Studente: Jacopo Tagliaferri

Matricola: 145954

Progetto di: Comunicazione della Scienza a.a. 2015-2016

Professore: Marco Andreatta

Titolo: Calendario Crittografia

Scelte divulgative:

Questo progetto prevede la creazione di un calendario che illustri l'evoluzione delle tecniche crittografiche nella storia.

Una delle prime iterazioni del progetto prevedeva la creazione di un poster che rappresentasse una linea temporale con le varie tappe dell'evoluzione della crittografia.

Ho deciso però di utilizzare il calendario perché, oltre altre a richiamare il concetto dello scorrere del tempo, serve a dare un'utilità secondaria al prodotto finale, che non sarà più un semplice poster contenente accenni a scoperte scientifiche ed al funzionamento delle stesse, ma avrà anche un'utilità pratica che ne giustificherà l'utilizzo per un numero maggiore di utenti.

Il calendario può anche essere riprogettato per sfruttarlo, una volta esaurita la funzione annuale. stampando fronte e retro le informazioni ed il calendario vero e proprio, in modo da poterle staccare e conservare come poster singoli, senza essere legati alla validità delle date.

Nel calendario ogni mese sarà dedicato ad una tecnologia di cifratura posteriore a quella presentata il mese precedente, partendo dunque da quelle più semplici ed antiche per arrivare alle più moderne tecniche crittografiche.

I contenuti sono così divisi: una contestualizzazione del periodo storico, la descrizione del funzionamento del cifrario, un esempio di codice cifrato ed una sezione per le curiosità.

Questo porta la parte di informazioni ad essere leggermente affollata di testo. Ciò potrebbe essere risolto fornendo unicamente la descrizione del funzionamento e inserendo, per integrarla, le formule matematiche che ne spiegano il funzionamento o la complessità, ma questo devierebbe dall'obbiettivo di inclusione in quanto diventerebbe attraente solo per un pubblico maggiormente specializzato.

Una sezione che era in progetto e non è poi stata aggiunta al prototipo è quella comprendente esempi ed esercizi da risolvere, ma è stata scartata in quanto questi diventavano improponibili al raggiungimento delle sezioni riguardanti le tecnologie moderne.

In ogni pagina è presente oltre ad un'immagine dell'apparecchio cifrante o una rappresentazione del funzionamento anche un codice QR che rimanda ad una pagina web sull'argomento. Per semplicità nel prototipo i codici QR contengono link a pagine di Wikipedia.

Questi codici sono stati aggiunti per permettere di approfondire gli argomenti senza dover essere limitati allo spazio fisico fornito dalla carta, oltre ad attirare l'attenzione inserendo un elemento innovativo nella composizione.

In un eventuale progetto su larga scala i link dovrebbero portare ad un sito personalizzato, organizzato appositamente per ampliare la presentazione.

I 12 mesi potrebbero essere così suddivisi:

Gennaio – Atbash

Febbraio – Scitale

Marzo – Cifrario di Cesare (presente nel prototipo)

Aprile – Disco Cifrante (presente nel prototipo)

Maggio - Cifrario di Vigenère

Giugno – Rullo di Jefferson (presente nel prototipo)

Luglio - Cifrario Playfair

Agosto – Cifrario bifido di Delastelle

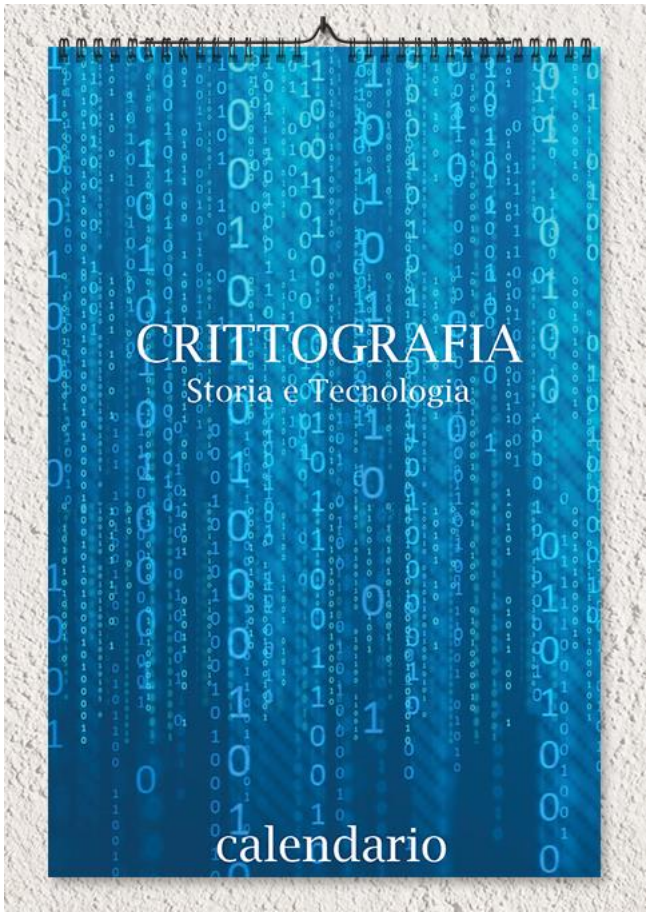
Settembre – Cifrario di Vernam

Ottobre – Enigma (presente nel prototipo)

Novembre – DES

Dicembre – Crittografia Quantistica

Di seguito il prototipo del calendario:



CIFRARIO DI CESARE

Il cifrario di Cesare prende il suo nome da Giulio Cesare, che nel I° secolo a.C. ne fu il primo utilizzatore documentato, grazie allo storico Svetonio sappiamo infatti che sostituiva la A con la D e le altre lettere in successione, utilizzando di fatto una chiave di 3 per questo cifrario a sostituzione monoalfabetica. Cesare sfruttava questo sistema per la corrispondenza militare ed era considerato discretamente sicuro in quanto i suoi avversari erano spesso illetterati o avrebbero considerato il messaggio come scritto in una lingua sconosciuta.

Il cifrario di Cesare è un cifrario a sostituzione o a scorrimento. Questo tipo di cifrari opera sostituendo lettera per lettera tutto il testo. Dunque utilizzando lo spostamento di 3 posizione come abitualmente nelle missive di Cesare la lettera "A" verrà sostituita con la lettera che nell'alfabeto in chiaro si trova 3 posizioni dopo, dunque "D", la "B" verrà sostituita sempre dalla terza successiva quindi "E" e così via. Per decifrare basta compiere la stessa operazione al contrario. Per aumentare la sicurezza nel messaggio cifrato venivano poi tolti gli spazi.

Curiosità

Cifrare più volte il testo non migliora la sicurezza poiché il testo cifrato non è altro che il testo in chiaro cifrato con una chiave che è la somma delle chiavi usate per le cifrature consecutive.

March

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

DISCO CIFRANTE

Nel suo trattato "De Cifris" (1466) Leon Battista Alberti esamina i difetti dei cifrari esistenti all'epoca ed espone il suo metodo di sostituzione polialfabetica con alfabeti mischiati, cambiati in modo segreto. Per la comunicazione i corrispondenti dovranno usare apparecchi con gli stessi alfabeti. Questi apparecchi erano composti da 2 dischi concentrici, il maggiore contente l'alfabeto latino ordinato ed in maiuscolo seguito da i numeri dall'1 al 4, il secondo ha impresso l'alfabeto in lettere minuscole ed ordine sparso.

Alberti propone diversi metodi di cifratura da utilizzare con il disco per aumentarne la sicurezza.
Il primo prevede che mittente e destinatario concordino su una lettera del disco minore come chiave segeta. Si porta quindi questa lettera sotto una delle maiuscole che viene quindi scritta come prima lettera del cifrario, si cifrano poi alcune lettere del messaggio e si ruota nuovamente il disco in modo casuale andando a segnare nuovamente la lettera maiuscola che si troverà sopra la chiave e si ripetono i passaggi precedenti.

Curiosità

Questo cifrario era molto più sicuro di quelli che uscirono nei quattro secoli successivi, ma data la decisione dell'Alberti di tenere il trattato segreto, questo venne pubblicato solo postumo e passò inosservato.

April

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

RULLO DI JEFFERSON

Il cilindro di Jefferson o cifrario a ruote fu inventato tra il 1790 ed il 1793, periodo in cui Thomas Jefferson era segretario di stato per cifrare le comunicazioni diplomatiche. Il cilindro è un cifrario polialfabetico formato da una serie di dischi rotanti ciascuno con le lettere scritte in ordine sparso sul bordo.

Per codificare i messaggi è necessario dividere il messaggio in blocchi di lettere pari al numero di rulli, riempiendo di nulle i posti avanzati alla fine. Per codificare si cercherà sulla prima ruota la prima lettera del blocco in chiaro, quindi si cerca la seconda sulla seconda ruota posizionandola vicino alla prima e così via finché il testo in chiaro non risulterà leggibile sulla riga scelta. Come cifrario si sceglierà dunque un'altra riga spostata rispetto al chiaro e la si trasmetterà. Per decifrare il messaggio basterà avere un dispositivo uguale e allinearne le ruote per ottenere il messaggio cifrato. A questo punto una delle 25 righe conterrà un messaggio leggibile, che sarà il testo inviato in chiaro.

Curiosità

Una volta eletto presidente Jefferson abbandonò l'uso di questo cifrario a favore di uno a trasposizione, considerato meno sicuro. Il cilindro verrà riscoperto indipendentemente un secolo dopo dal cripto-analista dell'esercito francese Etienne Bazeries ed in seguito adottato dall'esercito degli stati uniti tra il 1922 ed il 1945.

June

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

ENIGMA

Enigma è una macchina cifrante a rotori inventata nel 1918 dal tedesco Arthur Schrebius sul modello del cilindro di Jefferson reinventato da Bazeries. L'esercito tedesco la utilizzò dal 1925 fino alla seconda guerra mondiale per le comunicazioni segrete.

Su ogni macchina enigma erano montati 3 rotori (aumentati nelle versioni successive) settabili dall'utente, ognuno con 26 lettere. Questi rotori mescolavano le coppie di lettere in base alla loro posizione.
L'innovazione della macchina enigma è che ad ogni lettera i rotori girano, quindi le coppie di lettere cambiano ad ogni nuova lettera inserita. In questo modo pur intercettando il codice non è possibile interpretare il messaggio senza conoscere la composizione iniziale (26^3 possibili soluzioni = 17576). Questo combinato con la possibilità di cambiare la posizione dei rotori ed il settaggio delle coppie di lettere porta ad avere 10^{16} possibili combinazioni.

Curiosità

Enigma non fu decifrata perché inefficiente, ma perché a causa della scarsa qualità radio che comportava la ripetizioni di determinate lettere chiave e all'abitudine dei soldati tedeschi di girare di poco i rotori. Questo insieme al fatto che una lettera non poteva ritornare uguale dopo essere stata crittata permisero al team di cui faceva parte Alan Touring di migliorare la macchina Bomba inizialmente sviluppata dai servizi segreti polacchi e la conseguente decrittazione dei messaggi tedeschi.

October

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			