul testo in chiaro ed è del tutto sicuro dagli attacchi dell'avversario.
Questo avviene a patto che la chiave non venga ripetuta.
Si può facilmente capire quanto sia scomodo distribuire in modo sicuro chiavi di tali dimensioni. Ciò nonostante il cifrario di Vernam è stato utilizzato per le comunicazioni con le spie, che venivano equipaggiate di taccuini (pad in inglese) contenenti una lunga chiave per ogni pagina, da poter strappare e gettare una volta utilizzata (one time, ovvero "un solo uso").

```
CIHJT UUHML FRUGC ZIBGD BQPNI PDNJG LPLLP YJYXM
DCXAC JSJUK BIOYT MWQPX DLIRC BEXYK VKIMB TYIPE
UOLYQ OKOXH PIJKY DRDBC GEFZG UACKD RARCD HBYRI
DZJYO YKAIE LIUYW DFOHU IOHZV SRNDD KPSSO JMPQT
MHQHL OHQQD SMHNP HHOHQ GXRPJ XBXIP LLZAA VCMOG
AWSSZ YMFNI ATMON IXPBY FOZLE CVYSJ XZGPU CTFQY
HOVHU OCJGU QMWQV OIGOR BFHIZ TYFDB VBRMN XNLZC
```

Figura 1.9: Esempio di blocco monouso

La seguente immagine mostra i 2 procedimenti dello stesso cifrario.

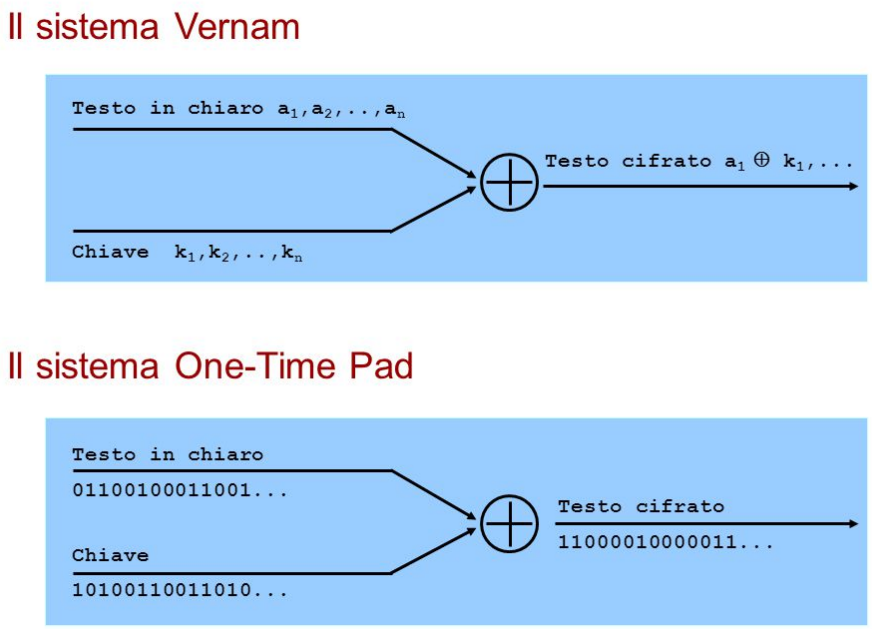

Figura 1.10: I due metodi a confronto

Nel prossimo capitolo si comprenderà meglio perché il cifrario di Vernam, sia definito il "cifrario perfetto".
Il tutto verrà spiegato nel secondo paragrafo del seguente capitolo con dimostrazioni matematiche.

Capitolo 2

Shannon e la sicurezza

Il seguente capitolo è suddiviso in due paragrafi.
Nel primo verrà presentata la biografia di Claude Shannon, raccontando dei suoi successi e delle sue invenzioni.
Nel secondo verrà descritto come Shannon sia riuscito a dimostrare che il "Cifrario di Vernam" sia il primo e unico sistema di crittografia perfettamente sicuro.

2.1 La vita di Shannon

Claude Elwood Shannon (Petoskey, 30 aprile 1916–Medford, 24 febbraio 2001) è stato un importante matematico e ingegnere americano, lontano parente dell'illustre inventore Thomas Edison.
Viene spesso definito "il padre della teoria dell'informazione".

Figura 2.1: Shannon in giovane età

Da ragazzo lavorò come telegrafista per la Western Union.
Nel 1932 iniziò a frequentare l'Università del Michigan dove nel 1936 conseguì due lauree triennali: una in matematica e l'altra in ingegneria elettronica. La tesi che presentò al master del 1938, *A Symbolic Analysis of Relay and Switching Circuits* [1], stabilì i fondamenti teorici per lo studio dei circuiti digitali collegando le reti logiche elettroniche, come relè ed interruttori, all'algebra booleana.
In questo studio Shannon dimostrò che il fluire di un segnale elettrico attraverso una rete di interruttori, ovvero dispositivi che possono essere in uno di due stati, segue esattamente le regole dell'algebra di Boole, se si fanno corrispondere i due valori di verità VERO e FALSO della logica simbolica allo stato APERTO o CHIUSO di un interruttore.
Pertanto un circuito digitale può essere descritto da un'espressione booleana, la quale può poi essere manipolata secondo le regole di questa algebra.
Shannon definì così un potente metodo, ancora oggi usato, per l'analisi e la progettazione dei sistemi digitali di elaborazione dell'informazione.
Nel 1940 Shannon conseguì il dottorato al Massachusetts Institute of Technology (MIT) dove collaborò alla costruzione dell'analizzatore differenziale di Vannevar Bush, un calcolatore analogico che si basava sulla teoria e progettazione di complessi circuiti di relè per risolvere equazioni differenziali.
Nello stesso anno Shannon si sposò una prima volta con Norma Levor. Il matrimonio però si ruppe l'anno successivo, quando la coppia si era spostata a Princeton.
Nell'estate del 1941, per alcuni mesi lavorò come ricercatore-matematico ingegnere presso la Bell Telephones Laboratories; subito dopo, accettò un'offerta per lavorare a tempo pieno su progetti di interesse militare. Ci rimase fino al 1972.
I primi progetti di Shannon riguardarono i dispositivi automatici di puntamento antiaereo ed i problemi connessi di riduzione del rumore. Iniziò anche ad occuparsi di crittografia, lavorando al progetto di un dispositivo digitale per la segretezza delle comunicazioni telefoniche.
In questo ruolo ebbe l'occasione di conoscere Alan Turing, anch'egli esperto crittoanalista, che nel 1943 passò alcuni mesi negli Stati Uniti su incarico del governo britannico. Poiché ambedue erano impegnati in attività riservate, delle quali non potevano parlare, nei loro incontri discussero principalmente di calcolatori e di intelligenza artificiale.
Nel 1948 pubblicò *A Mathematical Theory of Communication* [2], un trattato scientifico di eccelsa qualità, anche dal punto di vista della scrittura tecnica, che poneva la base teorica per lo studio dei sistemi di codificazione e trasmissione dell'informazione. In questo lavoro si concentrò sul problema di ricostruire, con un certo grado di certezza, le informazioni trasmesse da un mittente.
Shannon utilizzò strumenti quali l'analisi casuale e le grandi deviazioni, che in quegli anni si stavano appena sviluppando. Fu in questa ricerca che Shannon coniò la parola bit, per designare l'unità elementare d'informazione.
La sua teoria dell'informazione pose le basi per progettare sistemi informatici, partendo

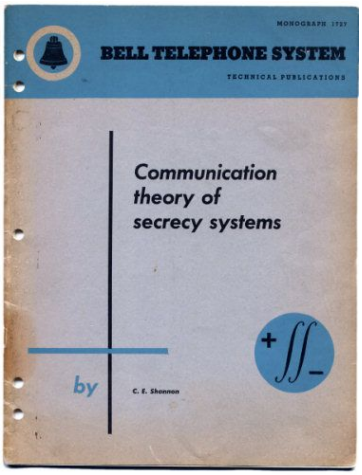

Figura 2.2: La seconda parte del saggio

dal presupposto che l'importante era cercare di memorizzare le informazioni in modo da poterle trasferire e collegare tra loro.
Shannon ha affermato che la maggiore ispirazione alla sua ricerca in questo campo venne dal lavoro sulla trasmissione delle informazioni del suo collega dei Bell Labs Ralph Hartley, del 1928, che aveva discusso anche con Weyl a Princeton.
Sempre nel 1948, Shannon incontrò Mary Elizabeth Moore, detta Betty, una matematica che lavorava come analista numerica ai Bell Labs; e l'anno successivo i due si sposarono, andando a vivere prima a New York e poi nel New Jersey. Assieme ebbero tre figli, Robert jr, Andrew e Margarita.
Nel 1949 pubblicò un altro notevole articolo, *Communication Theory of Secrecy Systems* [3], con il quale praticamente fondò la teoria matematica della crittografia.
Shannon è inoltre riconosciuto come il "padre" del teorema del campionamento, che studia la rappresentazione di un segnale continuo (analogico) mediante un insieme discreto di campioni a intervalli regolari (digitalizzazione).
Nel 1956, anno in cui fu eletto membro della National Academy of Sciences, assieme ad altri studiosi del Dartmouth College (New Hampshire), compì i primi esperimenti sull'Intelligenza Artificiale.
In questo periodo inoltre diede inizio alla sua collaborazione con il Massachusetts Institute of Technology; qui dopo due anni iniziò ad insegnare fino al 1978, anno in cui fu nominato professore emerito.
Shannon era conosciuto per la sua intelligenza vivacissima; molti hanno testimoniato che poteva dettare interi articoli accademici a memoria, senza alcuna correzione. Raramente utilizzava appunti o schizzi, e preferiva lavorare a mente.
Fuori dei suoi interessi accademici, era giocoliere e scacchista e si dilettava con il monociclo.

Ha inventato, inoltre, molti dispositivi, compresa una macchina per giocare a scacchi, un "saltapicchio" (pogo stick) a motore e una tromba lanciafiamme, per una mostra scientifica.
Nel 1961 creò il Minivac 601 Digital Computer Kit, un sistema di computer digitale elettromeccanico, che venne prodotto dalla Scientific Development Corporation e commercializzato per scopi ludici e didattici.
Dal punto di vista religioso e politico si dichiarava rispettivamente ateo e apolitico.
Negli ultimi anni della sua vita soffrì della malattia di Alzheimer fino alla morte.

2.2 Il cifrario perfetto

In questo paragrafo sarà analizzato il *cifrario di Vernam* dal punto di vista matematico, in particolare ci si soffermerà sulla sua sicurezza.
Ma prima è opportuno dare qualche definizione.

Definizione 2.1. La quintupla $(\boldsymbol{M},\boldsymbol{K},Gen,Enc,Dec)$ si dice un *sistema crittografico a chiave privata* sullo spazio dei messaggi $\boldsymbol{M}$ e sullo spazio delle chiavi $\boldsymbol{K}$ se:

(1) *Gen* (algoritmo che genera le chiavi) è un algoritmo probabilistico che restituisce una chiave $k \in \boldsymbol{K}$. Il processo di generazione di una chiave k si indica con $k \leftarrow Gen$. La distribuzione su $\boldsymbol{K}$ è uniforme.

(2) *Enc* (algoritmo di cifratura) è un algoritmo probabilistico che, presi $m \in \boldsymbol{M}$ e $k \in \boldsymbol{K}$ come input, restituisce un testo cifrato c. Si indica con $\boldsymbol{C}$ l'insieme di tutti i possibili testi cifrati che possono essere emessi da $Enc_k(m)$, $\forall k \in \boldsymbol{K}$, $\forall m \in \boldsymbol{M}$. L'operazione di cifratura del messaggio m effettuata dall'algoritmo *Enc* con chiave k si indica con $c \leftarrow Enc_k(m)$

(3) *Dec* (algoritmo di decifrazione) è un algoritmo deterministico che, presi un testo cifrato $c \in \boldsymbol{C}$ e una chiave $k \in \boldsymbol{K}$ come input, restituisce il testo in chiaro $m \in \boldsymbol{M}$. L'operazione di decifrazione del testo cifrato c effettuata dall'algoritmo *Dec* con chiave k si indica con $m \leftarrow Dec_k(c)$

(4) $\forall m \in \boldsymbol{M}$ e $\forall k \in \boldsymbol{K}$ data da $k \leftarrow Gen$,

$$Pr[Dec_k(Enc_k(m)) = m] = 1 \tag{2.1}$$

Nel 1949 Claude Shannon diede il via allo studio moderno della crittografia. Basandosi sul fatto che l'avversario, date alcune informazioni a priori, non può ottenere ulteriori informazioni sul testo in chiaro osservando il testo cifrato, Shannon intuì le condizioni affinché un sistema crittografico poteva definirsi sicuro.

Definizione 2.2. Un sistema crittografico a chiave privata ($\boldsymbol{M}$,$\boldsymbol{K}$,*Gen*,*Enc*,*Dec*) si dice che ha *sicurezza di Shannon rispetto alla distribuzione D sullo spazio dei messaggi* $\boldsymbol{M}$ se $\forall m' \in \boldsymbol{M}$ e $\forall c \in \boldsymbol{C}$, vale:

$$Pr[k \leftarrow Gen; m \leftarrow D : m = m' | Enc_k(m) = c] = Pr[m \leftarrow D : m = m'] \tag{2.2}$$

Si dice che un sistema crittografico ha *sicurezza di Shannon* se ha sicurezza di Shannon rispetto a ogni distribuzione D sullo spazio dei messaggi $\boldsymbol{M}$.

Definizione 2.3. Si dice che un sistema crittografico a chiave privata ($\boldsymbol{M}$,$\boldsymbol{K}$,*Gen*,*Enc*,*Dec*) ha *sicurezza perfetta* se $\forall m, m' \in \boldsymbol{M}$ e $\forall c \in \boldsymbol{C}$ vale:

$$Pr[k \leftarrow Gen : Enc_k(m) = c] = Pr[k \leftarrow Gen : Enc_k(m') = c] \tag{2.3}$$

Il prossimo teorema dimostra che le due definizioni precedenti sono equivalenti.

Teorema 2.4. *Un sistema crittografico a chiave privata ha sicurezza di Shannon se e solo se ha sicurezza perfetta.*

Dim. Sicurezza Perfetta $\Rightarrow$ Sicurezza di Shannon. Intuitivamente se, per due coppie di messaggi qualsiasi, la probabilità che uno dei messaggi sia crittografato su un determinato testo cifrato deve essere uguale, allora questo è vero anche per la coppia m e m' nella definizione di Sicurezza di Shannon. Pertanto, il testo cifrato non cede alcuna informazione all'avversario e le informazioni a priori e a posteriori sul messaggio devono essere uguali. Si suppone che il sistema ($\boldsymbol{M}$,$\boldsymbol{K}$,*Gen*,*Enc*,*Dec*) abbia sicurezza perfetta. Si consideri una qualsiasi distribuzione D su $\boldsymbol{M}$, un qualsiasi messaggio $m \in \boldsymbol{M}$ e un qualsiasi testo cifrato c.
Si deve provare che

$$Pr_{k,m}[m = m' | Enc_k(m) = c] = Pr_m[m = m'] \tag{2.4}$$

Per la definizione di probabilità condizionata, il membro sinistro dell'equazione sopra, può essere riscritto come

$$\frac{Pr_{k,m}[m = m' \cap Enc_k(m) = c]}{Pr_{k,m}[Enc_k(m) = c]}$$

che, per l'ipotesi di sicurezza perfetta, può essere riscritto come

$$\frac{Pr_{k,m}[m = m' \cap Enc_k(m') = c]}{Pr_{k,m}[Enc_k(m) = c]}$$

e infine, poiché la scelta della chiave è indipendente dalla scelta del messaggio, può essere riscritto come

$$\frac{Pr_m[m = m'] Pr_k[Enc_k(m') = c]}{Pr_{k,m}[Enc_k(m) = c]}$$

L'idea centrale dietro la dimostrazione è quella di mostrare che

$$Pr_{k,m}[Enc_k(m) = c] = Pr_k[Enc_k(m') = c]$$

che stabilisce il risultato. Per iniziare, si riscrive il membro sinistro:

$$Pr_{k,m}[Enc_k(m) = c] = \sum_{m'' \in \boldsymbol{M}} Pr_m[m = m'']Pr_k[Enc_k(m'') = c]$$

Dall'ipotesi di sicurezza perfetta, l'ultimo termine può essere sostituito per ottenere:

$$\sum_{m'' \in \boldsymbol{M}} Pr_m[m = m'']Pr_k[Enc_k(m') = c]$$

Quest'ultimo termine può ora essere spostato fuori dalla sommatoria e semplificato come:

$$Pr_k[Enc_k(m') = c] \sum_{m'' \in \boldsymbol{M}} Pr_m[m = m''] = Pr_k[Enc_k(m') = c]$$

e questo conclude la prima parte della dimostrazione.
Sicurezza di Shannon ⇒ Sicurezza Perfetta. In questo caso, l'intuizione è la sicurezza di Shannon che vale per tutte le distribuzioni D; quindi, deve valere anche per i casi speciali quando D sceglie solo tra due messaggi dati.
Si suppone che il sistema ($\boldsymbol{M}$,$\boldsymbol{K}$,Gen,Enc,Dec) abbia sicurezza di Shannon.
Si considerino $m_1, m_2 \in \boldsymbol{M}$ e un qualsiasi testo cifrato c. Sia D una distribuzione uniforme su $\{m_1, m_2\}$. Si deve provare che:

$$Pr_k[Enc_k(m_1) = c] = Pr_k[Enc_k(m_2) = c]$$

La definizione di D implica che

$$Pr_m[m = m_1] = Pr_m[m = m_2] = \frac{1}{2}$$

Segue quindi dalla sicurezza di Shannon che

$$Pr_{k,m}[m = m_1 | Enc_k(m) = c] = Pr_{k,m}[m = m_2 | Enc_k(m) = c]$$

Dalla definizione di probabilità condizionata,

$$Pr_{k,m}[m = m_1 | Enc_k(m) = c] = \frac{Pr_{k,m}[m = m_1 \cap Enc_k(m) = c]}{Pr_{k,m}[Enc_k(m) = c]}$$

$$= \frac{Pr_m[m = m_1]Pr_k[Enc_k(m_1) = c]}{Pr_{k,m}[Enc_k(m) = c]}$$

$$= \frac{\frac{1}{2} \cdot Pr_k[Enc_k(m_1) = c]}{Pr_{k,m}[Enc_k(m) = c]}$$

In modo analogo,

$$Pr_{k,m}[m = m_2 | Enc_k(m) = c] = \frac{\frac{1}{2} \cdot Pr_k[Enc_k(m_2) = c]}{Pr_{k,m}[Enc_k(m) = c]}$$

Cancellando i termini uguali, si ottiene che

$$Pr_k[Enc_k(m_1) = c] = Pr_k[Enc_k(m_2) = c]$$

ed è così dimostrato il teorema.
Data la definizione di sicurezza, ora si deve considerare se esistono sistemi di crittografia perfettamente sicuri.
I sistemi di crittografia come il Cifrario di Cesare e il Cifrario a sostituzione sono sicuri purché vengano considerati solo i messaggi di lunghezza 1. Tuttavia, quando si considerano i messaggi di lunghezza 2 (o più) i sistemi non sono più sicuri. Infatti, è facile vedere che le crittografie delle stringhe AA e AB hanno distribuzioni disgiunte, violando così la perfetta segretezza. Tuttavia, ciò suggerisce che si potrebbe ottenere la sicurezza perfetta adattando in qualche modo questi sistemi per operare su ogni elemento di un messaggio in modo indipendente. Questa è l'intuizione dietro al sistema crittografico *One-Time Pad*, inventato da Gilbert Vernam nel 1917.
Ora viene data una definizione formale del *One-Time Pad*, la versione binaria del cifrario di Vernam.

Definizione 2.5. Sia n un intero positivo. Il sistema crittografico *One-Time-Pad* è descritto dalla quintupla ($\boldsymbol{M}$,$\boldsymbol{K}$,*Gen*,*Enc*,*Dec*) dove:

$$\boldsymbol{M} = \{0,1\}^n$$

$$\boldsymbol{K} = \{0,1\}^n$$

$$\boldsymbol{C} = \{0,1\}^n$$

$$Gen = k = k_1 k_2 \dots k_n \leftarrow \{0,1\}^n$$

$$Enc_k(m_1 m_2 \dots m_n) = c_1 c_2 \dots c_n \quad dove \quad c_i = m_i \oplus k_i$$

$$Dec_k(c_1 c_2 \dots c_n) = m_1 m_2 \dots m_n \quad dove \quad m_i = c_i \oplus k_i$$

Quindi $\boldsymbol{M} = \boldsymbol{K} = \boldsymbol{C} = (\mathbb{Z}_2)^n$ perchè così definiti sopra. *Gen*, algoritmo di generazione delle chiavi, sceglie una stringa in $(\mathbb{Z}_2)^n$ attraverso la distribuzione uniforme.
Ognuna delle 2^n stringhe in $\boldsymbol{K}$ è scelta come chiave con una probabilità di 2^{-n}.

Data una chiave $k \in \boldsymbol{K}$ e un testo in chiaro $m \in \boldsymbol{M}$, l'algoritmo di cifratura funziona nel seguente modo:

$$Enc_k(m) = k \oplus m = c, \quad dove \quad c \in \boldsymbol{C}$$

Dato un testo cifrato $c \in \boldsymbol{C}$, l'algoritmo di decifrazione funziona nel seguente modo:

$$Dec_k(c) = k \oplus c = m, \quad dove \quad m \in \boldsymbol{M}$$

Si può ben notare che $\forall k \in \boldsymbol{K}$ e $\forall m \in \boldsymbol{M}$, si ha:

$$Dec_k(Enc_k(m)) = k \oplus k \oplus m = m$$

e da questo si può affermare che il cifrario è ben definito.
Il cifrario di Vernam è l'unico sistema crittografico perfettamente sicuro. La sua sicurezza è stata provata da una dimostrazione matematica. Viene anche chiamato *cifrario perfetto.* Nel 1949 Shannon pubblicò la prima dimostrazione che provava la sua sicurezza nel suo articolo *Communication Theory of Secrecy Systems.* [3]
Si ha quindi il seguente teorema:

Teorema 2.6. *Il One-Time Pad è un sistema crittografico a chiave privata con sicurezza perfetta.*

Dim. Verificare che il One-Time Pad sia uno schema di crittografia a chiave privata è semplice. Si deve dimostrare che il One-Time Pad ha sicurezza perfetta e lo si fa mostrando le seguenti richieste:

(1) $\forall c, m \in \{0,1\}^n$,

$$Pr[k \leftarrow \{0,1\}^n : Enc_k(m) = c] = 2^{-k}$$

(2) $\forall c \notin \{0,1\}^n, m \in \{0,1\}^n$,

$$Pr[k \leftarrow \{0,1\}^n : Enc_k(m) = c] = 0$$

Si dimostra la (1).
Segue dal fatto che $\forall c, m \in \{0,1\}^n$, c'è solo una chiave k tale che $Enc_k(m) = m \oplus k = c$, cioè tale che $k = m \oplus c$.
Si dimostra la (2).
Segue dal fatto che per una qualsiasi chiave $k \in \{0,1\}^n$, $Enc_k(m) = m \oplus k \in \{0,1\}^n$.
Dimostrate le richieste, si conclude che $\forall m_1, m_2 \in \{0,1\}^n$ e un qualunque testo cifrato c, si ha che:

$$Pr[k \leftarrow \{0,1\}^n : Enc_k(m_1) = c] = Pr[k \leftarrow \{0,1\}^n : Enc_k(m_2) = c]$$

La sicurezza perfetta è stata dimostrata, concludendo così il teorema.
Grazie al fatto che il cifrario di Vernam ha sicurezza perfetta, se un avversario intercetta un testo cifrato c, può usare tutte le chiavi per trovare tutti i possibili messaggi, ma non saprà quale possa essere quello giusto, in quanto hanno tutti la stessa probabilità.
Si è appena dimostrato che il cifrario di Vernam ha sicurezza perfetta, ma per il teorema 2.4 che afferma l'equivalenza tra sicurezza perfetta e sicurezza di Shannon, si ha che il cifrario di Vernam ha anche sicurezza di Shannon.
Dal punto di vista teorico si è trovato il "cifrario perfetto".
Dal punto di vista pratico invece si presentano alcuni problemi: il principale è quello di generare una chiave lunga quanto il messaggio da inviare.
Questo non dipende dal funzionamento del cifrario di Vernam, ma è una conseguenza della sicurezza perfetta, come verrà mostrato a breve attraverso il noto teorema di Shannon.
Il One-Time Pad è dunque un sistema crittografico perfetto se la chiave è scelta con una probabilità uniforme Pr[k]= 2^{-k}. Questo ovviamente quando ogni nuova chiave è generata casualmente per cifrare ogni nuova stringa di testo in chiaro.
Nel caso del cifrario di Vernam bisognerebbe spedire la chiave, lunga almeno quanto il messaggio, su un canale sicuro per essere conservata, ma è una cosa molto difficile da realizzare, il più delle volte non è possibile.
Più grande è la lunghezza del messaggio, più grande sarà la difficoltà nel conservare la chiave in modo sicuro; ecco che il cifrario di Vernam diventa sconveniente.
Non rimane altro che riutilizzare la stessa chiave per cifrare più di un testo in chiaro.
Ma se un sistema crittografico riutilizza la stessa chiave non gode più della sicurezza perfetta, la quale dipende dal fatto che ogni chiave è utilizzata per una sola cifratura.
In questo modo l'avversario può guadagnare informazioni sulla chiave o sul messaggio osservando il testo cifrato.
Tuttavia un sistema crittografico ritenuto insicuro dal punto di vista della teoria dell'informazione può essere computazionalmente sicuro e quindi fornire ancora un'elevata protezione nei confronti di eventuali *ciphertext attacks*, tenendo conto che l'avversario può disporre solo di una quantità limitata di risorse computazionali.
Per sistema crittografico computazionalmente sicuro si intende che il miglior algoritmo richiede almeno N operazioni per violarlo, dove N è un numero fissato molto elevato.
Il problema della lunghezza della chiave di cifratura non vale solo per il cifrario di Vernam, ma vale per ogni sistema crittografico che ha sicurezza di Shannon.
Adesso viene enunciato il noto teorema di Shannon.

Teorema 2.7. *Se un sistema crittografico (*$\boldsymbol{M}$*,*$\boldsymbol{K}$*,*Gen,Enc,Dec*) ha sicurezza di Shannon, allora* $|\boldsymbol{K}| \geq |\boldsymbol{M}|$.

Dim. Si suppone per assurdo che esista un sistema crittografico a chiave privata con sicurezza perfetta ($\boldsymbol{M}$,$\boldsymbol{K}$,*Gen*,*Enc*,*Dec*) tale che $|\boldsymbol{K}| < |\boldsymbol{M}|$.
Preso un qualsiasi $m_1 \in \boldsymbol{M}, k \in \boldsymbol{K}$ e sia $c \leftarrow Enc_k(m_1)$.
Sia **Dec**(c)= $\{m \mid \exists k \in \boldsymbol{K}$ tale che m=$Dec_k(c)\}$, l'insieme di tutte le possibili decifrazioni

di c sotto tutte le possibili chiavi.
Poiché l'algoritmo Dec è deterministico, questo insieme ha cardinalità al massimo $|\boldsymbol{K}|$.
Ma poiché $|\boldsymbol{M}| > |\boldsymbol{K}|$, esiste un messaggio $m_2 \notin \mathbf{Dec}(c)$.
Dalla definizione di sistema crittografico a chiave privata segue che

$$Pr[k \leftarrow \boldsymbol{K} : Enc_k(m_2) = c] = 0$$

Ma poiché

$$Pr[k \leftarrow \boldsymbol{K} : Enc_k(m_1) = c] > 0$$

si conclude che

$$Pr[k \leftarrow \boldsymbol{K} : Enc_k(m_1) = c] \neq Pr[k \leftarrow \boldsymbol{K} : Enc_k(m_2) = c]$$

Ma questo stabilisce che ($\boldsymbol{M}$,$\boldsymbol{K}$,*Gen*,*Enc*,*Dec*) non ha sicurezza perfetta e quindi equivalentemente non ha sicurezza di Shannon, contraddicendo così l'ipotesi del teorema. Mostrando l'assurdo la dimostrazione si conclude.
Si noti che la dimostrazione del teorema di Shannon descrive un possibile attacco contro ogni sistema crittografico a chiave privata per il quale $|\boldsymbol{K}| < |\boldsymbol{M}|$. Infatti si vede nella dimostrazione che per ogni schema di crittografia esistono $m_1, m_2 \in \boldsymbol{M}$ e una costante $\epsilon > 0$ tale che

$$Pr[k \leftarrow \boldsymbol{K}; Enc_k(m_1) = c : m_1 \in \mathbf{Dec}(c)] = 1$$

ma

$$Pr[k \leftarrow \boldsymbol{K}; Enc_k(m_1) = c : m_2 \in \mathbf{Dec}(c)] \leq 1 - \epsilon$$

La prima equazione segue direttamente dalla definizione di crittografia a chiave privata, mentre la seconda equazione deriva dal fatto che, per la dimostrazione del teorema di Shannon, esiste qualche chiave k per cui $Enc_k(m_1) = c$, ma $m_2 \notin \mathbf{Dec}(c)$.
Si consideri di scegliere uniformemente un messaggio m da $\{m_1, m_2\}$ e di inviare il testo cifrato c ottenuto da m.
Si supponga che l'avversario, avendo visto la cifratura di m, debba indovinare se $m = m_1$ o $m = m_2$ con probabilità $> \frac{1}{2}$.
L'avversario, una volta intercettato c, verifica semplicemente se $m_2 \in \mathbf{Dec}(c)$. Se $m_2 \notin \mathbf{Dec}(c)$, l'avversario indovina che $m = m_1$, altrimenti fa una scelta casuale.
Se il messaggio m inviato è m_2, allora $m_2 \in \mathbf{Dec}(c)$ e l'avversario indovinerà correttamente con probabilità $\frac{1}{2}$. Se, d'altra parte, il messaggio m inviato è m_1, allora con probabilità ϵ, $m_2 \notin \mathbf{Dec}(c)$ e l'avversario indovinerà correttamente con probabilità 1, mentre con probabilità $1 - \epsilon$ farà una scelta casuale, e quindi sarà corretto con probabilità $\frac{1}{2}$.
Si conclude che la probabilità di successo dell'avversario è

$$Pr[m = m_2] \cdot \frac{1}{2} + Pr[m = m_1](\epsilon \cdot 1 + (1 - \epsilon) \cdot \frac{1}{2}) = \frac{1}{2} + \frac{\epsilon}{4}$$

Dunque l'avversario riesce a distinguere se è stato cifrato m_1 oppure m_2.
Così è stato mostrato un attacco da parte dell'avversario che gli consente di indovinare quale messaggio è stato inviato con probabilità $> \frac{1}{2}$.
Occorre dire che se ϵ è molto piccolo, ad esempio 2^{-100}, l'efficacia di questo attacco è limitata. Tuttavia, se la chiave è più corta dei messaggi, anche di un solo bit, allora $\epsilon = \frac{1}{2}$ e quindi l'attacco ha successo con probabilità $\frac{5}{8} > \frac{1}{2}$.
Infatti esisteranno messaggi m_1 e m_2 tali che la probabilità di successo dell'avversario è $\frac{1}{2} + \frac{1}{8} = \frac{5}{8}$.

Capitolo 3

Conclusioni

Il cifrario di Vernam, ideato nel 1918, è da considerarsi il primo cifrario moderno.
Nel 1949, Claude Shannon, dimostrò che il cifrario di Vernam è l'unico metodo crittografico possibile che sia totalmente sicuro, l'unico vero cifrario perfetto, inviolabile sia in teoria che in pratica.
Con il possesso di un sistema crittografico perfetto, la battaglia teorica tra crittografia e crittoanalisi si è risolta con una vittoria della prima sulla seconda.
Tuttavia il Cifrario di Vernam è stato usato raramente nel corso della storia, come si è visto nel primo capitolo.
Ipotizzando di voler far uso di questa insuperabile protezione, restano infatti aperti molti problemi di ordine pratico. Bisogna infatti soddisfare gli stringenti requisiti del cifrario di Vernam: chiave lunga quanto il messaggio e mai più riutilizzabile.
Inoltre, per trasmettere un messaggio riservato su un canale insicuro è necessario impiegarne precedentemente uno sicuro per concordare un dato altrettanto lungo e segreto: la chiave.
In seguito si è quindi preferito usare versioni indebolite del cifrario di Vernam.
Ci si accontentò in pratica di difendere la riservatezza con cifrari simmetrici dotati di una chiave di lunghezza fissa e relativamente piccola.
Queste versioni non sono sistemi crittografici perfettamente sicuri e dunque sono violabili dal punto di vista teorico, tuttavia dal punto di vista pratico risultano comunque abbastanza efficaci.
Questi sistemi si dicono computazionalmente sicuri, molto utili nell'approccio crittografico moderno.
Il concetto di sicurezza computazionale è stato introdotto sempre da Shannon.
Un Cifrario è computazionalmente sicuro se, il calcolare il testo in chiaro m da quello cifrato c è possibile, ma richiede una potenza di elaborazione superiore a quella che si ipotizza essere a disposizione dell'attaccante.
Per dare sicurezza computazionale ad un cifrario non perfetto è necessario che la trasformazione di cifratura generi confusione e diffusione.

La *confusione* si ottiene imponendo al testo cifrato di dipendere in modo complesso dalla chiave e dal testo in chiaro, al punto che è difficile prevedere che cosa accadrà al testo cifrato modificando anche un solo simbolo del testo in chiaro.
La *diffusione* si ottiene imponendo ad ogni simbolo del testo in chiaro di influire sul valore di molti, se non tutti, i simboli del cifrato, al punto che è difficile prevedere quanti e quali di questi modificano il loro valore se si modifica anche un solo simbolo del testo in chiaro.
Shannon ha infine indicato il modello del *cifrario composto* (product cipher) come linea guida per conseguire tali proprietà: per determinare confusione il cifrario deve avvalersi di operazioni di sostituzione; per generare diffusione, deve invece avvalersi di operazioni di trasposizione (o permutazione).
Vernam e Shannon sono stati due figure importanti nella storia della crittografia.
Il loro contributo è stato fondamentale e ha determinato l'evoluzione della crittografia fino ad oggi.

Bibliografia

[1] C. E. Shannon, *A Symbolic Analysis of Relay and Switching Circuits*, Master of Science Thesis, MIT; poi pubblicato in Transactions of the American Institute of Electrical Engineers, vol. 57, pp. 713–723, 1938

[2] C. E. Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal, vol. 27, pp. 379–423 (luglio), 623–656 (ottobre), 1948.

[3] C. E. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal, vol. 28, pp. 656–715, 1949.

[4] R. Pass, A. Shelat, *A Course in Cryptography*, (gennaio), 2010

[5] D. Kahn, *The Codebreakers - The Story of Secret Writing*, 1967

Elenco delle figure

Ringraziamenti

Ringrazio di cuore i miei genitori e mio fratello che mi hanno sempre sostenuto e incoraggiato durante questo percorso, soprattutto nei momenti difficili.
Ringrazio tutti i miei amici per aver sempre creduto in me.
Ringrazio immensamente i miei amici compagni di corso a cui devo la mia laurea: Pier, Mary, Miri, Pippo, Michelone, Angela, Angelica, Benedetta, Giulia. Senza di loro non ce l'avrei mai fatta.
Ringrazio tutte le persone conosciute durante questo percorso.
Un ringraziamento particolare va al Professor Davide Aliffi, che con la sua massima disponibilità e pazienza, mi ha aiutato a realizzare questa tesi.
Un ringraziamento speciale va alla Professoressa Enrica Cavatorta, che tanti anni fa, mi ha fatto capire quale fosse il mio sogno da inseguire.
Un grazie immenso alle mie insegnanti delle elementari per avermi fatto amare la scuola e lo studio, un regalo che non ha prezzo.
Un grazie enorme ai ragazzi di catechismo, che in tutti questi anni mi hanno motivato sempre di più nel realizzare il sogno della mia vita.
Un gigantesco grazie a tutti i miei studenti, che mi hanno dato la forza di terminare questo percorso.
Infine ringrazio tutte le persone che non ho nominato, ma che in questi anni mi hanno regalato momenti meravigliosi e mi hanno aiutato a terminare questo percorso.
Grazie di cuore.