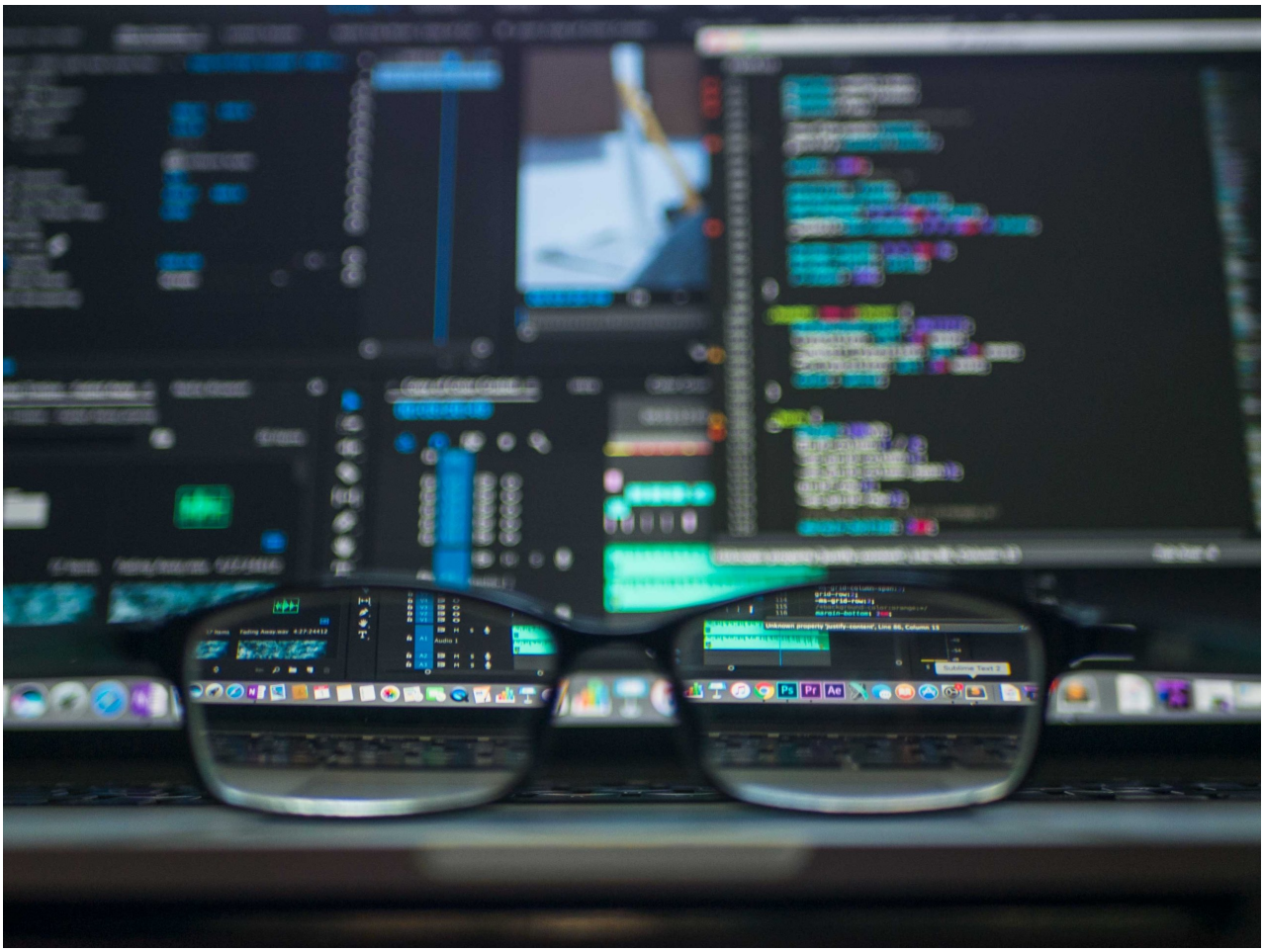
Cifratura dei dati. Storia, tecniche e interazione con la legislazione vigente – Parte I

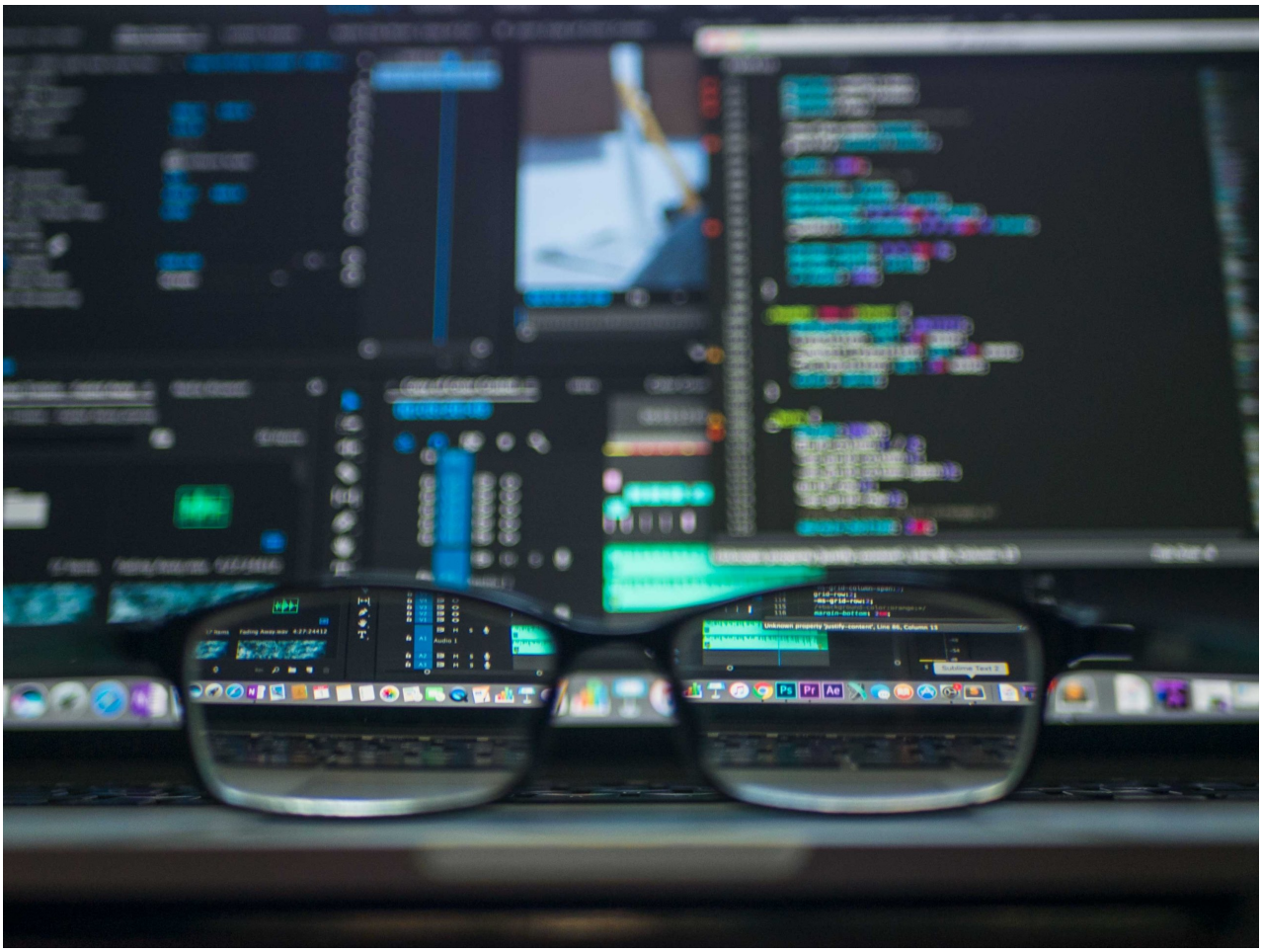
whynery.com/cifratura-dei-dati-storia-tecniche-e-interazione-con-la-legislazione-vigente-parte-i

24 febbraio 2021



Dietro le Quinte

David Scaffaro – 24 Febbraio 2021



Oggi proteggere i dati è vitale per ogni azienda.

Questo vale non solo nei settori storicamente vicini a queste esigenze, come quello militare, sanitario o finanziario, ma anche per i settori che hanno sviluppato recentemente un'alta sensibilità, come quello della ristorazione, dell'accoglienza turistica, e dovunque vi sia interazione con il pubblico.

David Scaffaro ci porterà a conoscere aspetti teorici e pratici di ciò, in un viaggio di tre puntate sul tema.

Cifratura, cos'è

La cifratura è l'insieme di tecniche atte a rendere crittografico un dato, un documento o un messaggio.

Rendere crittografico uno di questi elementi, significa renderlo illegibile, da come si può desumere dall'etimologia greca della parola stessa: kryptós (nascosto) e graphía (scrittura).

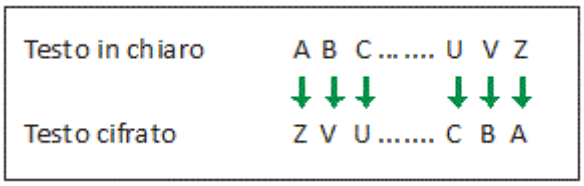
Cifratura, cenni storici

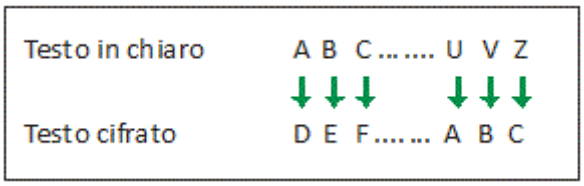
L'esigenza di crittografare messaggi ha radici molto antiche, ed era una pratica comune nel mondo antico e in voga presso gli antichi egizi, indiani, greci e romani.

Tra gli esempi classici dell'antichità, alcuni sono giunti fino a noi, come il cifrario di Atbash e il cifrario di Cesare.

Il cifrario di Atbash viene citato nella Bibbia e, sostanzialmente inverte le lettere dell'alfabeto, sostituendo la prima lettera con l'ultima, la seconda con la penultima e così seguendo.

Il codice di Cesare è un cifrario simmetrico a scorrimento, ovvero le lettere che compongono il messaggio cifrato, si ottengono facendo scorrere di "n" posti l'ordine normale della composizione dell'alfabeto. Veniva usato da Giulio Cesare nelle sue campagne belliche ed usava, normalmente, come chiave n=3. Oggi, per pura azione di offuscamento temporaneo, in enigmistica o in altri settori viene usata una variante chiamata ROT13 dove n=13.





Cifratura, tecniche nel corso degli anni

Partendo dai cifrari antichi, oggi facilmente decodificabili da chiunque, negli anni si sono affinate le tecniche di cifratura.

Tra queste va citato **il Cifrario di Vernam** e il suo precedessore, ovvero il **cifrario di Vigenère**.

Il cifrario di Vigenère ha goduto di ottima fama per alcuni secoli, finché non è stato decodificato (metodo Kasinki).

Il cifrario di Vigenère deriva dal cifrario di Cesare, la sostituzione della lettera da cifrare, però, viene spostata di **un numero variabile di posti** e non più per un numero fisso.

La chiave, essendo generalmente più corta del messaggio, **deve essere ripetuta più volte** fino ad assumere una **lunghezza uguale al messaggio da cifrare**.

La ripetizione della chiave è il **suo limite** maggiore, infatti, soprattutto se la lunghezza della chiave **è limitata**, nella crittanalisi si può determinare l'entità del numero di caratteri che la compongono e, come secondo step, utilizzare tecniche di **"analisi delle frequenze"**, basate sulla ricerca della frequenza di ripetizione di determinate lettere in un testo cifrato, in quanto, per ogni lingua, **sono note le percentuali di frequenza**

delle singole lettere. In italiano, per esempio, la lettera “a” e la lettera “e” sono quelle che hanno una frequenza maggiore (intorno al 12%), mentre la prima consonate con maggiore frequenza è la “n” (intorno al 7%).

Il cifrario di Vernam.

Note le debolezze del cifrario di Vigenère, la sua evoluzione la troviamo **nel cifrario di Vernam**.

Il cifrario di Vernam, basato su quello di Vigenère, ha introdotto una variante fondamentale, ovvero **la lunghezza della chiave è la stessa della lunghezza del testo**.

Altro elemento fondamentale è quello di **non riutilizzate mail la stessa chiave**, quindi deve essere un cifrario a chiave non riutilizzabile (One Time Pad, OTP).

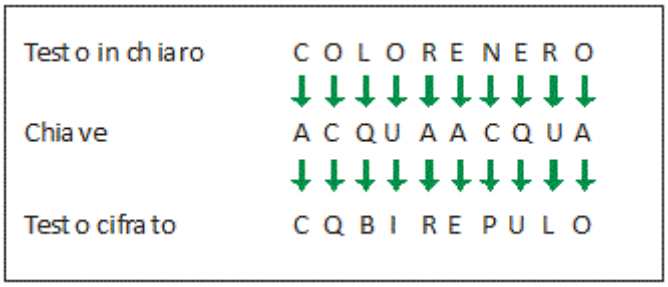
Il cifrario di Vernam è considerato un **cifrario perfetto, non decifrabile**, poichè sostanzialmente lo stesso messaggio può avere teoricamente un numero **infinito di soluzioni**.

L’aspetto maggiormente critico, si riscontra nel fatto che nei casi in cui il testo sia molto lungo, non è molto agevole trasmettere una chiave altrettanto lunga.

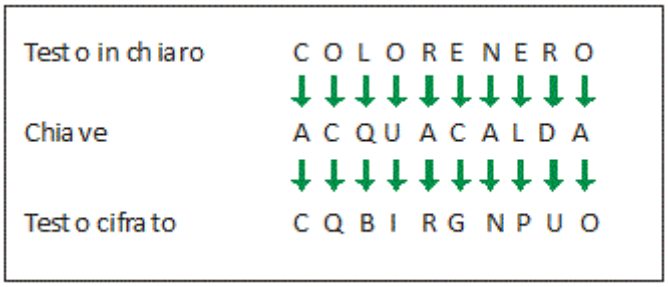
Altro aspetto da curare, come in altri casi dove la chiave ha la funzione sia di cifrare che di decifrare (sistemi simmetrici), è il **grado di sicurezza del canale di trasmissione** della chiave.

Esempio cifrario di Vigenère. Cifratura delle parole “COLORENERO” con chiave di cifratura “ACQUA” ; il testo cifrato è “CQBIREPULO”

Esempio cifrario di Vernam. Cifratura delle parole “COLORENERO” con chiave di cifratura “ACQUACALDA” ; il testo cifrato è “CQBIRGNPUO”



Mario Rossi o Carlo Verdi ? Perchè il cifrario di Vernam è inviolabile.



Valutiamo il seguente caso pratico utilizzando Vernam.

Consideriamo questo messaggio cifrato: **FKTEXAQLOB**

Quindi, visto che possiamo **usare qualsiasi chiave** che abbia lunghezza uguale alla lunghezza del testo da decrittare (Lkey = Ltext), di seguito vediamo

degli esempi concreti.

Se usassimo la chiave“**TKCWJJCTWT**“, avremo “**MARIOROSSI**“

Se usassimo la chiave “**DKCTJFMULT**“, avremo “**CARLOVERDI**“

Quindi, il messaggio decifrato è “**MARIOROSSI**” o “**CARLOVERDI**” **?**

Non lo sappiamo; può essere, l’uno, l’altro o altre “n” casistiche. (ES. “GATTOCIECO”, “CANETIMIDO”, “VINCEREORA” e così via)

Considerazioni parte I

In questa prima parte, abbiamo scritto sul **significato** della crittografia e accennato ad alcuni **sistemi di cifratura utlizzati in passato**. Abbiamo visto anche **l’evoluzione** e il miglioramento delle performance degli stessi, di come un semplice sistema, come il cifrario di Cesare, si sia modificato nel cifrario di Vigenère e successivamente nel cifrario di **Vernam, divenendo un sistema indecifrabile**. Negli anni, infine, si sono aggiunte alle esigenze di incolumità personale o belliche, anche esigenze di **sicurezza informatica** e di salvaguardia di informazioni riservate, sensibili o segrete. Con l’avvento dell’informatica moderna, infatti, si sono aperti molteplici nuovi aspetti da prendere in considerazione.

Nella prossima puntata

Nella seconda parte vedremo **l’evoluzione crittografica** fino ai giorni attuali, **alcuni attacchi crittografici, gli algoritmi più noti** e ci prepareremo ad introdurre le interazioni **con la legislazione vigente**, che analizzeremo, invece, nella terza parte.

Scopri il nostro online store

Accedi allo store Whynery, registrati per acquistare e profila la tua identità sensoriale.

Vai allo Store

Lascia un commento

Il tuo indirizzo email non sarà pubblicato. I campi obbligatori sono contrassegnati *