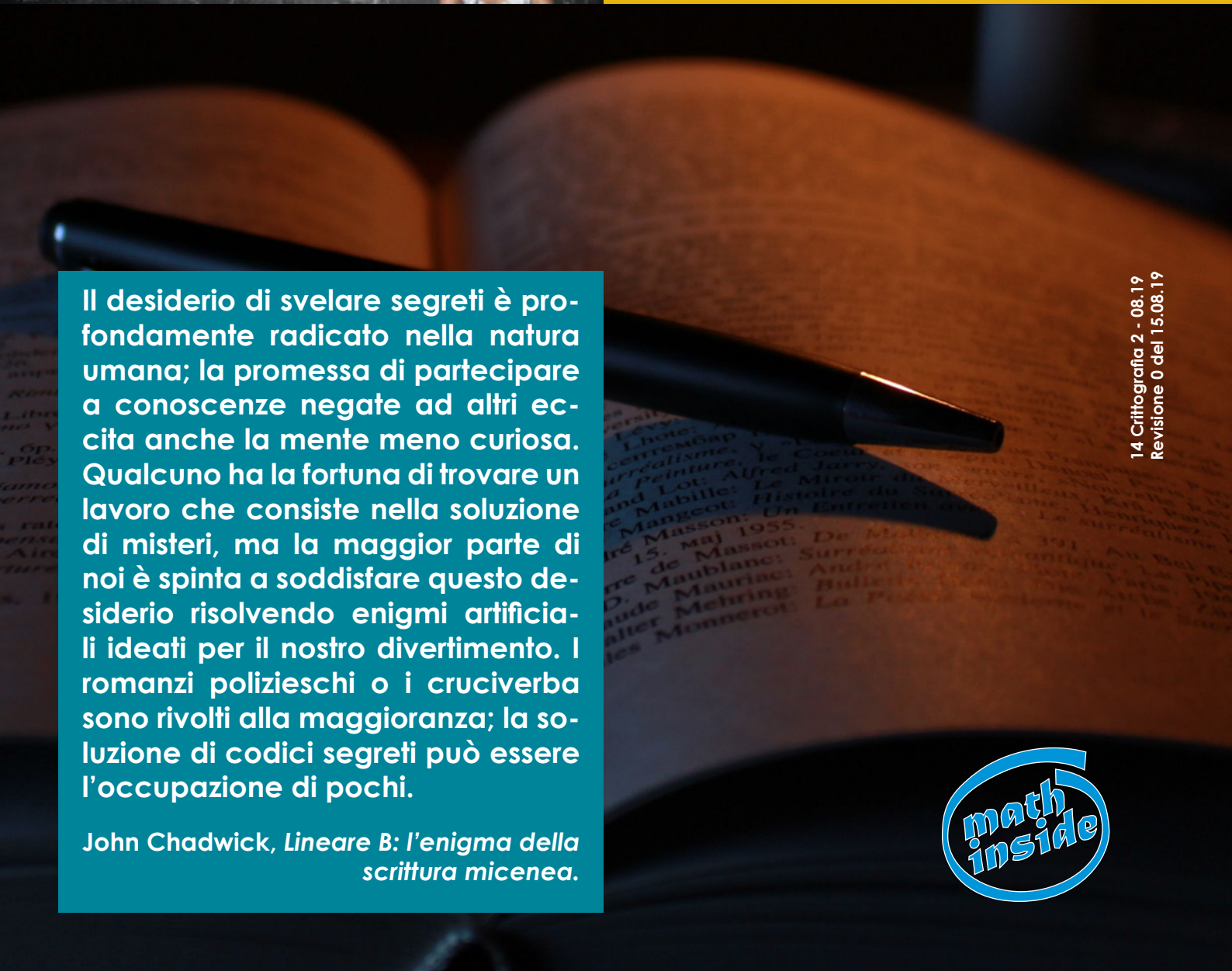
Crittografia - 2

Carta e penna non bastano!

Research in Action - RiA

researchinaction.it



Il desiderio di svelare segreti è profondamente radicato nella natura umana; la promessa di partecipare a conoscenze negate ad altri eccita anche la mente meno curiosa. Qualcuno ha la fortuna di trovare un lavoro che consiste nella soluzione di misteri, ma la maggior parte di noi è spinta a soddisfare questo desiderio risolvendo enigmi artificiali ideati per il nostro divertimento. I romanzi polizieschi o i cruciverba sono rivolti alla maggioranza; la soluzione di codici segreti può essere l'occupazione di pochi.

John Chadwick, *Lineare B: l'enigma della scrittura micenea.*

14 Crittografia 2 - 08.19
Revisione 0 del 15.08.19

La parola ria in inglese significa estuario, in particolare (dalla definizione che ne da l'Oxford Living Dictonaries):

> A long, narrow inlet formed by the partial submergence of a river valley ... the rias or estuaries contain very peculiar ecosystems which often contain important amounts of fish ... (a causa della loro natura, le rias o estuari contengono ecosistemi molto particolari che spesso contengono grandi quantità di pesce - www.eurotomic.com/spain/the-rias-altas-in-spain.php)

quindi questo prodotto che sarà realizzato grazie all'attività di alternanza scuola-lavoro di alcuni studenti del liceo scientifico G.B.Grassi di Latina - **www.liceograssilatina.org** - sarà un luogo virtuale da esplorare dove *pescare* molto materiale per la didattica laboratoriale.

Fare scienza

La scienza non è solo identificabile con la formula, il modello, la teoria. In altre parole la scienza non rappresenta solo un corpo di conoscenze organizzate e formalizzate. La scienza è anche e fondamentalmente ricerca. Una ricerca volta a conoscere e a capire sempre più e sempre meglio come è fatto e come funziona questo nostro complicatissimo mondo.

Fare scienza si identifica con l'interrogarsi, con l'indagare ed esplorare fatti e cose. Questo tipo di lavoro i bambini lo fanno spontaneamente sin dalla loro nascita ma si perde nel corso del percorso scolastico. L'intervento educativo deve tener conto di ciò e fornire stimoli, occasioni e strumenti per far acquisire agli studenti capacità sempre più ampie e affinate per poter compiere questo lavoro di indagine mantenendo viva (o risvegliando) la curiosità cognitiva, la voglia di sapere e di scoprire, la fiducia di poter capire.

Pensare in senso creativo, in campo scientifico, significa aggredire i problemi, attivare processi vivi dei pensiero, alimentare l'evoluzione dinamica dell'intelligenza duttile, dell'esercizio dell'intuizione e dell'immaginazione, della capacità di progettare e formulare ipotesi, di controllare e verificare quanto prodotto e ricercato.

Per questo è necessario bandire forme di apprendimento consumate entro schemi rigidi di elaborazione del pensiero e puntare al recupero della congettura, dell'ipotesi, di una coscienza scientifica aperta a interrogare ogni problematica.

La società odierna deve far fronte ad un rinnovamento scientifico e tecnico accelerato in cui lo sviluppo delle conoscenze scientifiche e la creazione di prodotti di alta tecnologia *(hi-tech)*, come anche la loro diffusione subiscono un'accelerazione sempre più rapida.

È necessaria, quindi, una diffusione della conoscenza in genere ed è indispensabile promuovere una nuova cultura scientifica e tecnica basata sull'informazione e sulla conoscenza. E quanto più è solida la base di conoscenze scientifiche scolastiche, tanto più si può approfittare dell'informazione e della conoscenza scientifica e tecnica.

» https://www.facebook.com/Research-in-Action-341307966417448/
» https://www.youtube.com/channel/UC1PA7Zu78RUMBJnkaiOR8kA/

Sommario dei contenuti

Crittografia 2 - Carta e penna non bastano!

Sommario dei contenuti

1. Introduzione 5

1.1. Prerequisiti 5
1.2. Obiettivi 5

2. Enigma 6

2.1. Come funziona 6
2.2. Qualche conticino 12
2.3. Proviamo a usare il simulatore mini 13
2.4. Forzare Enigma 13
2.5. Spedire e ricevere messaggi 14

3. Chiave pubblica: l'algoritmo RSA 15

3.1. Cifratura 15
3.2. Decifratura 16
3.3. Diamoci da fare 17

4. Enigma 20

4.1. Qualche conticino 20
4.2. Proviamo a usare il simulatore mini 21
4.3. Forzare Enigma 22

5. Chiave pubblica: l'algoritmo RSA 25

5.1. Diamoci da fare 25

6. Struttura della libreria 27

6.1. Enigma 27
6.2. Algortimo RSA 27

Blockly è un generatore di codice open source sostenuto da Google: https://developers.google.com/blockly/.

Materiale disponibile per questo laboratorio:

» il fascicolo con la prima parte del laboratorio (in formato PDF di circa 12MB): **http://researchinaction.it/materials/13-Crittografia-1.pdf**;

» il fascicolo con la seconda parte (questa) del laboratorio (in formato PDF di circa 6MB): **http://researchinaction.it/materials/14-Crittografia-2.pdf**;

» il simulatore di Enigma è descritto qui: **http://researchinaction.it/i-nostri-giochi/simulatore-enigma/**;

» la libreria, sviluppata con Blockly, si può provare sul campo: **http://researchinaction.it/myblockly/criptography.html** ed è descritta nel dettaglio qui: **http://researchinaction.it/laboratori/crittografia/**.

Per il materiale didattico a supporto del fascicolo visitare anche la pagina Download del sito dedicato al progetto: **http://researchinaction.it/download/**.

Per i videotutorial è possibile visitare il canale YouTube del progetto: **https://www.youtube.com/channel/UC1PA7Zu78RUMBJnkaiOR8kA**.

Crittografia 2

Carta e penna non bastano!

1. Introduzione

Questo laboratorio è stato sviluppato per la prima classe del liceo matematico ed è nato da una conversazione con la professoressa Lucilla Galterio, il progetto è stato coordinato da Gualtiero Grassucci (Iss G.B. Grassi di Latina).

Il desiderio di svelare segreti è profondamente radicato nella natura umana; la promessa di partecipare a conoscenze negate ad altri eccita anche la mente meno curiosa. Qualcuno ha la fortuna di trovare un lavoro che consiste nella soluzione di misteri, ma la maggior parte di noi è spinta a soddisfare questo desiderio risolvendo enigmi artificiali ideati per il nostro divertimento. I romanzi polizieschi o i cruciverba sono rivolti alla maggioranza; la soluzione di codici segreti può essere l'occupazione di pochi.

John Chadwick, Lineare B: l'enigma della scrittura micenea.

Per approfondire gli argomenti affrontati in questo laboratorio è possibile leggere, tra gli altri, Singh, S. - Codici & segreti. La storia affascinante dei messaggi cifrati dall'antico Egitto a internet.

Nella prima parte di questo laboratorio **(cfr. 13 - Crittografia 1)** abbiamo affrontato da un lato metodi di cifratura sempre più complessi e dall'altro meccanismi di analisi sempre più sofisticati in una continua lotta tra chi vorrebbe mantenere al sicuro dati, informazioni e messaggi e chi, invece, è assolutamente determinato a infrangere quei segreti.

A entrambi gli schieramenti, alla fine dell'ottocento, si presentano due problemi pricipali:

» le operazioni di cifratura (e quelle di decifrazione di un messaggio) sono diventate molto lunghe, complicate e a volte farraginose rendendo difficile completare il compito senza errori;
» il destinatario, per decifrare il messaggio, deve necessariamente essere a conoscenza anche della chiave che, in genere, è più corta e semplice del messaggio stesso e quindi, per forza di cose più facile da forzare.

Questi due problemi hanno disturbato i sonni di crittografi e criptoanalisti per decenni senza che si manifestasse una soluzione definitiva (che probabilmente non c'è) fino all'avvento delle prime macchine di calcolo meccaniche e poi dei moderni calcolatori elettronici. In questa seconda parte del laboratorio dedicato alla crittografia ci dedicheremo a due metodi, relativamente moderni ma evoluzione delle tecniche rinascimentali e ottocentesche, che hanno fornito, e in un certo senso ancora forniscono, soluzione ai due problemi segnalati.

1.1. Prerequisiti

Per affrontare questo laboratorio sono necessarie:

» conoscenze calcolo combinatorio (combinazioni, disposizioni, permutazioni);
» possono essere di aiuto (ma non sono essenziali) anche elementari conoscenze dei concetti di algoritmo, procedura, *coding*;

1.2. Obiettivi

Gli obiettivi della seconda parte sono essenzialmente:

» la costruzione di un simulatore della macchina Enigma;
» la conoscenza dei meccanismi alla base di Enigma;
» la conoscenza di una versione semplificata dell'algoritmo RSA;
» la capacità di valutare, per via empirica, la sicurezza di un metodo di cifratura.

2. Enigma

Una macchina Enigma, modello G, esposta nel 2005 al National Cryptologic Museum di Fort G. Meade in Maryland.
Si riconosce molto bene la tastiera e, immediatamente sopra, le lettere luminose. Nella parte più alta, i quattro ingranaggi che sembrano spuntare dalla macchina sono i rotori (nella versione costruita per prima i rotori erano solo tre).
CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=497329.

la prima difficoltà, la complessità delle operazioni di cifratura, oggi non è più un problema perchè la crittografia è ormai basata sulle enormi potenzialità di calcolo autumatico fornite dai moderni computer (vedremo meglio questo aspetto più avanti) ma già all'inizio del novecento si era cercata una soluzione ideando, progettando e infine costruendo macchine (meccaniche o elettriche, non elettroniche) capaci di svolgere tutte le operazioni in modo automatico.

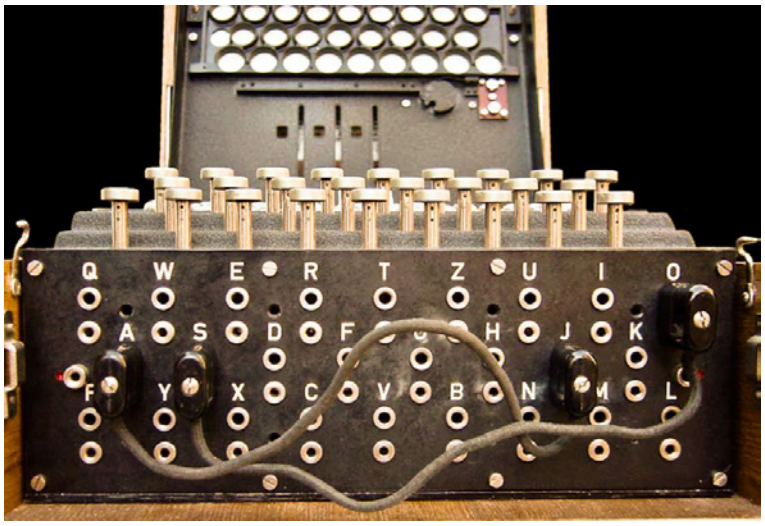
In realtà già nel XV secolo Leon Battista Alberti (Alberti, Leon Battista, *Dello scrivere in cifra*) aveva progettato un *disco cifrante* che rendeva meccaniche le operazioni di cifratura. Il suo disco permetteva una cifratura per sostituzione in cui l'alfabeto cifrante era modificato nel corso del messaggio attraverso l'inserimento nel testo di informazioni all'uopo.

Tornando alle macchine meccaniche, la più famosa è certamente Enigma. Progettata e costruita da Arthur Scherbius per il mercato civile con l'idea di proteggere le comunicazioni relative tra finanzieri e imprenditori, ma che in realtà divenne il principale metodo usato da marina, esercito e aeronautica tedesche nella seconda guerra mondiale per proteggere le comunicazioni da interferenze nemiche.

2.1. Come funziona

Enigma era composta da una tastiera, su cui l'operatore batteva il messaggio, un po' come fosse una macchina da scrivere meccanica, e da una serie di lettere che, illuminandosi una alla volta in corrispondenza della pressione di un tasto sulla tastiera, indicavano il simbolo cifrato.

Il cuore della macchina era costituito da (inizialmente) tre dischi rotanti sullo stesso asse (detti, per l'appunto *rotori*) su ognuno dei quali era presente un alfabeto cifrante. Alcuni contatti elettrici collegavano una lettera su un rotore con un simbolo su rotore successivo, questo era collegato, mediante ancora contatti elettrici, con una lettera sul terzo rotore realizzando in questo modo una cifratura per sostituzione con tre alfabeti cifranti.



Il pannello a prese multiple di una macchina Enigma. Si vedono chiaramente i collegamenti elettrici che scambiano la lettera S con la O e la lettera A con la J.
La foto è di Bob Lord (German Enigma Machine, uploaded in english wikipedia on 16. Feb. 2005 by en:User:Matt Crypto, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=258976).

A ogni pressione di un tasto però l'ultimo rotore girava sul proprio asse modificando così la cifratura. Dopo aver compiuto un giro completo, anche il secondo rotore ruotava compiendo 1/26 di giro e così poi anche il primo. Quindi la cifratura cambiava a ogni lettera/simbolo.

Un altro componente, il *riflessore*, costringeva il segnale elettrico ad attraversare di nuovo i tre rotori fino a illuminare la lettera cifrata. Il riflessore era davvero una buona idea, infatti riposizionando la macchina nella stessa configurazione e premendo il tasto corrispondente alla lettera cifrata si sarebbe ottenuta la corrispondente lettera in chiaro (infatti il segnale elettrico avrebbe attraversato i rotori esattamente in senso inverso, ma sullo stesso percorso).

La macchina era completata da un *pannello a prese multiple* posto anteriormente che permetteva all'operatore di scambiare sei coppie di lettere tra loro prima di attraversare i rotori, aggiungendo altre combinazioni a quelle già possibili (pur potendo *scambiare* tra loro anche meno di sei coppie, gli operatori avevano istruzione di usare sempre tutti i sei collegamenti tra coppie di lettere).

In conclusione, le operazioni di cifratura e decifratura erano davvero molto semplici se paragonate a quanto abbiamo visto nella prima parte di questo laboratorio. Per cifrare un messaggio il mittente doveva:

» configurare la macchina e prendere nota di questa configurazione (contatti sul pannello a prese multiple, disposizione e posizione iniziale dei rotori);
» cifrare il messaggio digitandolo sulla tastiera e trascrivendo i simboli corrispondenti che si illuminavano, questi simboli costituivano il messaggio cifrato.

Per decifrare lo stesso messaggio il destinatario doveva:

» impostare la macchina con la stessa identica configurazione usata dal mittente;
» decifrare il messaggio digitandolo sulla tastiera e trascrivendo le lettere che si illuminanvano in corrispondenza, queste lettere davano il messaggio in chiaro.

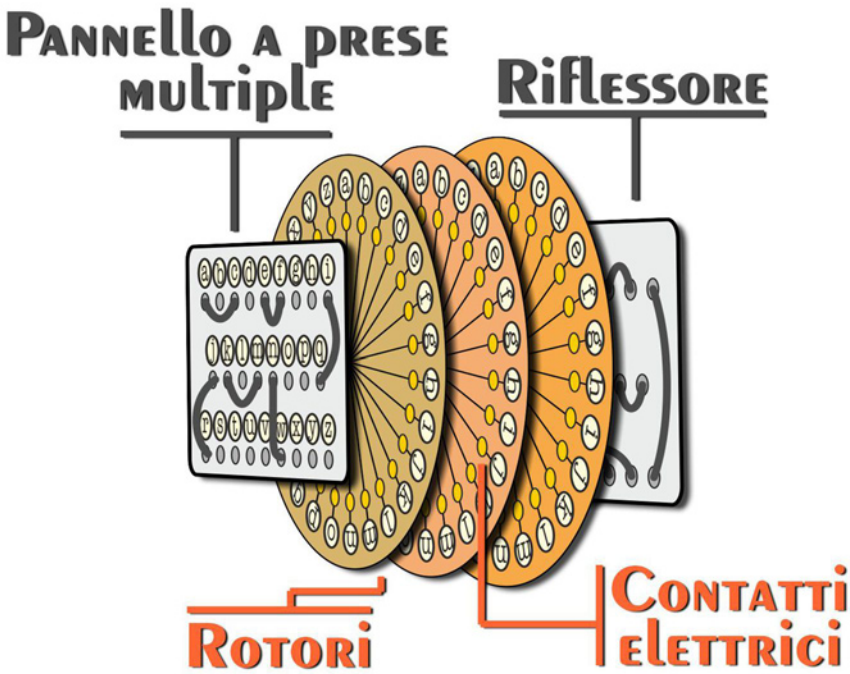
Tutto qui!

In sostanza i rotori cifravano usando il metodo di sostituzione, come si può capire facilmente, ma gli alfabeti cifranti (tre in tutto, tanti quanti i rotori) cambiavano ciclicamente, con un periodo molto lungo, a ogni carattere. La forza di Enigma stava proprio in questo!

Inoltre, grazie al riflessore, le operazioni di cifratura e decifratura erano pressoché identiche!

Il numero di configurazioni possibili, grazie soprattutto al pannello a prese multiple, era davvero enorme, rendendo impossibile una decriptazione del messaggio procedendo a tentativi (con l'uso della *forza bruta*)!

Bene. Se il funzionamento della macchina è chiaro, almeno nelle linee principali, possiamo iniziare a lavorarci un po' su.



Qui accanto lo schema di una macchina Enigma (privata della tastiera e delle lettere luminose). Sulla sinistra si nota il *pannello a prese multiple* con i sei cavi (collegamenti) che permettono di scambiare le lettere (per esempio la *a* è scambiata con la *c*). Al centro i tre *rotori*. I cerchi gialli sono i contatti che consentono al segnale elettrico di passare da un rotore all'altro (e quindi cifrare per sostituzione). Sulla destra il *riflessore* che *rimanda indietro* il segnale verso le lettere luminose (che, come detto, in questo schema non sono mostrate).

Blockly Google
A Visual Programming Language

Sul blog Research in Action è possibile utilizzare la libreria sviluppata con Blockly nel corso delle attività del progetto: http://researchinaction.it/myblockly/criptography.html
In particolare le funzioni *EnigmaCifra* e *EnigmaDecifra* permettono di cifrare e decifrare un testo fornendo la configurazione iniziale della macchina.
Blockly è un generatore di codice open source sostenuto da Google: https://developers.google.com/blockly/.

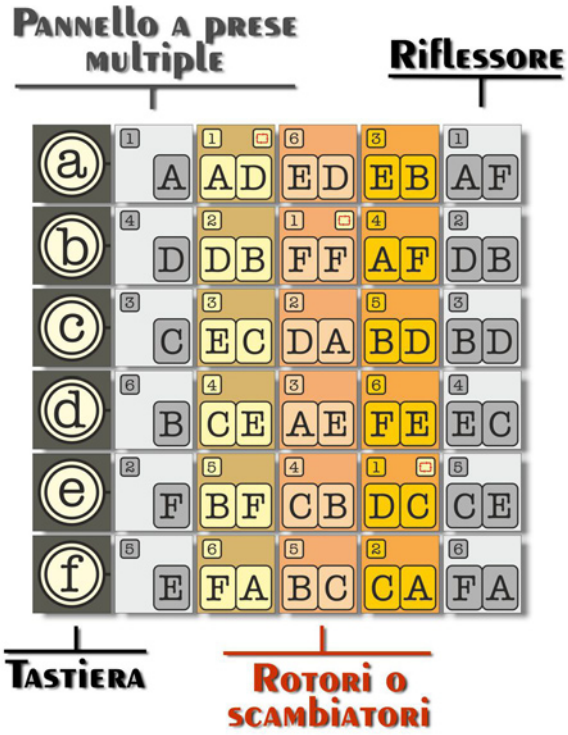
Enigma: il simulatore

Con pochissimo lavoro ci si può costruire un simulatore della macchina Enigma perfettamente funzionante senza bisogno di contatti elettrici o meccanismi meccanici. Certo, meno automatizzato, ma basato esattamente sulle stesse idee.

Anzi, i simulatori sono due. Il primo ricrea una versione *mini* della macchina, dotata di una tastiera di sole sei lettere ma il cui funzionamento è una replica fedele del funzionamento della macchina. Il secondo è una versione completa dello stesso simulatore con alfabeto di 26 lettere. Qui di seguito useremo la versione mini ma la versione completa funziona allo stesso modo.

Innanzitutto scaricate dal sito del progetto RiA il file in formato PDF contenente gli elementi del simulatore: **http://researchinaction.it/materials/enigmasimulator-all.pdf** e **http://researchinaction.it/materials/enigmasimulator-mini.pdf**.

Stampate le due pagine del file possibilmente a colori e su carta spessa o cartoncino e ritagliate i 36 quadrati: questi saranno gli elementi della nostra macchina Enigma. Disponete gli elementi come mostrato nella figura che segue.



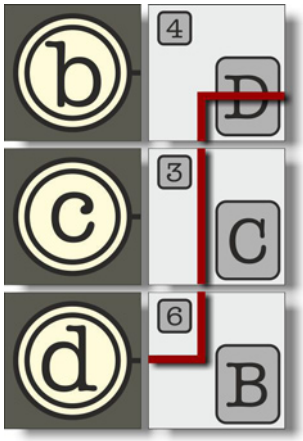
La prima colonna rappresenta la *tastiera*. La seconda il *pannello a prese multiple*, in questa configurazione sono state collegate (e quindi scambiate) le lettere *B* e *D*, infatti al tasto *b* della tastiera corrisponde l'elemento con la lettera *D* del pannello e viceversa, e le lettere *E* ed *F*, mentre tutti gli altri tasti non sono scambiati (tasto e lettera nel pannello sono uguali.

Le tre colonne (colorate) successive costituiscono i *rotori* mentre l'ultima rappresenta il *riflessore*. Le lettere luminose sono simulate dagli stessi componenti che costituiscono la tastiera (in altre parole, immaginiamo che i tasti si possano illuminare fungendo contemporaneamente da tastiera e da visore). I collegamenti elettrici sono simulati dalle lettere.

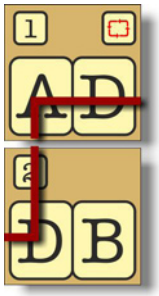
La figura che segue mostra le caratteristiche di un elemento.

Adesso siamo pronti per cifrare un testo, supponiamo di voler cifrare la lettera *d*: per determinare il simbolo corrispondente dobbiamo seguire i collegamenti fino al riflessore e poi indietro di nuovo fino alla tastiera/visore.

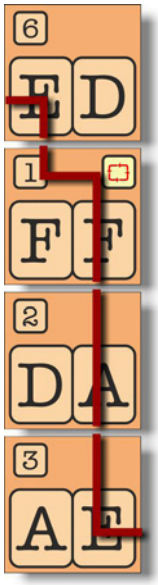
Partiamo quindi dal tasto *d*, dobbiamo cercare l'elemento corrispondente del pannello a prese multiple con la stessa lettera: è il numero 4 (vedi la figura che segue).



L'elemento adiacente nel primo rotore è il n. 2, visto che la lettera di entrata è la *D* dobbiamo spostarci sull'elemento dello stesso rotore la cui lettera di uscita è sempre *D* (come mostrato in figura), si tratta dell'elemento 1.



Passiamo al secondo rotore, l'elemento corrispondente è il n. 6. La lettera di entrata è la *E* e quindi cerchiamo l'elemento del secondo rotore con la lettera di uscita uguale, è il n. 3 (vedi figura).

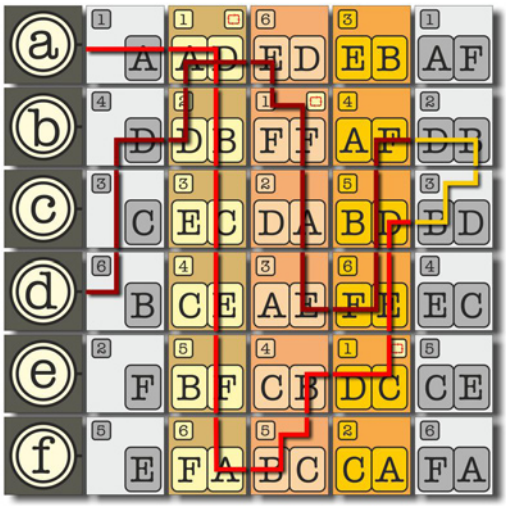


Poi il terzo rotore: l'elemento adiacente è il n. 6, lettera di entrata *F* che è collegata all'elemento n. 4 (lettera di uscita proprio *F*).

Siamo quasi a metà strada: al riflessore. L'elemento adiacente è il n. 2 che ha lettera di entrata *D* e quindi ci porta al n. 3 (stessa lettera di uscita).

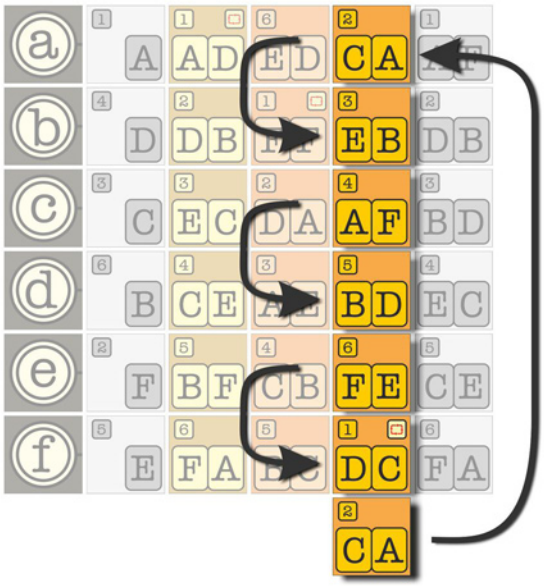
Adesso inizia il viaggio di ritorno. L'elemento n. 3 del riflessore è collegato all'elemento n. 5 del terzo rotore e così via ...

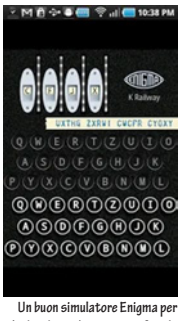
Nella figura qui sotto è mostrato tutto il percorso che riporta indietro fino alla tastiera/visore, per la precisione alla lettera *A* e quindi la lettera *d*, con queste impostazioni, è cifrata in *A*.



Un ottimo simulatore Enigma, per Windows facile da installare e da usare, si può trovare qui: http://users.telenet.be/d.rijmenants/en/enigma-sim.htm
L'applicazione permette di simulare diverse versioni della macchina e di salvare la configurazione usata per usi successivi.

Completata la cifratura di un carattere si deve simulare la rotazione del terzo rotore: tutti gli elementi sono spostati verso il basso di una posizione e l'ultimo (il n. 2 in questo caso) è portato nella prima posizione, quella più in alto.





Un buon simulatore Enigma per Android si può trovare su Google Play Store: *Enigma Simulator* di Franklin Heath Ltd. Come il precedente, anche questo è gratuito.

Se a questo punto l'elemento più in alto del terzo rotore ha il gancio di rotazione, identificato dall'icona ⬚, allora si deve simulare la rotazione anche del secondo rotore (allo stesso modo: tutti gli elementi sono spostati di una posizione verso il basso e l'ultimo è riportato in alto, in prima posizione) e, infine, se a questo punto l'elemento più in alto del secondo rotore ha il gancio di rotazione si deve ruotare anche il primo rotore!

Enigma: il simulatore

Il simulatore completo funziona allo stesso modo. Per costruirlo scaricate il file PDF ..., stampatelo su carta pesante o cartoncino, meglio se a colori, e ritagliate tutti gli elementi quadrati (sono leggermente più piccoli della versione mini). Una volta pronti disponeteli come nella figura qui a destra.

Per cifrare una lettera si procede come già detto:

» si parte dal tasto corrispondente alla lettera che si vuole cifrare;
» si passa al pannello a prese multiple (seconda colonna, in colore grigio) e si cerca l'elemento con la stessa lettera;
» ci si sposta sull'elemento corrispondente nel primo rotore (l'elemento che si trova sulla stessa riga), si legge la lettera di entrata (la prima, quella più a sinistra);
» si cerca, sempre nel primo rotore, l'elemento che ha la lettera di uscita uguale a quella di entrata appena letta;
» ci si sposta sul secondo rotore ... e si procede allo stesso modo fino ad arrivare al riflessore;
» si cerca l'elemento del riflessore cha ha la lettera di uscita uguale alla lettera di entrata che abbiamo appena letto;
» ci si sposta sul terzo rotore e si procede all'indietro, da destra verso sinistra, fino ad arrivare di nuovo alla tastiera.

È importante ricordare che nel percorso di ritorno in ogni elemento la lettera a destra è quella di entrata e la lettera a sinistra è quella di uscita!

Una volta cifrato un carattere, si spostano tutti gli elementi del terzo rotore di una posizione verso il basso e l'ultimo viene spostato in alto, nella prima riga. Se a questo punto l'elemento più in alto del terzo rotore ha il gancio di rotazione, identificato dall'icona ⊡, allora si deve simulare la rotazione anche del secondo scambiatore e, infine, se a questo punto l'elemento più in alto del secondo rotore ha il gancio di rotazione si deve ruotare anche il primo scambiatore!

Per la decifrazione si procede allo stesso modo: si sistema il simulatore così come era prima di cifrare il primo carattere e si procede (de)cifrando, con la stessa procedura, i simboli del messaggio cifrato.

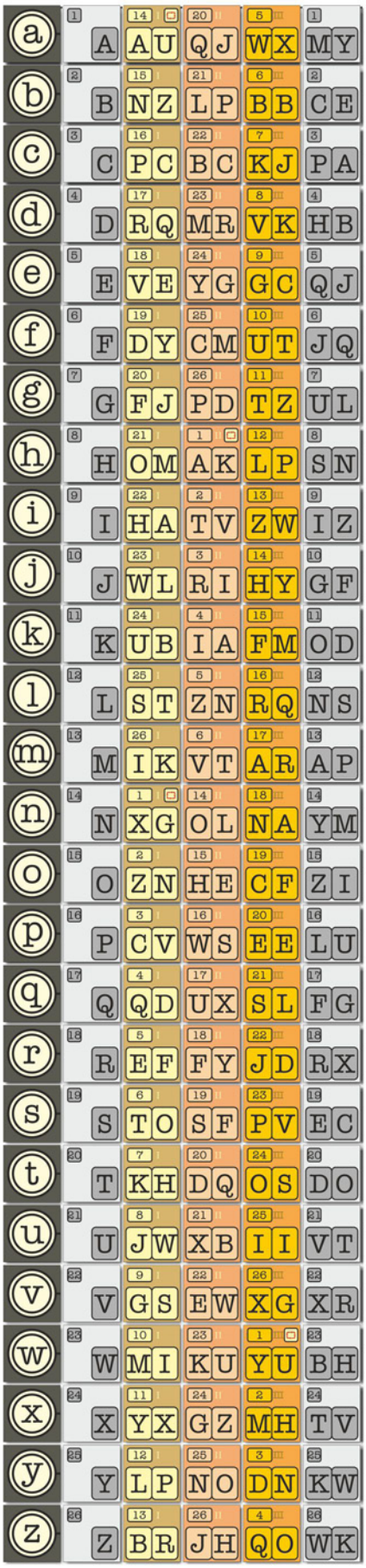
La configurazione del simulatore (che il destinatario deve conoscere per procedere alla decifrazione del testo) è determinata dalle coppie di lettere scambiate e dal numero identificativo dell'elemento di ciascun rotore. Per esempio, la configurazione del simulatore completo mostrata qui accanto è:

... I-14 II-20 III-5

dove i *tre puntini* indicano che nessuna lettera è stata scambiata e i numeri romani I, II e III indicano il rotore. La configurazione del mini simulatore mostrata a pagina 8 è:

B-D E-F I-1 II-6 III-3

dove con *B-D* si intende che le lettere *B* e *D* sono scambiate tra loro e così le lettere *E-F*. Non è necessario specificare la configurazione del riflessore che è invariabile.



Proviamo ora a impostare una configurazione per il nostro simulatore. Useremo la versione mini per comodità di rappresentazione e lettura ma le operazioni saranno esattamente le stesse anche per la versione completa.

Dobbiamo decifrare un messaggio e sappiamo che la configurazione deve essere la seguente:

B-C A-D II-1 I-1 III-2

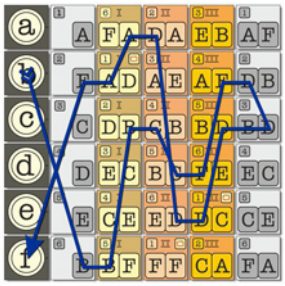
Iniziamo dal *pannello a prese multiple* (gli elementi in colore grigio che hanno una sola lettera). Le lettere *B* e *C* sono scambiate e quindi in corrispondenza del tasto *b* metteremo l'elemento 3 (con la lettera *C*) e in corrispondenza del tasto *c* l'elemento 6 (con la lettera *B*). Stessa cosa per le lettere *A* e *D*: tasto *A* corrispondente all'elemento 4 e tasto *D* corrispondente all'elemento 1. Le lettere *E* ed *F* non sono scambiate e quindi in corrispondenza del tasto ci sarà l'elemento con la stessa lettera.

Ora i *rotori*. Attenzione: il primo rotore da sistemare, immediatamente dopo il pannello a prese multiple, è il n. II (i cui elementi sono di colore rosa). L'elemento numero 1 va messo per primo, in alto, e via via gli altri verso il basso seguendo l'ordine numerico. Successivamente va sistemato il rotore n. I (i cui elementi sono di colore marrone). Per primo l'elemento n. 1 e poi gli altri seguendo la numerazione. Infine l'ultimo, il n. III a partire dall'elemento n. 2 e poi i successivi. Notare che l'elemento n.1 finisce nella posizione più in basso.

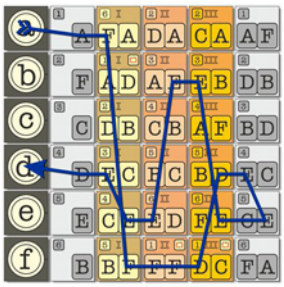
Nel nostro simulatore (com'era anche nella realtà) il riflessore non poteva essere modificato per cui inseriamo gli elementi dal n.1 (in alto) al n. 6 in basso (vedi figura qui di seguito).

Un ultimo esempio, ancora con il simulatore mini, cifriamo la parola *bacca*. Impostiamo la macchina secondo la configurazione:

B-F I-6 II-2 III-3



b->F

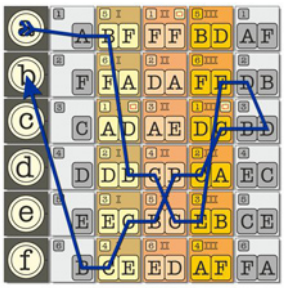


a->D

c->F

Notare nella figura precedente la rotazione di tutti e tre i rotori.

c->F



a->B

In conclusione, *bacca* è cifrata in *FDFFB*.

L'idea di proporre in questo laboratorio la costruzione di un simulatore di Enigma e, in particolare, la versione mini del simulatore, sono nate dopo la lettura di Singh, S. - Codici & segreti. La storia affascinante dei messaggi cifrati dall'antico Egitto a internet.

2.2. Qualche conticino

Innanzitutto riflettiamo un momento sul meccanismo di cifratutra e decifratura ...

Cosa doveva conoscere il destinatario del messaggio cifrato (oltre naturalmente al messaggio stesso) per poter decifrare correttamente la comunicazione ricevuta?

In realtà, come vedremo brevemente nelle soluzioni **(cfr. 4.1 Qualche conticino a pagina 20)** questa è un po' la debolezza (e non la sola) di questo sistema apparentemente inattaccabile.

Trascura per ora il pannello a prese multiple, considera quindi la macchina composta solo dai tre rotori e dal riflessore.

Quante sono le possibili configurazioni di una macchina Enigma composta di tre rotori (o scambiatori) e con un alfabeto anglosassone di 26 lettere?

Parecchie, non è vero? Ma non è finita qui, i tre rotori possono essere scambiati di posto tra di loro (per esempio, potremmo modificare la macchina in modo che gli scambiatori siano, da sinistra verso destra, il numero II, il numero III e infine il numero I).

Considerando anche la possibilità di scambiare tra loro i tre rotori, quante sono le possibili configurazioni della macchina Enigma (la stessa che abbiamo consuderato qui sopra)?

Ma l'ideatore di Enigma non era ancora soddisfatto. Teniamo ora conto anche della possibilità di scambiare tra loro le lettere grazie alla presenza del pannello a prese multiple.

Considerando inoltre la possibilità di scambiare tra loro sei coppie di lettere (sempre con la possibilità di scambiare la posizione dei rotori), quante diventano le possibili configurazioni di Enigma?

Come suggerimento, per calcolare le possibili configurazioni del pannello a prese multiple, procedi in questo modo: cerca di calcolare in quanti modi diversi puoi realizzare il primo collegamento tra due lettere, a questo punto calcola in quanti modi puoi calcolare due delle lettere rimanenti ... e così via fino al sesto collegamento. Ricorda che gli operatori di Enigma erano obbligati a usare sempre e comunque tutti i sei collegamenti possibili **(cfr Come funziona a pagina 6)**.

La residenza principale della tenuta di Bletchley Park. Allo scoppio della seconda guerra mondiale il governo britannico fece di questa proprietà la sede principale dei servizi di criptoanalisi e decifrazione.
È proprio qui che alcune delle migliori menti del paese lavorarono alla decodifica delle comunicazione e dei messaggi del nemico ed è sempre qui che, al termine di un duro lavoro, finalmente fu forzata Enigma!

Se hai fatto il conto bene, ti sarai reso conto che, nel complesso, questa macchina, anche nella sua prima versione, aveva un numero di possibili configurazioni davvero straordinario. E pensare che nel corso della seconda guerra mondiale ne furono costruite versioni via via più potenti fornite di rotori di ricambio che potevano sostituire i tre originali o aumentando il numero di scanbiatori collegati. Davvero un impresa ardua decifrare un messaggio senza conoscere la configurazione iniziale usata dallo scrivente!

2.3. Proviamo a usare il simulatore mini

Prepara la versione mini del simulatore **(cfr.. Enigma, il simulatore a pagina 8)**, è giunto il momento di mettere alla prova il meccanismo di cifratura e il nostro mini simulatore.

Configura il mini simulatore con la chiave *B-C A-D II-1 I-1 III-2*. Si tratta della stessa configurazione che abbiamo impostato nell'esempio che trovi **a pagina 11**.

Cifra la parola *fede*.

Ricorda che dopo la cifratura di ogni lettera lo scambiatore più a destra deve *ruotare* di una posizione e se dopo la rotazione l'elemento con il gancio di rotazione ⊡ si trova nella posizione più in alto, anche lo scambiatore successivo deve ruotare!

Osserva la parola cifrata, da quali simboli sono state sostituite le due *e* presenti nel testo in chiaro? È un vantaggio questa caratteristica? Perchè?

Come avevamo previsto, due lettere uguali sono cifrate in modo diverso. Un po' come avveniva con il metodo di Vigenère che abbiamo visto nella prima parte di questo laboratorio (cfr. 13 - Crittografia 1).

Ora prova a decifrare la parola che hai ottenuto. Ricorda che la macchina deve essere nella stessa configurazione usata per la cifratura.

Se tutto è andato bene, dovresti avere di nuovo la parola in chiaro: *fede*. E tutto semplicemente partendo dalla stessa configurazione ed eseguendo le stesse operazioni!

2.4. Forzare Enigma

La decifrazione di un messaggio nascosto criptato con una macchina Enigma fu, durante la guerra, un compito davvero difficile anzi, impossibile senza il supporto del calcolo automatico. Qui vogliamo proporre un esempio che, per quanto semplificato e applicato a un mini simulatore come in nostro, sarà comunque veramente complesso! L'obiettivo è di dare un'idea della difficoltà incontrate dal gruppo di *Bletchley Park* quando furono chiamati a decifrare le comunicazioni tedesche durante la guerra.

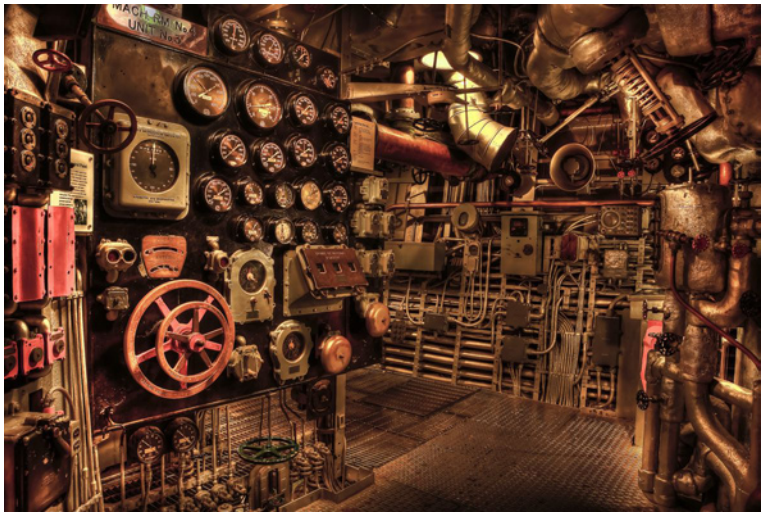
Con il simulatore in versione mini è stata cifrata una parola ottenendo *FDFFB*, sappiamo per certo che la parola in chiaro inizia con le lettere *ba*. Prova a ricostruire la configurazione iniziale del mini simulatore usata per cifrare la frase.

Si tratta, in pratica, di provare varie combinazioni fino a trovare quella corretta.

Potrebbe non essere facile rispondere al quesito precedente, cerchiamo di capire quanto è difficile ricostruire una configurazione del mini simulatore.

La macchina Enigma fu particolarmente utile per la comunicazione tra il comando della Kriegsmarine germanica e i sommergibili in Atlantico e, di conseguenza, per gli alleati, la decifrazione dei messaggi fu vitale per individuare e proteggere i convogli che attraversavano l'oceano per rifornire la Gran Bretagna.

Quante sono le combinazioni possibili del nostro mini simulatore?



Possiamo usare lo stesso metodo con il quale abbiamo affrontato il calcolo della macchina Enigma **(le cui soluzioni sono a pagina 21)** ma tieni conto che nel nostro simulatore mini non siamo obbligati a usare tutti i collegamenti possibili (che in ogni caso non possono essere più di tre, visto che è una macchina che ha un alfabeto di soli sei caratteri).

Se hai ricostruito la configurazione del mini simulatore, decifra l'intera frase.

Si tratta di una frase di Alan Mathison Turing, matematico britannico, il cui lavoro negli anni '40 contribuì in modo decisivo alla vittoria su Enigma!

2.5. Spedire e ricevere messaggi

Concludiamo questo capitolo dedicato alla macchina Enigma lavorando con il simulatore completo **(cfr.. Enigma, il simulatore a pagina 8)**. Per questo esercizio dovreste essere almeno due o due gruppi: ciascun gruppo fungerà sia da mittente che da destinatario simulando uno scambio di messaggi.

Ognuno dei due gruppi, dopo aver deciso una configurazione del simulatore, cifra una frase e passa all'altro gruppo la configurazione scelta e il messaggio cifrato. Poi ciascun gruppo decifra il messaggio ricevuto.

Al termine valutate la correttezza del lavoro fatto confrontando le versioni in chiaro e quelle decifrate di ciascun messaggio.

3. Chiave pubblica: l'algoritmo RSA

Il testo generato da una macchina Enigma era davvero sicuro, difficilissimo da decifrare per chi non doveva aver accesso al contenuto ma semplice da produrre e da decriptare per il mittente autorizzato: era sufficiente avere una macchina Enigma e conoscerne la configurazione da usare! Tutto perfetto ... oppure no?

Il punto debole sta proprio in questo ultimo punto: la configurazione. Nel corso della guerra navi e u-boot tedeschi solcavano l'oceano portandosi dietro una macchina Enigma ma anche un *librone* che conteneva le configurazioni da usare per la cifratura e decifratura per ogni giorno e ora di navigazione. Se il nemico però si fosse impadronito di questo manuale tutte le comunicazioni sarebbero state in pericolo e si sarebbe dovuto procedere rapidamente alla distribuzione di una nuova serie di configurazioni, diversa dalla precedente! Un lavoro tutt'altro che semplice se si dovevano raggiungere i sommergibili in navigazione. Infatti non era possibile comunicare via radio le configurazioni della macchina, dovevano essere consegnate fisicamente, su carta!

In effetti ogni codice che abbiamo affrontato in questo percorso ha il proprio punto debole nella trasmissione (o nella scelta, nel caso di Enigma) della chiave che deve essere conosciuta sia dal mittente che dal destinatario, ma tenuta nascosta a chiunque altro.

Nel 1977 Ronald Rivest, Adi Shamir e Leonard Adleman sviluppparono un algoritmo che, miracolo, non richiedeva la segretezza della chiave: il primo metodo di cifratutra *a chiave pubblica*! In pratica l'algoritmo RSA, dalle iniziali dei cognomi dei tre, è quello in uso in tutto il mondo per le comunicazioni diplomatiche, militari, finanziarie, ...

L'idea di base è davvero stupefacente per la sua semplicità: in matematica è molto più semplice calcolare il prodotto di due numeri primi rispetto all'operazione di determinare i fattori primi di un intero. E se l'intero è molto grande, o grandissimo, questo calcolo può richiedere mesi o anni anche ai computer più potenti. Tutto qui!

Il modulo di due numeri interi a e b è a mod b ed è definito come il resto della divisione di a per b. Siamo in un certo senso abituati all'operatore modulo perchè lo usiamo quotidianamente nel calcolo delle ore: se abbiamo una riunione alle 11 di mattina che durerà 3 ore sappiamo che finirà alle 2 del pomeriggio, infatti (11+3) mod 12 è 2 (il resto della divisione di 14 per 12. Per esempio: 7 mod 26 è 7 perchè dividendo 26 per 7 otteniamo zero come quoziente e 7 come resto, ma anche 33 mod 26 fa 7 perchè 33 diviso 26 fa uno con il resto ancora di 7 mentre 26 mod 26 fa zero!
É bene notare che sia a che b possono essere numeri negativi per cui, per esempio, -3 mod 26 fa 23, infatti il resto della divisione di -3 per 26 è proprio 23.

3.1. Cifratura

Innanzitutto è bene precisare che l'algoritmo RSA opera su numeri interi e non su caratteri, quindi la prima cosa da fare è trasformare in qualche modo il testo in una sequenza di numeri. Supponendo di averlo già fatto, vediamo come è possibile cifrare un numero intero con questo metodo.

Sia M il messaggio in chiaro (come detto un numero), il procedimento può essere schematizzato in questo modo:

- si scelgono due numeri primi p e q, sufficientemente grandi;
- si calcola $N = pq$ (il prodotto di p e q), il numero N sarà la prima parte della chiave pubblica;
- contemporaneamente si sceglie un numero e che sia primo con $\varphi(N) = (p-1)(q-1)$, questo numero costituirà la seconda parte della chiave pubblica;
- si calcola il valore cifrato C come $C = M^e \bmod N$

A questo punto si comunicano al destinatario il numero cifrato C e la chiave (M, e) e il gioco è fatto!

Facciamo un esempio semplice, scegliendo numeri piuttosto piccoli per seguire meglio i passaggi. Sia per esempio $M = 2$, scegliamo $p = 3$ e $q = 5$ per cui $N = 15$, considerato che

$$(p-1)\cdot(q-1) = 2 \cdot 4 = 8$$

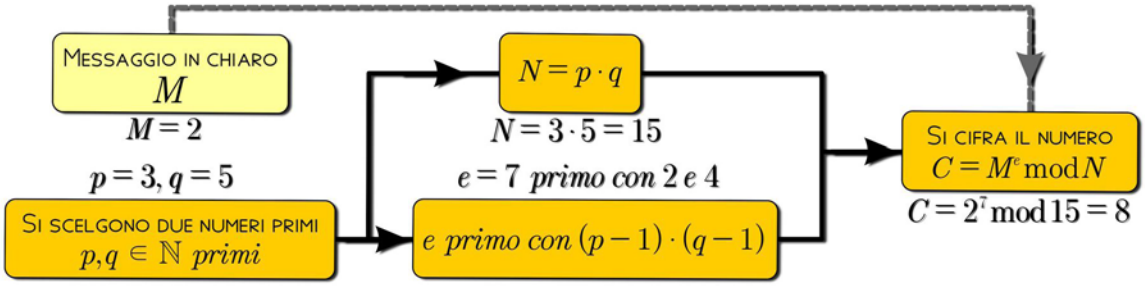
possiamo scegliere $e = 7$, che è primo con otto (oltre a essere primo esso stesso, ma questo non è indispensabile).

Sul blog Research in Action è possibile utilizzare la libreria sviluppata con Blockly nel corso delle attività del progetto: http://researchinaction.it/myblockly/criptography.html
In particolare le funzioni RSACifra e RSADecifra sono realizzate implementando i due algoritmi descritti in queste pagine.
Blockly è un generatore di codice open source sostenuto da Google: https://developers.google.com/blockly/.

A questo punto calcoliamo

$$C = 2^7 \bmod 15 = 128 \bmod 15 = 8$$

Questo è il numero cifrato da inviare al mittente. La figura che segue mostra uno schema dei passi da compiere per la cifratura usando l'algoritmo RSA e i pochi calcoli necessari (gli stessi eseguiti per il nostro esempio).



3.2. Decifratura

Mettiamoci ora nei panni del mittente che deve decifrare il messaggio ricevuto. Il mittente deve innanzitutto scegliere un numero d tale che $ed - 1$ sia multiplo di $\varphi(N) = (p-1)(q-1)$, dopodichè può procedere alla decifrazione del messaggio calcolando

$$M = C^d \bmod N$$

Anche più semplice, come meccanismo, della cifratura. Ricordiamo però che il mittente deve conoscere non solo il messaggio C, ma anche la chiave composta dai numeri N ed e (ma soprattutto, e questo è davvero importante, i due numeri primi p e q da cui si ricava N, sono proprio questi due numeri a essere la parte *segreta* della chiave).

Applichiamo questo metodo alla decifratura dell'esempio che abbiamo fatto in precedenza. Sappiamo che $C = 2$ e che $N = 15$ ed $e = 7$.

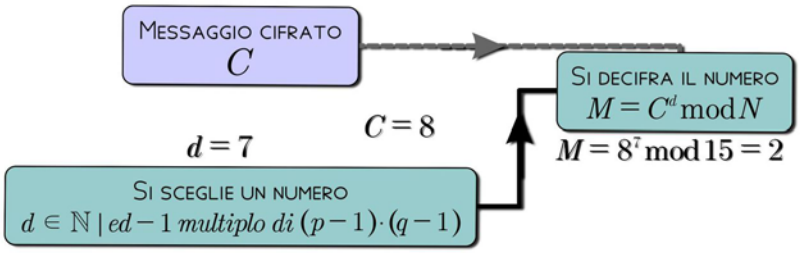
Dobbiamo scomporre il numero N in un prodotto di due primi e quindi $N = 3 * 5$ da cui deduciamo che $p = 3$ e $q = 5$ (o anche $p = 5$ e $q = 3$ ma è indifferente). Ora sappiamo che $(p-1)(q-1)$ è pari a otto e possiamo scegliere un numero d in modo che $ed - 1$ sia multiplo proprio di questo prodotto. Se $d = 7$ abbiamo che $ed - 1 = 48$ che è multiplo di 8, bene. Il fatto che d sia uguale a e è dovuto alla estrema semplicità dell'esempio, in generale i due numeri sono diversi tra loro.

Concludiamo decifrando il messaggio:

$$M = 8^7 \bmod 15 = 2097152 \bmod 15 = 2$$

Proprio quello che ci aspettavamo. Un procedimento quasi magico!

Nella figura che segue uno schema con le operazioni da eseguire per la decifratura.



Il calcolo delle due espressioni M^e mod N e C^d mod N può diventare impossibile con le normali calcolatrici perchè le potenze crescono rapidamente al crescere degli esponenti ma c'è un piccolo trucco che si può usare per mantenere i numeri entro limiti ragionevoli.
Infatti le proprietà delle potenze e dell'operatore modulo, usate insieme, permettono di scomporre, per esempio, M^e mod N come il prodotto M^a mod N * M^b mod N dove $e = a+b$.
In pratica 8^7 mod 15 può diventare, per esempio: 8^4 mod 15 * 8^2 mod 15 * 8^1 mod 15, più facile da calcolare ma soprattutto alla portata di una normale calcolatrice.

Normalmente, nell'uso reale dell'algoritmo RSA, i due primi sono molto grandi e quindi il loro prodotto è ancora più grande. Negli esempi che stiamo facendo, pensati per essere eseguiti con carta, penna e calcolatrice, abbiamo scelto primi piuttosto piccoli ma dobbiamo avere l'accortezza di fare in modo che il prodotto $N = p \times q$ sia maggiore di tutti gli interi usati per codificare i caratteri.

Precisazioni

La conoscenza della chiave si è resa necessaria in due passi dell'algoritmo di decifratura:

» Il numero N è stato usato per determinare i due primi p e q. Ricordiamo che N è pubblico ma non lo sono i suoi fattori, è proprio questo il cuore del metodo: se i due primi sono molto grandi la fattorizzazione del prodotto è estremamente difficile o comunque così dispendiosa in termini di tempo che le informazioni secretate non sono più utili quando si riesce a decifrarle forzando la protezione. Mittente e destinatario dovranno accordarsi, all'inizio del loro rapporto di corrispondenza, per una tabella di numeri (e relative coppie di primi) da usare, la differenza rispetto per esempio a Enigma sta nel fatto che non è necessario accordarsi su quale numero usare, visto che conoscendo N chi dispone della tabella può ricavare p e q.

» Il numero e (anch'esso pubblico) è necessario per la scelta del numero d ma quest'ultimo dipende dal prodotto $(p-1)(q-1)$ e quindi, di nuovo, dalla fattorizzazione di N.

In pratica la sicurezza del metodo è garantita dalla difficoltà di scomporre in fattori il prodotto dei due primi, non è una sicurezza illimitata, *per sempre*: il messaggio è sicuro finchè la fattorizzazione non ha successo, ma questa scomposizione potrebbe richiedere talmente tanto tempo da far diventare obsolete le informazioni contenute nel messaggio cifrato e quindi inutile la forzatura del codice.

3.3. Diamoci da fare

Sporchiamoci le mani e mettiamo alla prova l'algoritmo RSA. Vogliamo cifrare la frase *Quando le cose si surriscaldano, le nuvole si dissipano o scompaiono* usando il metodo ideato da Rivest Shamir e Adleman o meglio, una sua versione semplificata.

Cifratura

Ricordiamo che l'algoritmo RSA opera su numeri per cui dobbiamo innanzitutto trasformare la frase da cifrare in una serie di numeri.

Individua un metodo, una codifica, che associ a ogni carattere dell'alfabeto anglosassone un numero intero positivo. Scegli un meccanismo facile e fai in modo che gli interi non siano troppo grandi.

Nella realtà l'algoritmo RSA non opera sui singoli caratteri (in questo caso l'algoritmo sarebbe attaccabile con l'analisi delle frequenze che abbiamo affrontato in 13 - Crittografia 1) ma qui abbiamo solo lo scopo di familiarizzare con la cifratura RSA e quindi possiamo scegliere una codifica delle lettere semplice, anche banale.

Trasforma la frase da cifrare, *Quando le cose si surriscaldano, le nuvole si dissipano o scompaiono*, in una serie di numeri interi usando la codifica che hai scelto.

Questo è un passo indispensabile, ora siamo pronti per la codifica.

Scegli una chiave e cifra la frase usando l'algoritmo RSA.

Ricorda che scegliere una chiave equivale a individuare due numeri primi p e q e un numero e che sia primo con il prodotto $(p-1)(q-1)$. I due primi non devono essere troppo grandi perchè, come già detto, le potenze che appaiono nella codifica diventano rapidamente intrattabili anche con le migliori calcolatrici. In precedenza abbiamo suggerito un metodo per *spezzare* il calcolo di un'espressione del tipo $M^e \bmod N$ in potenze più semplici **(cfr. la nota a margine a pagina 16)**. Notare che il *messaggio* cifrato in realtà consiste di una lista di numeri interi.

Sul blog Research in Action è possibile utilizzare la libreria sviluppata con Blockly nel corso delle attività del progetto: http://researchinaction.it/myblockly/criptografy.html
In particolare le funzioni *RSACifra* e *RSADecifra* sono realizzate implementando i due algoritmi descritti in queste pagine.
Blockly è un generatore di codice open source sostenuto da Google: https://developers.google.com/blockly/.

Per l'operazione inversa possiamo rendere la cosa un po' più interessante. Se state lavorando in gruppo o, meglio, ci sono più gruppi che affrontano lo stesso laboratorio, accordatevi prima su una codifica comune che converta caratteri in numeri interi e dividetevi in due *team*, ogni *team* svolge contemporaneamente il ruolo di mittente e destinatario e lavora separatamente ai quesiti che proponiamo qui di seguito.

Ora scegliete una chiave e cifrate una (breve) frase di vostra scelta.

Questa operazione ormai dovrebbe essere familiare, seguite le stesse raccomandazioni che abbiamo suggerito poco fa. Come già detto il testo cifrato altro non sarà che una lista di interi.

Ora passiamo alla decifratura del messaggio criptato dall'altro gruppo. Passate all'altro gruppo il messaggio cifrato (la lista di interi) e la chiave (i numeri N ed e) e, al contrario, chiedete all'altro gruppo testo criptato e chiave. Ricordate che la chiave (pubblica) è composta solo dal prodotto N (e non dai due primi p e q) e dal numero e.

Decifrate il messaggio!

Per decifrare il testo dovete nell'ordine:

» scomporre il numero N nel prodotto di due primi p e q;
» calcolare il prodotto $\varphi(N) = (p-1)(q-1)$ e scegliere un numero d in modo che $ed - 1$ sia un multiplo di $\varphi(N)$, conviene scegliere interi piccoli e procedere via via per tentativi;
» a questo punto decifrate il messaggio (dovete decifrare uno a uno tutti i numeri della lista).

Completate il lavoro trasformando di nuovo in testo la lista dei numeri decifrati e confrontatelo con la frase originale che aveva scelto l'altro gruppo.

Se tutto ha funzionato, dovremmo essere riusciti a trasmettere un messaggio criptato con l'algoritmo RSA.

Un particolare di Colossus, la macchina elettrica usata a Bletchley Park per decifrare Enigma.
Solo una grande potenza di calcolo poteva permettere di provare tutte le possibili configurazioni in un tempo ragionevole!

4. Enigma

4.1. Qualche conticino

Cosa doveva conoscere il destinatario del messaggio cifrato (oltre naturalmente al messaggio stesso) per poter decifrare correttamente la comunicazione ricevuta?

È chiaro che il destinatario per decifrare il messaggio deve conoscere la configurazione della macchina (quali lettere scambiare nel pannello multifunzione, quali rotori, la loro disposizione e posizione iniziale, ...). A questo scopo reparti terrestri e unità navali tedesche, nel corso della guerra, avevano un calendario che riportava, per ciascun giorno e per un periodo di tempo piuttosto lungo (anche svariati mesi), la configurazione iniziale di Enigma da usare in ciascun giorno del calendario.

In realtà lo scrivente all'inizio del messaggio, cifrato con la configurazione indicata nel calendario, descriveva una diversa impostazione della macchina che veniva usata nel resto del dispaccio e quindi, in un certo senso, ogni messaggio aveva una configurazione propria. Il destinatario interpretava la prima parte del testo, modificava le impostazioni di conseguenza e poi proseguiva con la decriptazione.

Quante sono le possibili configurazioni di una macchina Enigma composta di tre rotori (o scambiatori) e con un alfabeto anglosassone di 26 lettere?

Ogni rotore aveva, ovviamente, 26 posizioni possibili (corrispondenti ognuna a una lettera dell'alfabeto angolosassone) e per ogni posizione del primo scambiatore ne abbiamo 26 per il secondo e ancora 26 per il terzo. In totale $26 \times 26 \times 26$ posizioni: 15.576. Non moltissime in realtà ma la funzione dei rotori era soprattutto quella di impedire l'analisi delle frequenze. La macchina Enigma-G, una versione successiva usata principalmente dalla marina, aveva la possibilità di usare quattro rotori scelti da un insieme di otto, chiaramente per aumentare il numero di combinazioni possibili.

Considerando anche la possibilità di scambiare tra loro i tre rotori, quante sono le possibili configurazioni della macchina Enigma (la prima che abbiamo considerato qui sopra, quella con tre scambiatori)?

Tutte i possibili ordinamenti del tre rotori sono $3! = 6$, in pratica le permutazioni di tre elementi, tutti i modi in cui possiamo disporre tre oggetti tenendo conto del loro ordine. Le configurazioni della macchina, tenendo anche conto di questa caratteristica, si ottengono moltiplicando le possibili posizioni dei rotori per tutti i possibili ordinamenti: $15.576 \times 6 = 105.456$. Sono già parecchie di più!

Considerando inoltre la possibilità di scambiare tra loro sei coppie di lettere (sempre con l'opportunità di scambiare la posizione dei rotori), quante diventano le possibili configurazioni di Enigma?

Qui il calcolo è un po' più complicato. La prima versione di Enigma permetteva, come detto nel

quesito, di scambiare tra loro sei coppie di lettere, in pratica, si tratta di chiedersi in quanti modi diversi possiamo formare sei coppie a partire dall'alfabeto anglosassone di 26 lettere. Procediamo una coppia alla volta: calcoliamo in quanti modi possibili possiamo formare la prima coppia, in altre parole quante coppie - non ordinate - possiamo creare con 26 lettere, si tratta delle combinazioni di 26 lettere a due a due:

$$C_{26,2} = \frac{26 \cdot 25}{2!} = 325$$

Un ottimo simulatore Enigma, per Windows facile da installare e da usare, si può trovare qui: http://users.telenet.be/d.rijmenants/en/enigma-sim.htm L'applicazione permette di simulare diverse versioni della macchina e di salvare la configurazione usata per usi successivi.

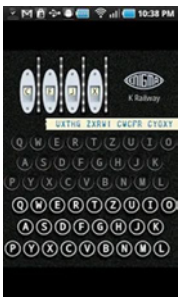
Per ciascuna di quelle coppie possiamo formare un'altra coppia scegliendo tra le 24 lettere rimanenti, le nuove possibili coppie sono le combinazioni di 24 lettere a due a due:

$$C_{24,2} = \frac{24 \cdot 23}{2!} = 276$$

e così via per le sei coppie (i sei collegamenti sul pannello a prese multiple).

In realtà abbiamo *troppe* coppie! Ogni combinazione di sei collegamenti fissati si presenta più volte, per essere precisi ogni sestina di collegamenti si presenta in tutti i modi possibili (avremo una sestina del tipo AB CD EG HP MN YZ ma anche CD AB EG HP MN YZ, CD EG AB HP MN YZ, ... dobbiamo quindi dividere il numero di coppie trovato per tutte le possibili permutazioni di una determinata sestina di collegamenti. In conclusione abbiamo che le possibili combinazioni del pannello a prese multiple si possono calcolare con la formula:

$$\frac{C_{26,2} \cdot C_{24,2} \cdot C_{22,2} \cdot C_{20,2} \cdot C_{18,2} \cdot C_{16,2}}{6!}$$



Un buon simulatore Enigma per Android si può trovare su Google Play Store: *Enigma Simulator* di Franklin Heath Ltd. Come il precedente, anche questo è gratuito.

che in numeri è

$$\frac{325 \cdot 276 \cdot 231 \cdot 190 \cdot 153 \cdot 120}{720} = 100.391.791.500$$

Un numero impressionante, oltre cento miliardi di possibili combinazioni. Il pannello a prese multiple era di gran lunga il componente capace di complicare la decifrazione.

A questo punto possiamo calcolare il numero di configurazioni totale, basta moltiplicare tra loro le possibilità date dalla posizione dei rotori, dalla disposiizione dei rotori in un certo ordine e dallo scambio delle lettere sul pannello:

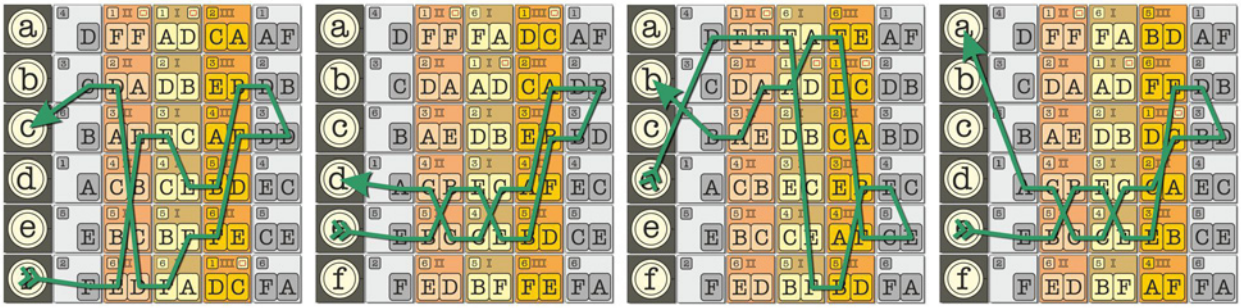
$$15.576 \cdot 6 \cdot 100.391.791.500 = 9.382.215.266.424.000$$

Straordinario: oltre *nove milioni di miliardi* di possibili configurazioni!

4.2. Proviamo a usare il simulatore mini

Cifra la parola *fede*.

La figura che segue mostra il simulatore mini nel corso delle operazioni di cifratura della parola *fede*, in ogni immagine la linea verde indica il percorso fatto per cifrare il singolo carattere. Il testo cifrato è *CDBA*. Notare la posizione del rotore più a destra in ciascuna immagine: dopo aver cifrato un carattere infatti l'ultimo scambiatore viene fatto ruotare di una posizione (verso il basso). In particolare, dopo la cifratura della lettera *f* (la prima immagine a sinistra) ruota anche lo scambiatore centrale (notare che nella seconda immagine l'ultimo rotore ha il gancio di rotazione ⊡ nella posizione più in alto).

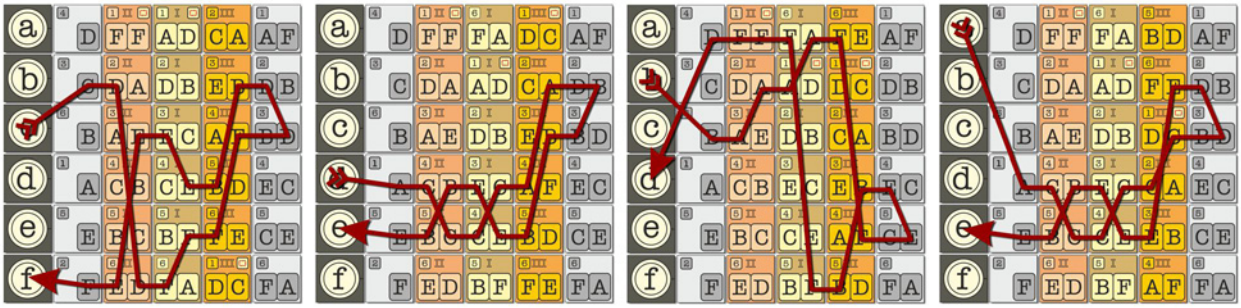


Osserva la parola cifrata, da quali simboli sono state sostituite le due *e* presenti nel testo in chiaro? È un vantaggio questa caratteristica? Perchè?

La prima e è sostituita da *D* mentre la seconda da *A*: la rotazione degli scambiatori fa in modo che lettere uguali siano cifrate da simboli differenti. Questo *protegge* il testo cifrato con Enigma dall'analisi delle frequenze. Si tratta di una conseguenza, voluta, della rotazione degli scambiatori, un po' come nel metodo di Vigenére che usa alfabeti cifranti diversi per ciascuna lettere del testo in chiaro, ma in maniera automatizzata (cfr. 13 - Crittografia 1).

Ora prova a decifrare la parola che hai ottenuto. Ricorda che la macchina deve essere nella stessa configurazione usata per la cifratura.

La figura qui di seguito mostra i vari passaggi dell'operazione di decifratura. Una volta configurata la macchina (il simulatore mini) allo stesso modo, si segue il percorso che va da ogni simbolo fino alla lettera corrispondente. Si nota subito la conformità dei percorsi tra la figura qui sotto e quella nella pagina precedente, solo con il verso è differente meglio, è l'opposto: questa è una preziosa caratteristica, in questo modo le operazioni di cifratura e decifratura si eseguono esattamente allo stesso modo. Il messaggio in chiaro risulta, ovviamente, *fede*!



4.3. Forzare Enigma

La decifrazione di un messaggio nascosto criptato con una macchina Enigma fu, durante la guerra, un compito davvero difficile anzi, impossibile senza il supporto del calcolo automatico. Qui vogliamo proporre un esempio che, per quanto semplificato e applicato a un mini simulatore come in nostro, sarà comunque veramente complesso!

Con il simulatore in versione mini è stata cifrata una parola ottenendo *FDFFB*, sappiamo per certo che la parola in chiaro inizia con le lettere *ba*. Prova a ricostruire la configurazione iniziale del mini simulatore usata per cifrare la frase.

Prima di buttarsi a capofitto nelle prove, conviene fare un po' di conti per cercare di capire quante sono le possibili configurazioni del simulatore mini, un po' come abbiamo fatto per la macchina Enigma di prima generazione **(cfr. 4.1 Qualche conticino a pagina 20)**.

Procediamo allo stesso modo tenendo conto delle differenze. Ogni rotore del simulatore mini ha

6 posizioni possibili (corrispondenti ognuna a una lettera del mini alfabeto *a, b, c, d, e, f*) per cui le combinazioni sono $6 \times 6 \times 6 = 216$.

Tutte i possibili ordinamenti del tre rotori sono $3! = 6$ e moltiplicando le possibili posizioni dei rotori per tutti i possibili ordinamenti si ha $216 \times 6 = 1296$.

Per il pannello a prese multiple procediamo come per la macchina Enigma **(cfr. pagina 21)** e calcoliamo il numero di possibili coppie che possiamo formare con sei lettere: $C_{6,2} = 15$, con le restanti quattro lettere possiamo formare $C_{4,2} = 6$ coppie e infine con le ultime due lettere abbiamo una sola coppia, infatti $C_{2,2} = 1$. Se fossimo obbligati, un po' come gli operatori Enigma, a usare tutti i tre collegamenti, in totale avremmo (con n_3 indichiamo il numero di configurazioni del pannello a prese multiple ottenute con tre collegamenti):

$$n_3 = \frac{C_{6,2} \cdot C_{4,2} \cdot C_{2,2}}{3!} = \frac{15 \cdot 6 \cdot 1}{6} = 15$$

possibili configurazioni. Ma dobbiamo tener conto che possiamo anche usare due soli collegamenti per cui si avranno altre configurazioni possibili che possiamo calcolare in modo simile ma tenendo conto solo delle coppie formate a partire da sei lettere e dalle coppie composte a partire da due lettere (con n_2 indichiamo il numero di configurazioni con due scambi):

$$n_2 = \frac{C_{6,2} \cdot C_{4,2}}{2!} = \frac{15 \cdot 6}{2} = 45$$

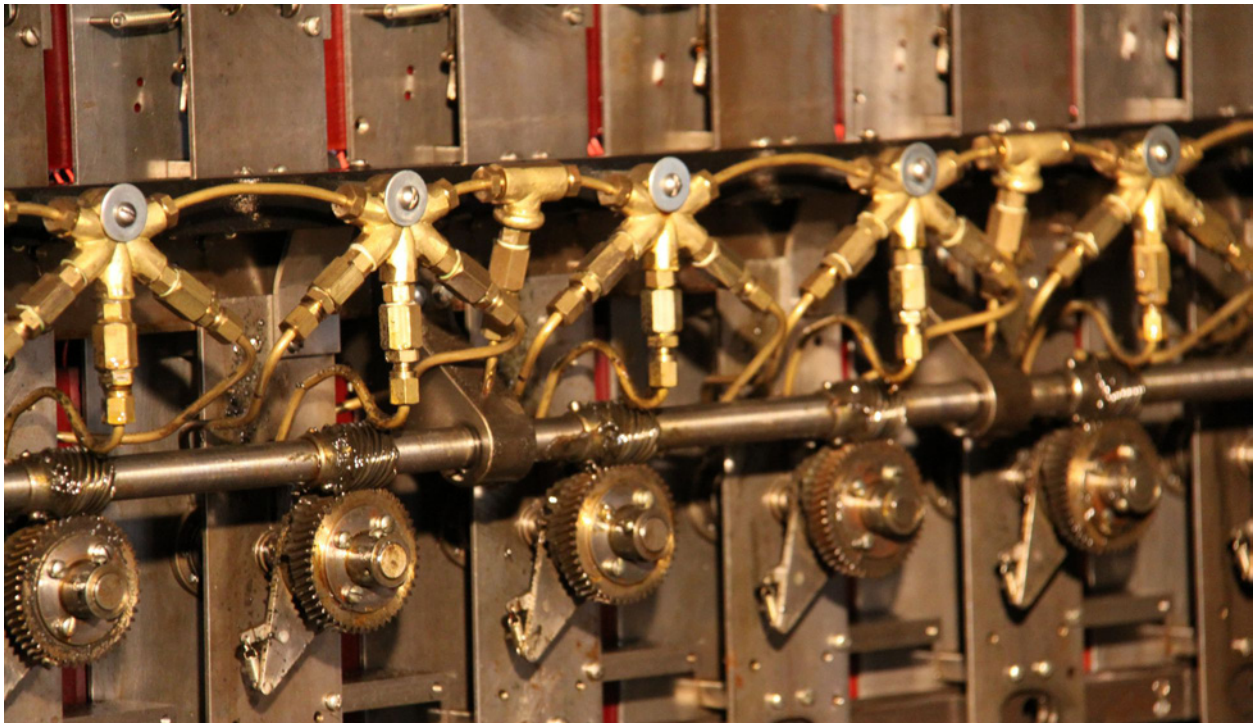
Poi delle configurazioni costruite con un solo collegamento (quindi *accoppiando* due sole lettere):

$$n_1 = \frac{C_{6,2}}{1!} = 15$$

E infine dalla configurazione, unica, realizzata senza nessuno scambio.

In totale abbiamo $n_3 + n_2 + n_1 + 1 = 76$ configurazioni possibili del pannello a prese multiple.

In conclusione le possibili configurazioni sono $216 \times 6 \times 76 = 98.496$. Un numero largamente inferiore a quello della macchina originale ma comunque grande: impossibile riuscire a recuperare la configurazione con cui è stata cifrata la parola che ci hanno comunicato!



Ancora un particolare di Colossus, la macchina automatica costruita a Bletchley Park.

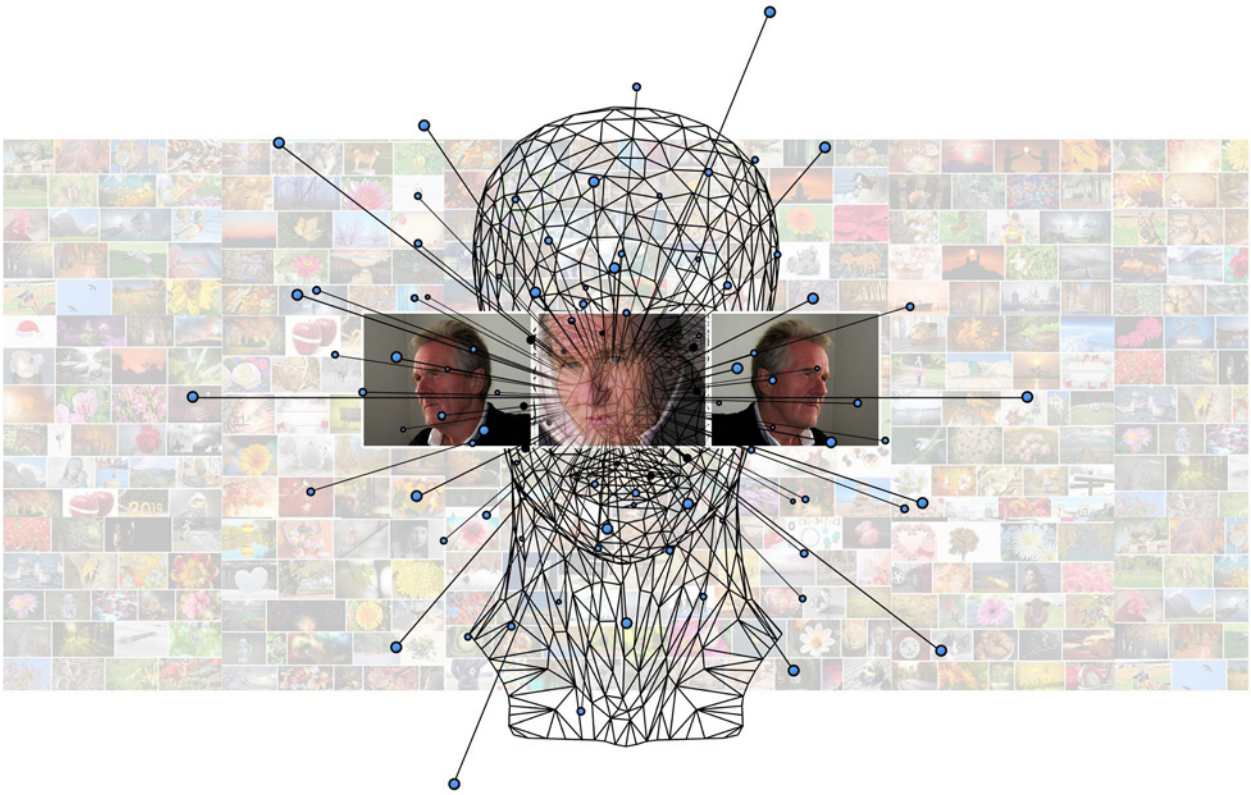
Questo quesito (che, ripetiamo, non si può risolvere *a mano*) vuole dare un'idea del lavoro che i criptoanalisti britannici, Alan Mathison Turing in testa, dovettero affrontare per decifrare le comunicazione tedesche nel corso della guerra. Il gruppo di *Betchley Park* ideò e costruì una macchina, *Colossus*, molto simile nello schema a quelli che sarebbero diventati vent'anni dopo i moderni calcolatori, capace di provare migliaia, decine di migliaia, di configurazioni in un tempo ragionevole contribuendo alla decifrazione delle comunicazioni nemiche.

Per tornare al quesito, la decriptazione dei messaggi avvenne grazie alla presenza di brani o parole ripetuti ogni giorno (come le previsioni del tempo, che iniziavano allo stesso modo ogni volta) che gli analisti chiamarono *crib*. La presenza dei *crib* consentiva di programmare Colossus perchè ricercasse la configurazione usata (un po' come suggerivamo nel quesito) e conosciuta la configurazione il testo era facilmente decifrabile usando una copia di Enigma!

Se hai ricostruito la configurazione del mini simulatore, decifra la parola.

La parola è stata cifrata configurando la macchina in questo modo: *B-F I-5 II-1 III-5*. La figura che segue mostra le operazioni di decifratura, che poi sono le stesse che sono state eseguite per cifrare la frase. Il teso in chiaro è *bacca*.

Notare come, nel passaggio dalla seconda immagine alla terza la rotazione dello scambiatore più a destra abbia innescato la rotazione di quello centrale e successivamente anche di quello più a sinistra, grazie alla presenza del gancio di rotazione nella posizione più in alto del rotore III e poi del rotore II.



5. Chiave pubblica: l'algoritmo RSA

5.1. Diamoci da fare

Cifratura

Ricordiamo che l'algoritmo RSA opera su numeri per cui dobbiamo innanzitutto trasformare la frase da cifrare in una serie di numeri.

Individua un metodo, una codifica, che associ a ogni carattere dell'alfabeto anglosassone un numero intero positivo. Scegli un meccanismo facile e fai in modo che gli interi non siano troppo grandi.

La cosa più semplice è associare a ogni lettera la sua posizione nell'alfabeto, per cui alla lettera *a* corrisponderà il numero uno, alla sarà associato *b* il numero 2 e così via fino alla *zeta* che avrà codice 26.

Trasforma la frase da cifrare, *Quando le cose si surriscaldano, le nuvole si dissipano*, in una serie di numeri interi usando la codifica che hai scelto.

Questo passaggio non è difficile con il meccanismo che abbiamo scelto. Per comodità abbiamo rappresentato il testo e la relativa codifica in una tabella: nella prima e quarta riga il testo, nella seconda e quinta la codifica in chiaro e, infine, nella terza e sesta riga la frase cifrata (i cui valori sono evidenziati in colore rosso) che discuteremo nel seguito.

q	u	a	n	d	o	l	e	c	o	s	e	s	i	s	u	r	r	i	s	c	a	l
17	21	1	14	4	15	12	5	3	15	19	5	19	12	19	21	18	18	12	19	3	1	12
8	21	1	9	49	5	23	25	42	5	24	25	24	4	24	21	17	17	4	24	42	1	23
d	a	n	o	l	e	n	u	v	o	l	e	s	i	d	i	s	s	i	p	a	n	o
4	1	14	15	12	5	14	21	22	15	12	5	19	12	4	9	19	19	9	16	1	14	15
49	1	9	5	23	25	9	21	33	5	23	25	24	4	49	4	24	24	4	36	1	9	5

Scegli una chiave e cifra la frase usando l'algoritmo RSA.

Per cifrare il nostro messaggio abbiamo scelto $p = 11$ e $q = 5$, da cui $N = 55$, successivamente, visto che $(p-1)(q-1) = 40$, abbiamo posto $e = 7$.

Con questa chiave abbiamo, per esempio:

- per la lettera *q*: $M = 17$ e quindi $C = 17^7 \bmod 55 = 8$;
- per la lettera *u*: $M = 21$ e quindi $C = 21^7 \bmod 55 = 21$;
- o, ancora, per la lettera *a*: $M = 1$ da cui $C = 1^7 \bmod 55 = 1$, il che ci fa pensare che non sia una buona idea usare una codifica che associ a uno dei caratteri il numero uno, visto che in questo caso il valore cifrato sarà comunque uguale a uno (l'unità elevata a qualsiasi potenza dà sempre uno).

E così via per tutti gli altri caratteri. I valori cifrati sono evidenziati nella tabella in colore rosso.

Decifratura

Ora scegliete una chiave e cifrate una (breve) frase di vostra scelta.

Come esempio prendiamo la stessa frase che abbiamo cifrato poco fa. Supponiamo di conoscere solo la chiave pubblica $N = 55$, $e = 7$.

Sul blog Research in Action è possibile utilizzare la libreria sviluppata con Blockly nel corso delle attività del progetto: http://researchinaction.it/myblockly/criptography.html
In particolare le funzioni *RSACifra* e *RSADecifra* sono realizzate implementando i due algoritmi descritti in queste pagine.
Blockly è un generatore di codice open source sostenuto da Google: https://developers.google.com/blockly/.

Decifrate il messaggio!

Per prima cosa scomponiamo N in 5×11.

Questo è il passaggio cruciale della decodifica del testo, facile nei nostri esempi ma tutt'altro che semplice in realtà. Tanto per fare un esempio, conoscendo la prima parte di una ipotetica chiave $N = 2.109.539$, prova a scomporla nel prodotto di due primi: per niente agevole anche se i due primi non sono eccessivamente grandi infatti $N = 1049 \times 2011$. Ora immagina una chiave composta da due primi di qualche centinaio di cifre ... la sicurezza dell'algoritmo RSA si basa proprio sulla difficoltà di scomporre un numero intero nei suoi fattori primi.

Torniamo al nostro esempio. Calcoliamo il prodotto $\varphi(N) = (p-1)(q-1) = 40$ e scegliamo un numero d per cui $ed - 1 = 7d - 1$ sia multiplo di $\varphi(N) = 40$. Dopo qualche tentativo arriviamo a $d = 23$ (infatti $7d - 1 = 161 - 1 = 160$ che è multiplo di 40, è il più piccolo intero che ha questa proprietà).

Adesso possiamo decifrare il messaggio:

» per $C = 8$ (il primo valore della sequenza cifrata) si ha $M = 8^{23} \bmod 55 = 17$, la diciassettesima lettera dell'alfabeto è la q, corretto;
» per $C = 21$ abbiamo $M = 21^{23} \bmod 55 = 21$, il carattere corrispondente è u, ancora corretto;
» infine, per chiudere con l'esempio, se $C = 1$ otteniamo facilmente $M = 1^{23} \bmod 55 = 1$ che corrisponde alla lettera a.

Se hai svolto la decifrazione ti sarai accorto che, pur avendo scelto primi *piccoli*, i calcoli intermedi sono al limite delle capacità di una normale calcolatrice. È però che in precedenza abbiamo suggerito un *piccolo trucco* per ridurre la complessità dei calcoli. Per esempio, per $C = 21$ possiamo immaginare di scrivere 21^{23} come il prodotto $21^2 \times 21^2 \times \ldots 21^2 \times 21^1$ quindi:

$$M = 21^{23} \bmod 55 = 21^2 \bmod 55 \cdot 21^2 \bmod 55 \cdot \ldots 21^2 \bmod 55 \cdot 21^1 \bmod 55$$

dove abbiamo undici fattori del tipo $21^2 \bmod 55$.

Ma se consideriamo che $21^2 \bmod 55 = 441 \bmod 55 = 1$ mentre $21^1 \bmod 55 = 21 \bmod 55 = 21$, la formula qui sopra diventa $M = 1 \times 1 \times \ldots \times 21 = 21$. E senza nemmeno usare la calcolatrice!

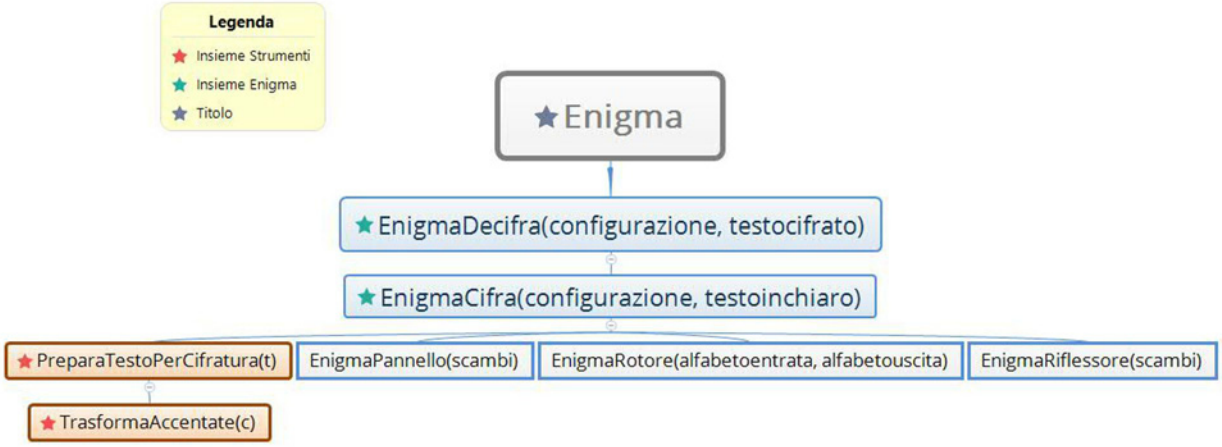
6. Struttura della libreria

I paragrafi qui di seguito riportano le dipendenze tra le varie funzioni della libreria dedicate all'approssimazione dei numeri irrazionali e trascendenti: le funzioni più in alto nella figura usano le funzioni più in basso a cui sono collegate. Per esempio: *CodiceCesareCifra* usa *PreparaTestoPer-Cifratura* che a sua volta usa *TrasformaAccentate*.

La legenda indica in quale insieme di funzioni possono essere trovate le procedure corrispondenti (le piccole stelle colorate presenti davanti al nome di ogni funzione son riportate nella legenda, in cui è indicato l'insieme di funzioni opportuno).

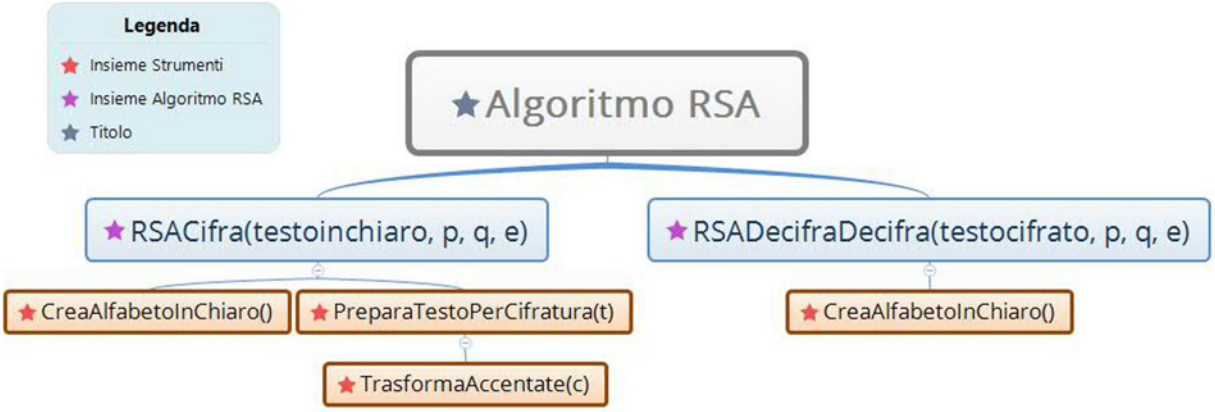
6.1. Enigma

Funzioni per cifrare e decifrare simulando una macchina Enigma **(cfr. Enigma a pagina 6)**.



6.2. Algortimo RSA

Funzioni per cifrare e decifrare mediante l'allgortimo RSA **(cfr. Chiave pubblica: l'algortimo RSA a pagina 15)**.



LICEO SCIENTIFICO GRASSI LATINA

CNR IAC
Istituto per le Applicazioni del Calcolo

CNR IFN
Istituto di Fotonica e Nanotecnologie

INM

ISMAR
Istituto di Scienze Marine

LSS G.B. Grassi

liceo scientifico statale G.B. Grassi di LAtina

www.liceograssilatina.org

CNR - IAC

Istituto per le Applicazioni del Calcolo Mauro Picone

www.iac.cnr.org

CNR - IFN Roma

Istituto di Fotonica e Nanotecnologie

www.roma.ifn.cnr.org

CNR - INM

Istituto di iNgegneria del Mare

www.insean.cnr.org

CNR - ISMAR

Istituto di Scienze MARine

www.ismar.cnr.org