PROGETTO

di

COMUNICAZIONE DELLE SCIENZE

"CRITTOHOOD"

Gabriella Bettonte

Povo, 7 febbraio 2017 **Mariamichela Serafini**

Il pubblico del nostro progetto è un qualsiasi lettore di un quotidiano, dunque anche persone non competenti in ambito matematico; l'obiettivo che ci siamo poste è stato quello di trasmettere i primi rudimenti della crittografia. L'espediente di cui ci siano avvalse per comunicare il nostro argomento scientifico è stato quello di istituire il "Mese della Matematica" su un ipotetico quotidiano, per rendere il tutto più accattivante abbiamo pensato che durante il mese matematico, il nostro giornale avrebbe pubblicato sulla sua pagina culturale le avventure, a puntate, di un Robin Hood intento a scoprire i meccanismi basilari della crittografia. La scelta è ricaduta su Robin Hood in quanto si tratta di una figura nota ai più e anche si adatta ad una storia in cui i personaggi hanno la necessità di comunicare segretamente. Col trascorrere delle puntate si susseguono metodi crittografici in ordine crescente di difficoltà ma allo stesso tempo in ordine cronologico; alla fine di ogni spiegazione di ogni sistema crittografico abbiamo inserito un giochino che rispettasse la storia di Robin Hood, che stavamo raccontando, per aiutare il lettore a fissare le idee. Durante la stesura della storia abbiamo riscontrato alcune difficoltà nel far trasmettere la chiave tra gli interlocutori, dunque abbiamo pensato di trasformare queste difficoltà in vantaggio: calcando la mano sulla complessità della trasmissione della chiave privata abbiamo indotto il lettore a rendersi conto dell'impossibilità della crittografia a chiave privata a giorni nostri. In fondo a questo percorso, dunque, il lettore incontrerà i metodi crittografici a chiave pubblica, abbiamo pensato di non appesantire la descrizione del metodo dell'RSA con l'algoritmo matematico per non stancare il lettore: nella scrittura del progetto infatti non abbiamo avuto un intento didascalico, piuttosto abbiamo cercato di suscitare curiosità e interesse per l'argomento. Avendo ulteriore tempo si potrebbe continuare il progetto puntando a una serie di articoli sulla sicurezza informatica, infatti l'elaborazione di metodi crittografici sempre più sicuri è compito degli addetti hai lavori, ma ogni persona può contribuire a mettere al sicuro i propri dati non cliccando su link sospetti incontrati navigando in Internet o arrivati per email che, ad oggi, sono i maggiori responsabili di truffe ai danni di persone inconsapevoli senza nessuna educazione informatica.

PAGINA DELLA CULTURA

PUNTATA ZERO

La crittografia è stata associata per secoli ad aspetti lontani dalla vita ordinaria e fino a pochi decenni fa veniva utilizzata soprattutto in ambito militare e governativo, e i messaggi segreti viaggiavano materialmente affidati a corrieri fidati. L'invenzione del computer ha completamente rivoluzionato lo scenario, infatti al giorno d'oggi ciascuno di noi fa uso della crittografia anche se spesso inconsapevolmente. L'informatica e internet hanno reso necessario preoccuparsi della segretezza delle comunicazioni, infatti trasmettiamo informazioni che potrebbero essere captate ogni volta che svolgiamo azioni quotidiane come chiamare con il cellulare, aprire l'auto con il telecomando, acquistare un libro su internet o utilizzare il bancomat. Per evitare che una potenziale terza persona usi queste informazioni a nostro svantaggio è indispensabile che se anche dovesse intercettare il messaggio questo gli risulti incomprensibile. Lo stesso ricevente avrà quindi la certezza non solo che le informazioni siano rimaste segrete ma anche non manomesse da terzi. La crittografia si occupa proprio dell'insieme dei sistemi in grado di rendere incomprensibile un messaggio a chiunque ne venga in possesso ad eccezione del legittimo destinatario. Per far conoscere al grande pubblico una realtà a cui i matematici lavorano quotidianamente, abbiamo deciso di istituire il "mese della Matematica" sul nostro giornale. La scelta dell'argomento è ricaduta sulla crittografia perché si tratta di una materia attuale sia per i ricercatori che per le persone comuni. Nelle prossime settimane, dunque, seguiremo le avventure di un Robin Hood alle prese con la crittografia.

Re Riccardo Cuor di Leone partì per una crociata in Terra Santa. Durante la sua assenza, il principe Giovanni, suo avido e sleale fratello, lasciato in patria come reggente, usurpò la corona di Inghilterra. In quel tempo, Robin Hood era l'unica speranza dei poveri: egli derubava i ricchi per dare ai poveri, il popolo lo adorava. Ci sono un'infinità di leggende su Robin Hood, la nostra è ambientata in un mondo in cui esistono i computer e la conoscenza matematica.

Avendo Robin Hood dichiarato la sua fedeltà a re Riccardo, il principe Giovanni lo considerava suo nemico tanto da aver ordinato allo sceriffo di Nottingham di catturarlo ad ogni costo. Robin Hood e Little John erano soliti trascorrere le loro giornate nella foresta di Sherwood. In una delle loro scorribande caddero nella trappola dello sceriffo, solo Little John riuscì a sfuggire all'agguato. Robin Hood fu tenuto strettamente sorvegliato nelle prigioni del principe Giovanni per più di un anno.

PAGINA DELLA CULTURA

PRIMA PUNTATA

La nostra storia comincia con il salvataggio da parte di Little John e i suoi seguaci del loro amato compagno d'avventure Robin Hood. Quest'ultimo viene portato alla base dei ribelli al governo del principe Giovanni nella foresta di Sherwood; qui Fra Tuck, religioso del villaggio e compare di Robin Hood, lo informa della situazione attuale a Nottingham. Nonostante le casse della sua chiesa siano vuote, in quel periodo di improponibili tasse, Fra Tuck dà ogni singola moneta alla bisognosa cittadinanza di Nottingham senza appropriarsi di nulla. Lo sceriffo, esattore delle tasse per conto del principe Giovanni, riesce a privare i poveri cittadini di ogni loro possedimento andando casa per casa a riscuotere le ingiuste imposte. La situazione è talmente insostenibile che si è ad un punto tale per cui la popolazione non ha di che sopravvivere, infatti l'assenza di Robin ha permesso allo sceriffo di imperversare senza controllo. Inoltre, Fra Tuck mette al corrente il fuorilegge del fatto che aveva ritrovato dei libri di matematica nella biblioteca della canonica, da cui, dopo attenti studi, aveva ricavato un compendio di metodi crittografici che aveva successivamente insegnato a tutti i membri della compagnia e che permetteva loro di comunicare in segreto tenendo così nascoste al principe le incursioni al patrimonio dei ricchi.

Robin comincia a leggere…

Cos'è la crittografia?

Il termine "crittografia" deriva dall'unione di due parole greche: "*kryptós* ", che significa "nascosto", e *"graphía"*, che significa "scrittura"; essa è dunque l'arte di scrivere messaggi segreti. Per crittografia si intende quella tecnica che permette di "cifrare" un messaggio rendendolo incomprensibile a tutti fuorché al suo destinatario.

Schema di trasmissione del messaggio

Il mittente deve quindi cercare di mantenere la riservatezza nascondendo l'informazione contenuta nel messaggio e per fare ciò adopera un sistema di cifratura, detto algoritmo di cifratura, che trasforma il testo in chiaro (plain text) in un crittogramma (cyper text), apparentemente privo di significato e tale che solamente il legittimo destinatario possa comprenderlo.
Se il canale di trasmissione non fosse sicuro una terza persona (avversario) potrebbe cercare di intercettare il messaggio e decifrarlo (ruolo passivo) o, addirittura, di intromettere suoi messaggi nel canale (ruolo attivo). Questo sistema funziona se mittente e destinatario condividono una chiave, sconosciuta all'avversario.
La prima considerazione nella sicurezza di un sistema di crittografia riguarda la lunghezza della chiave. Se usiamo una chiave troppo corta (se comparata alla lunghezza del testo in chiaro) molto probabilmente l'algoritmo da noi usato, arrivato ad un certo punto della codifica, dovrà ripetere dei caratteri, o delle sequenze di caratteri, fornendo così uno schema che l'avversario potrebbe sfruttare per compiere il suo lavoro. Se la cosa dovesse ripetersi molte volte l'avversario potrebbe avere abbastanza materiale in mano per poter ottenere la nostra chiave. Un altro fattore importante da tenere in considerazione è il numero di chiavi che l'algoritmo ammette; se ammettesse, ad esempio, 10000 chiavi, possiamo essere certi che un "nemico" dotato di mezzi di calcolo, anche modesti, potrebbe provarle tutte in un lasso di tempo accettabile, vanificando quindi il sistema di crittografia. Questo metodo (ricerca esaustiva su tutte le chiavi possibili) viene chiamato approccio di "forza bruta". Si introduce, dunque, il concetto del "fattore lavoro", necessario per rompere un sistema di crittografia. In linea di principio un sistema sicuro in assoluto non esiste, ma se possiamo fare in modo che il fattore lavoro necessario per romperlo sia il più alto possibile, ci saremo messi al riparo dalla grande maggioranza degli attacchi. Il nostro avversario prima di lanciarsi nel tentativo di decodifica di un sistema complesso eseguirà un bilancio costi-benefici; se il beneficio che esso potrà avere dalla decodifica del nostro messaggio è inferiore allo sforzo (anche economico) che deve sostenere per decodificarlo (o per tentare di farlo) molto probabilmente lascerà perdere. Nelle prossime pagine prenderemo in esame alcuni algoritmi di cifratura.

PAGINA DELLA CULTURA

SECONDA PUNTATA

Robin, dopo aver letto l'introduzione al compendio di Fra Tuck, comprende perché questi gli abbia voluto comunicare tali metodi: ora, finalmente, può comunicare con i compagni senza correre il rischio che il principe Giovanni ostacoli i loro piani. Decide quindi di mettersi immediatamente a studiare il primo metodo che incontra.

Codice con i numeri

Uno dei codici più semplici consiste nel numerare dall'1 al 26 le lettere dell'alfabeto, sostituendo alle decine il punto e alle ventine i due punti. Per codificare e decodificare un messaggio basta scrivere l'alfabeto e sotto le lettere i numeri corrispondenti nel seguente modo:

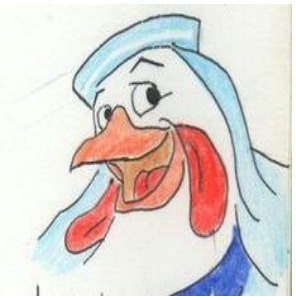
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	.1	.2	.3	.4	.5	.6	.7	.8	.9	:1	:2	:3	:4	:5	:6	:7	:8

Nel crittogramma si omettono gli spazi tra le parole per aumentare la sicurezza: infatti l'avversario potrebbe utilizzare la lunghezza delle parole come indizio.

Robin decide di applicare immediatamente il primo metodo appreso dalla lettura delle prime pagine del libro per liberarsi di un dubbio che lo angustia ormai da tempo: dove sia lady Marian. Molti anni fa, infatti, egli era fidanzato con la nipote di re Riccardo, lady Marian, ma, sette anni prima, furono costretti a separarsi poiché ella, come ogni fanciulla di nobili origini, era stata

mandata a Londra per completare i suoi studi. Dopo la partenza di re Riccardo, il principe che era a conoscenza della storia d'amore tra Robin e Marian, decise di farla sparire e da allora il nostro protagonista non ha più sue notizie. Decide così di contattare lady Cocca, dama di compagnia di lady Marian, che dopo la sua partenza per Londra era diventata parte della compagnia dei ribelli e svolgeva il ruolo di infiltrata alla corte del principe Giovanni. Robin stabilisce che, d'ora in poi, per consegnare i messaggi crittati ai suoi compagni, arrotolerà una striscia di pergamena, con il testo, ad una freccia, vista la sua abilità con l'arco.

4.6:45:19:2.9.6:41
.314:7.41.991.5



Robin Hood *Lady Cocca*

Scrivi qui la tua soluzione: _____

PAGINA DELLA CULTURA

TERZA PUNTATA

Lady Cocca, dopo aver letto il messaggio di Robin, gli suggerisce di continuare a studiare la crittografia perché il messaggio da lui scritto era facilmente decifrabile e lei aveva faticato a non farlo cadere nelle mani di sir Biss, perfido consigliere del principe Giovanni, che avrebbe sicuramente compreso il testo codificato in quanto il metodo utilizzato era troppo elementare. Gli rivela, inoltre, che la sua amata Marian è più vicina di quanto pensi, infatti è stata richiamata a Nottingham dal principe Giovanni, intenzionato a darla in sposa a chiunque avesse vinto il torneo di tiro con l'arco da lui organizzato; infatti egli desiderava liberarsi dell'ultima erede diretta al trono e anche organizzare un matrimonio che potesse rivalutare la sua cattiva reputazione agli occhi del popolo.

Robin decide dunque di mettersi in contatto con il suo compare Little John per mascherarsi da nobili e partecipare al torneo, sicuro di avere la vittoria in tasca, essendo lui il migliore arciere della Gran Bretagna. Per incontrarsi in totale sicurezza ed esporgli la sua idea, gli manda un messaggio crittato.

Codice di Atabash

L'**atabash** è un semplice cifrario a sostituzione monoalfabetica in cui la prima lettera dell'alfabeto è sostituita con l'ultima, la seconda con la penultima, e così via, "invertendo" l'ordine alfabetico delle lettere. Dunque il nostro alfabeto diventa:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

L'origine di questo cifrario si può trovare nella Bibbia, Il nome stesso del cifrario viene dalla lingua ebraica: la prima lettera dell'alfabeto ebraico è *aleph*, l'ultima *taw*, la seconda *beth*, e la penultima *shin*; messe assieme, formano la parola *atabash*.

EVWRZNLXRWLNZMRZNVAA
ZMLGGVZOOZOYVILXZEL

Robin Hood

Little John

Scrivi qui la tua soluzione: _____

Soluzione puntata precedente: **Dove si trova lady Marian**

PAGINA DELLA CULTURA

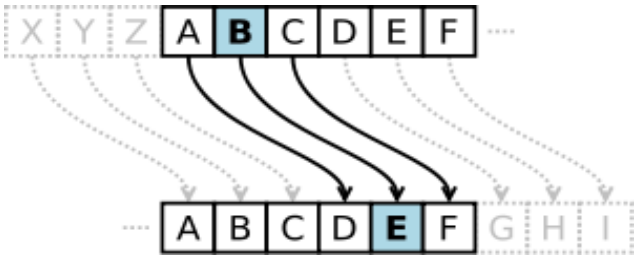
QUARTA PUNTATA

Little John si sveglia e, incastrata sullo stipite della sua casupola sugli alberi, trova una freccia del suo compagno Robin Hood; si appresta a leggere la pergamena che vede arrotolata attorno alla punta ma nota che era stata aperta. Dopo aver letto il contenuto del biglietto, John viene pervaso da una grande preoccupazione: sir Biss sicuramente aveva intercettato il messaggio di Robin e, vista l'arguzia e l'erudizione del malvagio consigliere, lo aveva decifrato e avrebbe teso una trappola ad entrambi al loro luogo di incontro. Little John non ha possibilità di comunicare con Robin perché non ha idea di dove possa essere, si risolve dunque ad andare ugualmente al loro appuntamento e cercare di salvare l'amico dalla cattura.

Robin, ignaro del pericolo incombente, si presenta all'appuntamento ma non vede il suo compagno John; questi è appostato su un ramo poco lontano in attesa che i suoi sospetti vengano confermati. Pochi istanti dopo l'arrivo di Robin, la radura si riempie delle urla dei soldati del principe Giovanni che arrivano a tutta carica e lo circondano. Little John non attendeva altro: si cala con una fune e, in modo assai rocambolesco, porta in salvo il suo amico fuggendo subito in velocità. Appena al sicuro Robin comincia a riflettere su quanto era avvenuto: nonostante avesse crittografato il messaggio, i suoi piani erano stati scoperti e capisce che è necessario approfondire ulteriormente lo studio della crittografia per far in modo che, anche se le sue frecce fossero intercettate, gli scagnozzi del principe non possano capire la natura del messaggio.

Il cifrario di Cesare

Il cifrario di Cesare è un cifrario a sostituzione monoalfabetica in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova ad un certo numero di posizioni dopo nell'alfabeto. Si procede fissando un numero K da 0 a 25 che sarà la nostra chiave segreta. L'operazione di cifratura tramite cifrario di Cesare consiste nel sommare K ad ogni carattere del messaggio in chiaro, sostanzialmente dunque per ottenere il crittogramma spostiamo di K posizioni ogni lettera del messaggio in chiaro. Dalla testiomonianza di Svetonio sappiamo che Cesare usava come chiave di cifratura K=3.



Era inoltre uso antico omettere gli spazi tra le parole allo scopo di aumentare la sicurezza nel cifrario: in questo modo infatti si toglieva un importante punto di riferimento, quale è la suddivisione in parole.

Per decifrare un messaggio è sufficiente eseguire l'operazione inversa, cioè associare ad ogni lettera del crittogramma la lettera dell'alfabeto che si trova indietro di K posti. Nel caso in cui l'avversario riesca ad impadronirsi del crittogramma e sospetti trattarsi di un Codice di Cesare, potrebbe provare a decifrare il messaggio utilizzando tutte le possibili chiavi da K=1 a K=26, sperando di imbattersi in un messaggio di senso compiuto. Questo tipo di metodo è detto di "forza bruta" ed è reso possibile dal numero esiguo di chiavi. Il Codice di Cesare perciò garantisce una scarsa sicurezza soprattutto nell'epoca dei computer.

Robin, quella stessa notte, scaglia una freccia verso la finestra dove sa che riposa Lady Marian.

Robin Hood

TPHHTHAHKVTHUPHSAVYUL
VHCYVBUHWPBTHYVZZHYO

Anni lontani

Lady Marian

Scrivi qui la tua soluzione: _____

Soluzione puntata precedente: **Vediamoci domani a mezzanotte all' albero cavo**

PAGINA DELLA CULTURA

QUINTA PUNTATA

Lady Marian vede una freccia, con arrotolata una pergamena, sul davanzale della sua finestra, incuriosita si avvicina per leggerla ma questa contiene solamente una serie di lettere a prima vista incomprensibili; in basso a destra scorge una firma: anni lontani. Inquieta comincia a chiedersi che cosa significhi e all'improvviso viene colta da una subitanea rivelazione, erano sette lunghi anni che non vedeva il suo amato Robin, così corre a prendere da sotto al materasso il compendio di Fra Tuck: poteva trattarsi del Cifrario di Cesare! Infatti riesce a decifrare il contenuto del messaggio, è Robin che la avvisa che il giorno seguente l'avrebbe strappata dalle grinfie del principe Giovanni.

L'indomani Robin e Little John, travestiti da ricchi nobili, si iscrivono al torneo di tiro con l'arco di Nottingham, passando inosservati tranne che per Marian che riconosce il suo amato dalla piuma rossa che porta in capo. Robin ottiene una vittoria schiacciante in tutte le prove grazie alla sua abilità straordinaria con l'arco. Il principe chiama al suo cospetto il vincitore per complimentarsi e promettergli la mano di Lady Marian ma appena questi si presenta alla sua vista il principe viene colto da un sospetto, la sua abilità gli ricordava quella del suo acerrimo nemico Robin Hood, quindi con un gesto ordina alle guardie di circondare discretamente il suo interlocutore. Lady Marian si accorge delle manovre del principe e comprende che la situazione sta precipitando, dunque lancia la sua sciarpa di seta sul volto del principe per offrire un diversivo a Robin. Il fuorilegge approfitta del tempo concesso dall'abile mossa di Marian e comincia a farsi largo tra le guardie; nel frattempo John

si era avvicinato dietro al trono del principe e riesce, nella confusione generale a prendere con se' Lady Marian. I nostri tre fuggitivi si dirigono di gran corsa verso la foresta. Il principe Giovanni, furioso poiché le sue guardie si erano fatte sfuggire sua nipote e il suo nemico, decide di dare ordine di catturare l'ignaro Fra Tuck per carpirgli informazioni sui ribelli, in quanto da tempo sospettava che egli fosse implicato con la rivolta al suo governo.

Giunta la notte, mentre i ribelli erano a festeggiare spensierati la riunione di Robin con Marian, arriva un membro della compagnia a portare un'orrenda notizia: Fra Tuck sarebbe stato impiccato la domenica successiva se nel frattempo al principe Giovanni non fosse stata consegnata la testa di Robin Hood. Robin, allarmato, riflette su come fare a comunicare segretamente con il frate e risolve che il modo migliore sia utilizzare il disco che lui stesso gli aveva dato; scrive il suo messaggio e lo consegna ad una guardia, loro infiltrata della prigione del principe.

Il Codice di Leon Battista Alberti

In crittografia il disco cifrante di Leon Battista Alberti, descritto nel *De cifris* intorno al 1467, è il primo sistema di cifratura polialfabetica. Questi cifrari polialfabetici si erano resi necessari dal IX secolo dopo la scoperta del matematico e filosofo arabo Al-Kindi delle analisi delle frequenze. Essi si distinguono dai monoalfabetici in quanto un dato carattere del testo chiaro non viene cifrato sempre con lo stesso carattere, ma con caratteri diversi in base ad una qualche regola, in genere legata ad una parola segreta da concordare.
Il metodo di Leon Battista Alberti si serve di un dispositivo meccanico, chiamato disco cifrante costituito da due dischi concentrici in rame. Il disco maggiore (disco stabile) viene suddiviso in 24 parti uguali, dette anche Case. Su queste vengono poi riportate le lettere dell'alfabeto in chiaro: 20 lettere in ordine alfabetico, escludendo le lettere "inutili" (H, K, Y, W) e considerando J=I e V=U e i numeri da 1 a 4. Sulle case del cerchio interno (disco mobile) sono invece riportate tutte le 24 lettere dell'alfabeto (solo considerando I=J e U=V) ma in ordine sparso e un simbolo speciale end (o "et").

Mittente e destinatario devono essere in possesso dello stesso disco e aver concordato una chiave cifrante, costituita da una coppia di lettere che determinano la corrispondenza iniziale fra i caratteri dei due dischi. Per cifrare il messaggio, il mittente scrive il testo in chiaro senza spazi e inserendo a caso numeri da 1 a 4 all'interno del testo. Quindi, ad ogni lettera del messaggio in chiaro, che va letta sul disco più grande, si associa la lettera corrispondente nel disco più piccolo. Si procede finché non si incontra uno dei numeri, a quel punto la lettera corrispondente al numero determina una nuova disposizione: alla prima lettera della chiave si fa corrispondere quella dedotta dal numero. Nella cifra di Alberti gli alfabeti sono due, mischiati, e la chiave varia in continuazione durante il messaggio, quindi la scoperta di una sola lettera non permette altri progressi nella decrittazione e lo studio delle frequenze non dà risultati perché la stessa lettera chiara è cifrata sempre in modo diverso; per questo motivo il disco di Leon Battista Alberti è considerato uno dei codici polialfabetici più sicuri.

Robin Hood

VZILNZOQNPT&NMQOEMI
LEPPNDDDRORXCQ&

Fra Tuck

Scrivi qui la tua soluzione: _____

Soluzione puntata precedente: Mia amata, domani al torneo avrò una piuma rossa. RH

PAGINA DELLA CULTURA

SESTA PUNTATA

Fra Tuck, seduto nella cella, è preoccupato per la vita dei suoi concittadini che sono stati catturati con lui per soddisfare la sete di vendetta del principe Giovanni, quando arrivano le guardie con il rancio. Fra Tuck si rifiuta di mangiare, ma la guardia gli ficca a forza la scodella tra le mani; egli avverte che incollato sul fondo c'è un foglietto, subito lo nasconde nella manica. Successivamente, tornata la tranquillità, lo apre e si accorge che contiene un messaggio crittato: non poteva essere altri che Robin Hood. Dopo qualche tentativo, il frate comprende che potrebbe trattarsi del codice di Leon Battista Alberti, mancava solo capire quale fosse la chiave così decide di provare con le iniziali dei loro nomi. Decritta il messaggio usando la chiave **RT** e si affretta ad appostarsi presso la finestra sud della sua cella in attesa di un segnale.

Passata qualche ora Tuck avverte dei movimenti sotto la sua finestra, si affaccia pronto ad eseguire l'ordine di Robin Hood. Quest'ultimo è riuscito ad introdursi nelle mura della prigione travestendosi, insieme a Little John, da guardia, scaglia una freccia, con una robusta corda attaccata, sul cornicione della finestra sud. Fra Tuck afferra la corda e la lega saldamente alle sbarre della sua cella, mentre Robin, favorito dall'oscurità della notte, si arrampica con la sola forza delle braccia fino alla finestra. Nel frattempo le guardie erano state tramortite dalla guardia infiltrata, il fuorilegge passa una lima al frate e attende che quest'ultimo gli apra un varco. Robin balza dentro la cella, incoraggia tutti a tenersi pronti alla fuga e con il pugnale rompe le catene che tenevano chiusa la porta, e fuggono

tutti giù dalle scale della torre. Arrivati all'uscita c'è Little John ad attenderli e li spinge a dirigersi verso il ponte levatoio che aveva precedentemente aperto. Una delle guardie purtroppo si accorge del tentativo di fuga, lancia l'allarme e ordina che venga immediatamente chiuso il ponte levatoio ma, grazie alla loro rapidità riescono a svignarsela.

Raggiunta in tutta fretta la foresta di Sherwood, ad attenderli una notizia: re Riccardo, vittorioso, ha fatto ritorno a sorpresa a Nottingham e ha ripreso il trono. Il malvagio fratello, però, astutamente stava fingendo di essere sempre stato fedele a Riccardo e ha chiuso fuori dal castello tutto il popolo cosicché nessuno gli rivelasse della sua pessima condotta in quegli anni e dell'usurpazione del trono. Robin allora, non sapendo come altro comunicare col re, corrompe una guardia e gli fa portare un messaggio dicendogli di dargli assolutamente il BENTORNATO. Nello scrivere il messaggio Robin utilizza il codice di Vigenère.

HMBOOEAITFBQNVCEGRHRJ
ZBBJZFAEJFVRFCIU

Robin Hood *Re Riccardo*

Scrivi qui la tua soluzione: _____

Soluzione puntata precedente: **Stanot2te finestra sud. Affe1rra la fune**

Il Codice di Vigenère

Il cifrario di Vigenère è il più semplice dei cifrari polialfabetici. Pubblicato nel 1586, fu considerato inattaccabile per secoli, godendo di una fama in buona parte immeritata essendo molto più debole di altri cifrari polialfabetici precedenti, quali il disco cifrante di Leon Battista Alberti.

Il metodo è una generalizzazione del Cifrario di Cesare, invece di spostare sempre dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile ma ripetuto, determinato in base ad una parola chiave, da concordarsi tra mittente e destinatario, e da scrivere ripetutamente sotto il messaggio, carattere per carattere; la chiave era detta anche verme, per il motivo che, essendo in genere molto più corta del messaggio, deve essere ripetuta molte volte sotto questo. Il testo cifrato si ottiene spostando la lettera chiara di un numero fisso di caratteri, pari al numero ordinale della lettera corrispondente del verme. Di fatto si esegue una somma aritmetica tra l'ordinale del chiaro (A = 0, B = 1, C = 2...) e quello del verme; se si supera l'ultima lettera, la Z, si ricomincia dalla A. Il vantaggio rispetto ad un cifrario monoalfabetico è che il testo in chiaro viene crittato con n alfabeti cifranti, cioè ogni lettera viene cifrata in n modi diversi, dove n è la lunghezza del verme. La crittoanalisi del testo cifrato è più complessa poiché non vi è più una corrispondenza biunivoca fra caratteri del testo in chiaro e del crittogramma, non permettendo quindi un'analisi delle frequenze.

Ecco un esempio

Testo in chiaro:	QUOTIDIANO
Verme:	CIAOCIAOCI
Cifratura	SCOHKLIOPW

Per semplificare la cifratura, Vigenère propose l'uso della seguente "matrice" quadrata, composta da alfabeti ordinati e spostati. Se si vuole cifrare, con la chiave dell'esempio precedente, la lettera "Q" della parola *quotidiano* basterà trovare la lettera "Q" nella prima riga, individuando la colonna relativa. Basterà poi trovare la "C" di *ciao* nella prima colonna per trovare la riga, individuando, tramite l'incrocio, la lettera corretta da usare.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Per decifrare il messaggio si applica l'operazione inversa, cioè sottrarre invece che sommare. Usando la tavola quadrata si potrà decifrare la prima S ricercandola nella riga della corrispondente lettera del verme, la C; la colonna dove si trova la S ha quindi al primo posto in alto la lettera chiara, la Q.

La debolezza di Vigenère sta nel fatto che se l'avversario riesce a determinare la lunghezza della chiave, la decrittazione diventa molto semplice. Per far ciò si possono utilizzare metodi statistici per trovare n, e successivamente applicare l'analisi delle frequenze per tutte le lettere cifrate dalla C, poi per quelle cifrate dalla I, e così via. Perciò, nel nostro esempio, nel quale n=4, la prima, la quinta, la decima, ecc. lettera avranno lo stesso alfabeto cifrante. La parte più complicata di questo processo è determinare la lunghezza della chiave, la difficoltà è proporzionale alla lunghezza del verme.

PAGINA DELLA CULTURA

SETTIMA PUNTATA

Re Riccardo, dopo aver ricevuto uno strano e sconclusionato biglietto, è inquieto, potrebbe confidarsi con suo fratello ma un cattivo presentimento lo coglie; intenzionato a scoprire la natura del messaggio comincia a chiedersi chi potrebbe essergli d'aiuto e ripensa alla storia che gli aveva raccontato il principe Giovanni: Lady Cocca, Robin Hood e i suoi compari avevano tramato per rapire e uccidere la sua amata nipote Marian. Dal momento che questa versione dei fatti cozzava con i suoi ricordi, decide di andare a discutere su quanto accaduto in sua assenza con Lady Cocca, rinchiusa negli ex appartamenti di Marian. Riccardo sale nella torre e intima alle guardie che volevano dissuaderlo, per ordine del principe, di farsi da parte, così arriva in presenza di Cocca. Quest'ultima, incredula ma felice nel rivedere l'amato re, si trova però ad affrontare la rabbia di questi che la accusa di essere complice del rapimento e della morte della nipote; ella si affretta a spiegare che sì, aveva partecipato al rapimento, ma a fin di bene, per liberarla dalle grinfie del suo perfido fratello. A questo punto Cuor di Leone le ordina di raccontargli gli avvenimenti degli ultimi anni e apprende del colpo di stato di Giovanni e della sua crudeltà verso il popolo. Indignato per le malefatte del fratello, decide di crederle e le porge il biglietto misterioso chiedendole se lei ne capisse qualcosa; ella dopo aver letto attentamente il testo comprende che si tratta di un messaggio da parte dei ribelli e chiede al re se, chiunque gliel'abbia consegnato, gli abbia anche detto qualcosa. Re Riccardo, prontamente, le dice che la guardia gli aveva detto: "Bentornato", e Lady Cocca, alla luce di questa informazione,

decodifica rapidamente il messaggio: “GIOVANNI TRAMA CONTRO DI VOI. VI SALVEREMO. RH.”

Nel frattempo Giovanni, in un’altra ala del castello, sta complottando con i suoi perfidi consiglieri per eliminare con l’inganno il legittimo regnante: hanno deciso di colpirlo durante il banchetto in onore del suo ritorno in Gran Bretagna, mentre le sue fidate guardie erano ubriache.

Robin Hood nella foresta di Sherwood, sta allestendo tutti i preparativi per l’assalto al castello di Giovanni per salvare il re con l’aiuto dei suoi compagni; egli progetta di attraversare a nuoto il fossato, con favore delle tenebre e poi introdursi da un passaggio segreto aperto dalla guardia infiltrata.

Re Riccardo raduna i suoi soldati e si prepara ad affrontare il fratello. Sir Biss, notato il tumulto, corre da Giovanni ad avvertirlo che i soldati del re si stavano armando, egli dunque decide di non aspettare il banchetto per effettuare il suo insediamento e dà ordine di barricarsi all’interno della sala del consiglio nella torre, dove egli si trovava. A quel punto Riccardo e i suoi tentano di stanare Giovanni, egli urla al fratello che ha scoperto l’inganno ma se si fosse arreso avrebbe avuto salva la vita. Giovanni si rifiuta di obbedire al fratello e dunque ordina ai suoi soldati di dare battaglia, mentre questa infuria arriva la compagnia dei fuorilegge e unitasi al plotone di Riccardo riescono a sconfiggere i nemici e a catturare Giovanni.

Dopo qualche tempo l’ordine è stato ristabilito: Riccardo Cuor di Leone ha ripreso il controllo del suo regno, i ribelli hanno smesso di essere considerati fuorilegge e finalmente il popolo è libero dal giogo delle tasse eccessive. Robin Hood, con la collaborazione di Fra Tuck e della sua colta fidanzata, istituisce una sezione di ricerca e approfondimento dei metodi crittografici: si è reso conto della difficoltà di scambiarsi la chiave, quindi da allora inizia a lavorare a metodi più efficienti.

Il metodo RSA

Il problema principale che affliggeva tutti i metodi di crittografia consisteva nello scambio della chiave, ossia nel prendere accordi con il destinatario del messaggio su quale codice usare, in caso contrario il messaggio risulta incomprensibile. Inoltre un altro problema è il fatto che se questo "scambio della chiave" fosse spiato da un eventuale avversario, quest'ultimo potrebbe decifrare tutti i messaggi invalidando l'intero sistema. Se dover far incontrare i due corrispondenti poteva essere difficoltoso un tempo, adesso è impossibile a causa della notevole distanza tra i due eventuali comunicanti.

L'RSA è il più conosciuto sistema crittografico a chiave pubblica (asimmetrica) e fu proposto dai ricercatori Rivest, Shamir e Adelman nel 1978. Il sistema di crittografia si basa sull'esistenza di due chiavi distinte, che vengono usate per cifrare e decifrare. Se la prima chiave viene usata per la cifratura, la seconda deve necessariamente essere utilizzata per la decifratura e viceversa. La questione fondamentale è che nonostante le due chiavi siano fra loro dipendenti, non sia possibile risalire dall'una all'altra, in modo che se anche si è a conoscenza di una delle due chiavi, non si possa risalire all'altra, garantendo in questo modo l'integrità della crittografia. Per poter realizzare con il cifrario asimmetrico un sistema crittografico pubblico è importante che un utente si crei autonomamente entrambe le chiavi, denominate "diretta" ed "inversa", e ne renda pubblica una soltanto. Così facendo si viene a creare una sorta di "elenco telefonico" a disposizione di tutti gli utenti, che raggruppa tutte le chiavi dirette, mentre quelle inverse saranno tenute segrete dagli utenti che le hanno create e da questi utilizzate solo quando ricevono un messaggio cifrato con la rispettiva chiave pubblica dell'"elenco" da parte di un certo mittente, ottenendo in questo modo i presupposti necessari alla sicurezza del sistema.

Facendo un esempio pratico, se Alice vuole spedire un messaggio a Bob e non vuole che altri all'infuori di Bob possano leggerlo, Alice cercherà sull'elenco la chiave pubblica di Bob e con quella potrà cifrare il messaggio. Essendo Bob l'unico a possedere la chiave inversa, sarà anche l'unico a poter decifrare il messaggio, che rimarrà così segreto per tutti gli altri, compresa Alice, che non disponendo della chiave inversa non sarà in grado di decifrare il messaggio da lei stessa creato. Ovviamente il successo di questo sistema si basa sull'assoluta necessità che Bob sia l'unico ad essere in possesso della chiave inversa. In caso contrario, avendo entrambe le chiavi, chiunque potrebbe decifrare agevolmente il messaggio. Con questo metodo di cifratura è possibile anche garantire la provenienza di un messaggio. Riprendiamo l'esempio precedente: Alice questa volta, prima di cifrare il messaggio usando la chiave pubblica di Bob, lo cifrerà usando la propria chiave inversa e solo in un secondo momento lo ri-crittograferà utilizzando la chiave pubblica di Bob. Quando Bob riceverà il messaggio e lo decifrerà usando la propria chiave inversa, otterrà ancora un messaggio crittografato.

Quel dato messaggio necessiterà poi della chiave pubblica di Alice per essere decifrato, garantendo in questo modo che il messaggio è stato spedito solo e soltanto da Alice, unica a possedere la chiave inversa con la quale era stato crittografato il messaggio. Più semplicemente, utilizzando questo metodo di cifratura, Alice può mandare messaggi a tutti, garantendo la provenienza. Infatti cifrando il messaggio con la propria chiave inversa, chiunque sarà in grado di leggere il messaggio, decifrandolo con la sua chiave pubblica, assicurandosi in tal modo che il mittente sia proprio Alice.

Per semplificare il funzionamento immaginiamo che Alice debba spedire un messaggio segreto a Bob. Occorrono i seguenti passaggi:

1. Bob sceglie due numeri primi molto grandi (per esempio di 300 cifre) e li moltiplica con il suo computer (impiegando meno di un secondo).
2. Bob invia il numero che ha ottenuto ad Alice; chiunque può vedere questo numero.
3. Alice usa questo numero per cifrare il messaggio.
4. Alice manda il messaggio cifrato a Bob; chiunque può vederlo, ma non decifrarlo.
5. Bob riceve il messaggio e, utilizzando i due fattori primi che solo lui conosceva, lo decifra.

Alice e Bob hanno impiegato pochi secondi a cifrare e decifrare, ma chiunque avesse intercettato le loro comunicazioni impiegherebbe troppo tempo per scoprire i due fattori primi necessari a decifrare il messaggio.

La forza di questo metodo crittografico è che la fattorizzazione in numeri primi di un intero molto grande richiede un elevato dispendio di tempo.

Bibliografia:

- “Problemi di logica per ragazze e ragazzi svegli” di Elvira Marinelli e Fabio Castelli, Giunti Editore.
- Tesi di laurea di Chiara Gilberti “La storia della crittografia: appunti e riflessioni”.
- Wikipedia , per gli argomenti afferenti.
- http://www.di.unisa.it/~ads/corso-security/www/CORSO-9900/crittografiaclassica/www.apogeonline.com/catalogo/allegati/483/doc/algoritmi/crypto.htm
- Film Disney: “Robin Hood”.