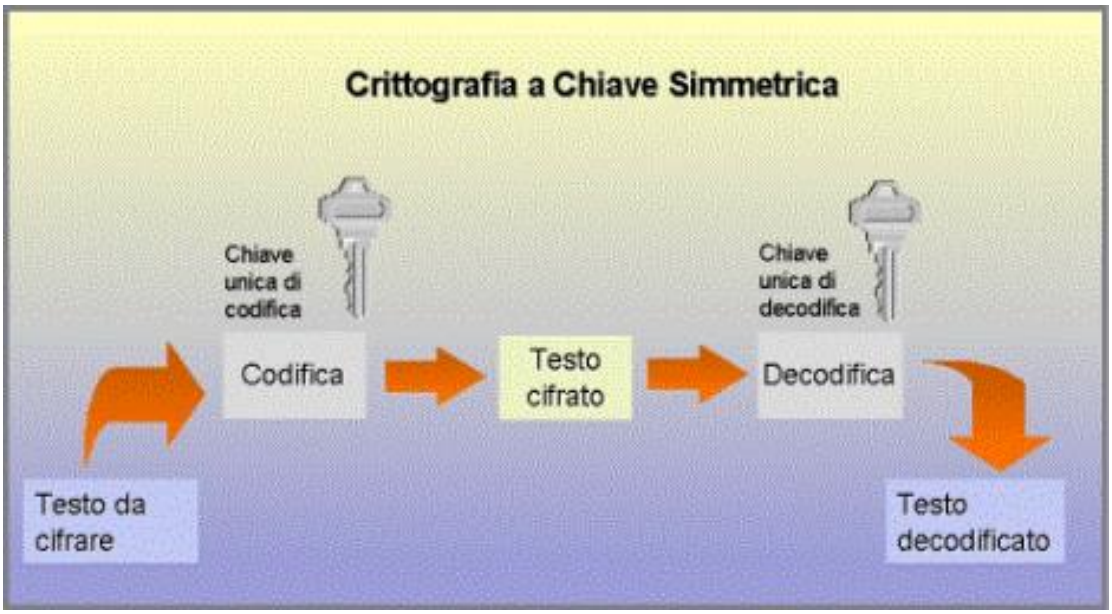
Storia della crittografia

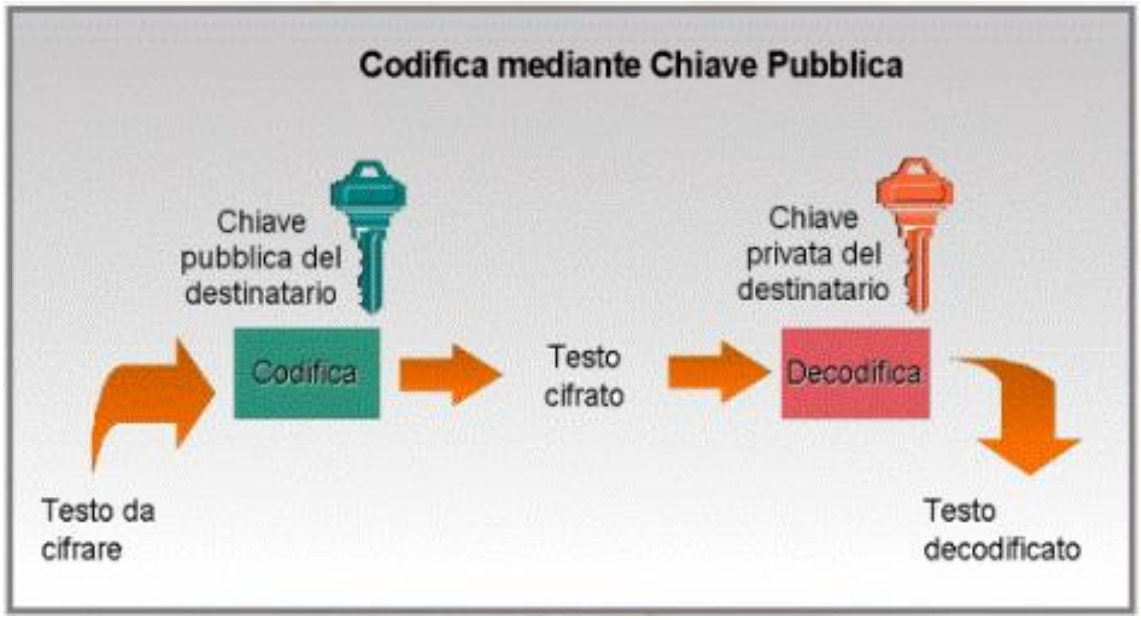
Cifrario di Cesare
(inizio discorso progetto)

La necessità di nascondere messaggi strategici da occhi nemici è antica quanto l'uomo: ci sono tracce di cifrari antichi quanto gli Ebrei con il loro codice di atbash; gli Spartani avevano un loro particolare sistema di comunicazione dei messaggi segreti, la scitala; a Gaio Giulio Cesare si attribuisce l'uso del cosiddetto cifrario di Cesare, un sistema crittografico oggi ritenuto elementare, ma emblema della nascita di un concetto totalmente nuovo e ottimo per comprendere le idee basilari della crittografia e i primi attacchi della sua "avversaria": la crittoanalisi.
La **crittografia** (dall'unione di due parole greche: κρυπτός (kryptós) che significa "nascosto", e γραφία (graphía) che significa "scrittura") è la branca della crittologia che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile/intelligibile a persone non autorizzate a leggerlo.
Un tale messaggio si chiama comunemente crittogramma e i metodi usati sono detti tecniche di cifratura.
La **crittografia** ha origini remote ed ha inizio con la *crittografia classica*. La crittografia classica prevedeva metodi di cifratura poco complessi, generalmente contemplavano l'utilizzo di carta e penna o, al massimo, semplici supporti meccanici. Uno dei primi esempi di cifratura lo troviamo ai tempi dell'antico impero Romano, il cifrario di Cesare, che prende il nome dal suo inventore, veniva utilizzato per proteggere i propri messaggi segreti. Grazie allo storico Svetonio sappiamo che Cesare utilizzava in genere una chiave di 3 per il cifrario, come nel caso della corrispondenza militare inviata alle sue truppe. Al tempo era sicuro perché gli avversari spesso non erano neanche in grado di leggere un testo in chiaro, men che mai uno cifrato.
Anche se la crittografia ha una lunga e complessa storia, fino al XIX secolo essa non sviluppò niente più che approcci *ad hoc* sia alla cifratura sia alla crittanalisi, come i lavori sull'analisi dei cifrari polialfabetici di Charles Babbage, rielaborati e pubblicati dal prussiano Friedrich Kasiski.
L'invenzione delle trasmissioni radio ha permesso alla crittografia di assumere sin dal XIX secolo un ruolo fondamentale per trasmettere messaggi di tipo militare. L'interesse a trasmettere un messaggio occulto agli occhi di tutti i lettori, eccetto il destinatario, risale a più di 4500 anni. Ovviamente le regole di cifratura devono essere note sia al mittente che al destinatario.

Esistono due tipi di crittografia:

1. 

Con crittografia simmetrica, o crittografia a chiave privata, si intende una tecnica di cifratura. Rappresenta un metodo semplice per cifrare testo in chiaro dove la chiave di crittazione è la stessa chiave di decrittazione, rendendo l'algoritmo molto performante e semplice da implementare. Tuttavia, presuppone che le due parti siano già in possesso delle chiavi, richiesta che non rende possibile uno scambio di chiavi con questo genere di algoritmi. Lo scambio avviene attraverso algoritmi a chiave asimmetrica o pubblica, generalmente più complessi sia da implementare che da eseguire ma permettono questo scambio in modo sicuro. Dopodiché la comunicazione verrà crittata usando solo algoritmi a chiave simmetrica per garantire una comunicazione sicura ma veloce.

2. 

La crittografia asimmetrica, conosciuta anche come crittografia a coppia di chiavi, crittografia a chiave pubblica/privata o anche solo crittografia a chiave pubblica, è un tipo di crittografia dove, come si evince dal nome, ad ogni attore coinvolto nella comunicazione è associata una coppia di chiavi:

- La chiave pubblica, che deve essere distribuita;
- La chiave privata, appunto personale e segreta;

evitando così qualunque problema connesso alla necessità di uno scambio in modo sicuro dell'unica chiave utile alla cifratura/decifratura presente invece nella crittografia simmetrica. Il meccanismo si basa sul fatto che, se con una delle due chiavi si cifra (o codifica) un messaggio, allora quest'ultimo sarà decifrato solo con l'altra.
Ci sono due funzioni che possono essere realizzate: usare la chiave pubblica per autenticare un messaggio inviato dal titolare con la chiave privata abbinata; o cifrare messaggi con la chiave pubblica per garantire che solo il titolare della chiave privata possa decifrarlo.
In un sistema di crittografia a chiave pubblica, chiunque può cifrare un messaggio usando la chiave pubblica del destinatario, ma tale messaggio può essere decifrato solo con la chiave privata del destinatario. Per fare ciò, deve essere computazionalmente facile per un utente generare una coppia di chiavi pubblica e privata da utilizzare per cifrare e decifrare. La forza di un sistema di crittografia a chiave pubblica si basa sulla difficoltà di determinare la chiave privata corrispondente alla chiave pubblica.
La sicurezza dipende quindi solo dal mantenere la chiave privata segreta, mentre la chiave pubblica può essere pubblicata senza compromettere la sicurezza.

I sistemi di crittografia a chiave pubblica spesso si basano su algoritmi di crittografia basati su problemi matematici che attualmente non ammettono alcuna soluzione particolarmente efficiente, quelli che riguardano la fattorizzazione di un numero intero, il logaritmo discreto e le relazioni delle curve ellittiche. Gli algoritmi a chiave pubblica, a differenza degli algoritmi a chiave simmetrica, non richiedono un canale sicuro per lo scambio iniziale di una (o più) chiavi segrete tra le parti.

A causa del peso computazionale della crittografia asimmetrica, essa di solito è usata solo per piccoli blocchi di dati, in genere il trasferimento di una chiave di cifratura simmetrica (per esempio una chiave di sessione). Questa chiave simmetrica è utilizzata per cifrare messaggi lunghi. La cifratura/decifratura simmetrica è basata su algoritmi semplici ed è molto più veloce.

ENIGMA
(storia)

Tra le **cause scatenanti della seconda guerra mondiale** c'è l'insoddisfazione dei paesi sconfitti nella **Grande Guerra** su cui vengono fatti gravare gran parte dei costi del conflitto; questo negli anni crea un forte malessere economico e sociale che si aggrava con la crisi del 1929 e che, unitamente "*all' umiliazione di Versailles*" e alla debolezza della neonata Società delle Nazioni, apre la strada a regimi totalitari come quello nazista in Germania e quello fascista in Italia.

La Seconda Guerra Mondiale è stato il più grande conflitto armato della storia che ha visto scontrarsi le potenze dell'asse e degli alleati tra il 1939 e 1945: non solo la forza delle armi, ma anche i mezzi di comunicazione hanno avuto un vero e proprio ruolo in questo scontro, infatti si può definire una vera e propria **"guerra dei codici".**

Enigma fu una macchina elettro-meccanica per cifrare e decifrare messaggi. Nata da un tentativo di commercializzazione poi fallito (con lo scopo di stroncare lo spionaggio industriale), fu ampiamente utilizzata dal servizio delle forze armate tedesche durante il periodo nazista e della seconda guerra mondiale. La facilità d'uso e la presunta indecifrabilità (il modello base permetteva già di arrivare a 150 milioni di milioni di combinazioni diverse) furono le maggiori ragioni del suo ampio utilizzo.

Fu inventata dal tedesco Arthur Scherbius intorno agli anni 20, fu un dispositivo innovativo rispetto i metodi di cifratura esistenti fino a quel periodo. La macchina era costituita da una tastiera, simile a quelle delle macchine da scrivere, il cuore era lo scambiatore costituito dai rotori e dallo statore i quali permettevano la corrispondenza tra la lettera digitata e la visualizzazione attraverso dei collegamenti elettrici cablati nei dispositivi che essendo mobili potevano cambiare a seconda della posizione dei rotori.

All’ingresso dell’Inghilterra nella seconda guerra mondiale un matematico, logico e crittografo, entra come protagonista contro Enigma, Alan Mathison Turing.

Alan Turing
(inglese)

Alan Turing was born in London in 1912 and in 1931 he was admitted to Cambridge University, where he graduated with the highest marks. In 1936, he moved to Princeton University where he obtained a Ph.D. In those years, he published an article in which he described, for the first time, the "Turing machine".
During the Second World War, Alan Turing was enlisted by the English Department of Communications, in the cryptographic group, to develop the researches, already carried out by the Polish office, with the Bomb machine.
Based on these experience, Turing made a new version, much more effective, than the Rejewsky Bomb.
It was on Alan Turning’s concept that in 1942 the mathematician Max Newman designed a machine called Colossus, which quickly and efficiently deciphered the German codes created with encoder Lorenz SZ40/42, the enhancement Enigma encoder. Thanks to Colossus machine the Allies managed to defeat Nazi Germany.
In 1952 Alan Turing was arrested for homosexuality, sentenced and forced to choose a two-year prison sentence or chemical castration. Turing chose the second alternative, for over a year he took estrogens. In the opinion of many historians, led Turing to depression and humiliation, the decisive reason that led him to suicide in 1954.

(Alan Turing nacque a Londra nel 1912 e nel 1931 fu ammesso all’Università di Cambridge, dove si laureò a pieni voti. Nel 1936, si trasferì a Princeton dove ottenne il master. In quegli anni Turing pubblicò un articolo dove descrisse, per la prima volta, la macchina di Turing. Turing fu arruolato dal Department of Communication, nel gruppo do crittografici, sviluppò ricerche già svolte dall’ufficio Cifra polacco con la macchina Bomba.
Basandosi su tali esperienze, Turing realizzò una nuova versione, molto più efficace, della bomba di Rejewsky. Fu sul concetto di Alan Turing che nel 1942 il matematico Max Newman progettò una macchina chiamata Colossus, che decifrava in modo veloce ed efficiente i codici tedeschi creati con la cifratrice Lorenz SZ40/42, perfezionamento della cifratrice Enigma. Fu grazie a Colossus che gli alleati riuscirono a sconfiggere la Germania nazista.
Nel 1952 Alan Turing fu arrestato per omosessualità, condannato, fu costretto a scegliere da una pena detentiva di due anni o la castrazione chimica. Turing scelse la seconda alternativa, per oltre un anno assunse estrogeni, questo a parere

di molti storici, portò Turing alla depressione e all'umiliazione, motivo determinante che lo condusse, nel 1954 al suicidio.

Primo Levi
(italiano)

Primo Levi nasce nel 1919 da una famiglia ebrea a Torino dove compie gli studi fino alla laurea in chimica, è stato uno scrittore, partigiano e chimico italiano, autore di racconti, memorie poesie e romanzi.
Nel 1938, in seguito alle leggi razziali in Italia, perde l'impiego di chimico e nel 1943 si aggrega alle formazioni partigiane in Valle d'Aosta. Arrestato il 13 dicembre dello stesso anno è inviato, per la sua condizione di ebreo, al campo di raccolta di Fossoli, Modena. Nel 1944 viene deportato, insieme ad altri 650 ebrei, nel lager di Auschwitz, in Polonia.
Salvato dalla camera a gas perché i tedeschi avevano bisogno di chimici, viene liberato nel gennaio 1945 dalle truppe russe. Tornato in Italia alla fine del 1945 scrive della sua drammatica esperienza nei libri autobiografici "Se questo è un uomo" e "La tregua" (1963).
Ad animare la più importante produzione di Levi è la volontà di comunicare con i suoi simili, di condividerne l'esperienza per capire, di fornire una testimonianza oggettiva e documentaria della tragica esperienza del lager. In questo approccio scientifico di fiducia nella ragione umana risiede il suo profondo rispetto per la dignità umana. Dalla necessità di instaurare una comunicazione diretta con il lettore deriva la scelta di una lingua chiara e limpida. A ciò si aggiungono toni che talvolta si caricano di ironia, che fanno quasi da contrappunto alla tragicità dei temi.

Se questo è un uomo

Se questo è un uomo è una testimonianza autobiografica drammatica del degrado dell'uomo nei lager nazisti.
Rappresenta la coinvolgente ma immediata testimonianza di quanto vissuto dall'autore nel campo di concentramento di Monowitz. È nato, come afferma l'autore, da un impulso immediato e violento di raccontare agli altri le atrocità che si consumavano all'interno dei lager e a scopo di liberazione interiore.

(Levi, 1947) <<Considerate se questo è un uomo
Che lavora nel fango
Che non conosce pace
Che lotta per mezzo pane
Che muore per un sì o per un no.>>

- Sono alcuni versi introduttivi del romanzo, ispirati all'antica preghiera dello Shemà, e ne spiegano il titolo.

Le riflessioni dell'autore permettono al lettore di immedesimarsi con il protagonista ed affiancarlo idealmente nella sua esperienza. Per questo, la lettura del libro è un'esperienza intensa per il lettore. Si tratta inoltre di una esperienza che porta alla riflessione e che non di rado fa sorgere delle domande, per cui Levi ne pubblicò una parte tentando di rispondere.

Primo levi afferma “Vivendo e poi scrivendo e meditando quegli avvenimenti, ho imparato molte cose sugli uomini e sul mondo, e di queste ci rende partecipi”.
Con la sua testimonianza ci chiede di riflettere sul pericolo incombente di un ritorno delle barbarie del razzismo con i suoi spietati meccanismi dello sterminio di massa.

I linguaggi di programmazione

Un linguaggio di programmazione è un linguaggio formale dotato di una sintassi ben definita per scrivere programmi per calcolatori in una forma più vicina al linguaggio umano scritto: l’alternativa sarebbe scrivere in linguaggio macchina, compito improponibile per programmi complessi.
I linguaggi di programmazione si possono distinguere in due tipi:

- Alto livello, sono linguaggi comprensibili all’uomo (ad esempio Java, C, C++ ecc.);

- Basso livello, è il linguaggio macchina (ad esempio assembly).

Un linguaggio di programmazione deve soddisfare delle condizioni:

- Essere sequenziale (deve eseguire le istruzioni in sequenza);
- Possedere una struttura di selezione logica ed una iterazione.
- Variabile:
  - Un dato, noto o ignoto, già memorizzato o da memorizzare;
  - Ad una variabile corrisponde sempre un certo numero di locazioni di memoria.

Molti linguaggi inoltre attribuiscono alle variabili un tipo, con differenti proprietà (stringhe di testo, numeri, oggetti ecc.…)

Un linguaggio di programmazione è un linguaggio formale che specifica delle istruzioni che possono essere usate per produrre dati in output.
In informatica un linguaggio di programmazione è utilizzabile per il controllo del comportamento di una macchina formale o di una implementazione di essa (tipicamente, un computer) ovvero in fase di programmazione di questa attraverso la scrittura del codice sorgente di un programma ad opera di un programmatore. Un linguaggio di programmazione è considerato a tutti gli effetti tale se è Turing completo.

Tutti i linguaggi di programmazione esistenti sono definiti da un lessico, una sintassi ed una semantica e possiedono:

- Istruzione: un comando oppure una regola descrittiva: anche il concetto di istruzione è molto variabile fra i vari linguaggi. A prescindere dal particolare linguaggio però, ogni volta che un'istruzione viene eseguita, lo stato interno del calcolatore (che sia lo stato reale della macchina oppure un ambiente virtuale, teorico, creato dal linguaggio) cambia.

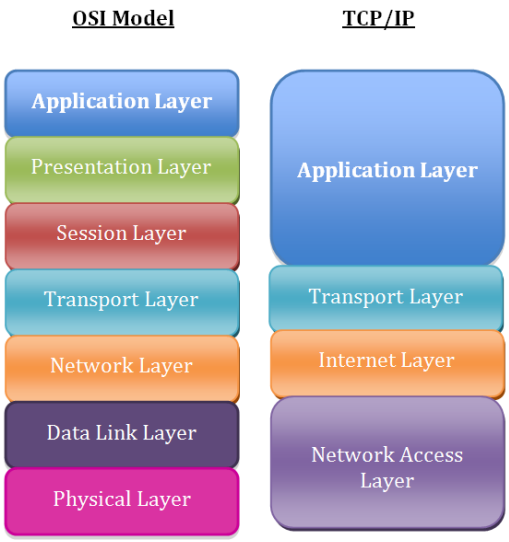
Alcuni concetti sono poi presenti nella gran parte dei linguaggi:

- Variabile e costante: un dato o un insieme di dati, noti o ignoti, già memorizzati o da memorizzare; ad una variabile corrisponde sempre, da qualche parte, un certo numero (fisso o variabile) di locazioni di memoria che vengono allocate, cioè riservate, per contenere i dati stessi. Molti linguaggi inoltre attribuiscono alle variabili un tipo, con differenti proprietà (stringhe di testo, numeri, liste, atomi ecc.) che può essere assegnato in maniera forte (tipizzazione forte) o in maniera debole (tipizzazione debole). Vi sono linguaggi di programmazione, come unlambda, che invece non utilizzano variabili. Alcuni linguaggi supportano l'uso dei cosiddetti puntatori a variabili.
- Espressione: una combinazione di variabili e costanti, unite da operatori; le espressioni sono state introdotte inizialmente per rappresentare le espressioni matematiche, ma in seguito la loro funzionalità si è estesa. Una espressione viene **valutata** per produrre un valore, e la sua valutazione può produrre "effetti collaterali" sul sistema e/o sugli oggetti che vi partecipano.
- Strutture dati, meccanismi che permettono di organizzare e gestire dati complessi.
- Strutture di controllo, che permettono di governare il flusso di esecuzione del programma, alterandolo in base al risultato o valutazione di una espressione (che può ridursi al contenuto di una variabile, o essere anche molto complessa) (cicli iterativi quali ad esempio for, do, while e strutture condizionali quali ad esempio if, switch-case).
- Sottoprogramma: un blocco di codice che può essere richiamato da qualsiasi altro punto del programma. In tale ambito quasi tutti linguaggi offrono funzionalità di riuso di codice accorpando cioè sequenze di istruzioni all'interno di funzioni richiamabili secondo necessità all'interno di programmi o all'interno di librerie richiamabili in ogni programma.
- Funzionalità di input dati da tastiera e visualizzazione dati in output (stampa a video) attraverso i cosiddetti canali standard (standard input, standard output).
- Possibilità di inserire dei commenti sul codice scritto, sintatticamente identificati e delimitati, che ne esplichino le funzionalità a beneficio della leggibilità o intelligibilità.

La crittografia nelle reti
(sistemi)

Nella sicurezza informatica la **sicurezza delle reti** è una problematica che nasce nel momento in cui si hanno più computer interconnessi fra loro cioè in una rete di calcolatori: essi, infatti, offrono diverse vulnerabilità sfruttabili, più o meno facilmente, da terzi per intromettersi nel sistema ed intercettarne i dati. Un'importante aggravante deriva dal fatto che Internet è nata come rete didattica in un ambiente universitario e le sue regole non prevedono metodi di sicurezza impliciti alla propria struttura: le difese devono essere messe in atto sulle macchine stesse o creando strutture di rete particolari.

Così nascono i protocolli: SSL (Secure Sockets Layer) e il suo successore TSL (Transport Layer Security), sono dei protocolli crittografici di presentazione usati nel campo delle telecomunicazioni e dell'informatica che permettono una comunicazione sicura dalla sorgente al destinatario su reti TCP/IP (Transmission Control Protocol e Internet Protocol) (come ad esempio internet) fornendo autenticazione, integrità dei dati e cifratura operando al di sopra del livello trasporto.



Diverse versioni del protocollo sono ampiamente usate in applicazioni quali i browser, l'e-mail, la messaggistica istantanea e il voice over IP (VOIP). Un esempio di applicazione di SSL/TSL è nel protocollo HTTPS.
L'HTTPS (HyperText Transfer Protocol over Secure Socket Layer), è un protocollo per la comunicazione sicura attraverso una rete di computer, il quale è largamente utilizzato su Internet. HTTPS consiste nella comunicazione tramite protocollo http all'interno di una connessione criptata dal TLS o dal suo predecessore SSL. Il principio che sta alla base di HTTPS è quello di avere:

- Un'autenticazione del sito web visitato;
- Protezione della privacy;
- Integrità dei dati scambiati tra le parti comunicanti.

In telecomunicazioni ed informatica è il risultato dell'applicazione di un protocollo di crittografia asimmetrica al protocollo di trasferimento di ipertesti HTTP. Viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire l'intercettazione dei contenuti.
Il protocollo TLS consente alle applicazioni client/server di comunicare attraverso una rete in modo da prevenire il 'tampering' (manomissione) dei dati, nella sua ultima versione, è definito RFC 5246(Request for Comments) sviluppata sulla base del precedente protocollo SSL da Netscape Communications.
Nell'utilizzo tipico di un browser da parte di un utente finale, l'autenticazione TSL è unilaterale: è il solo server ad autenticarsi presso il client (il client, cioè, conosce l'identità del server, ma non viceversa cioè il client rimane anonimo e non autenticato sul server).
Il funzionamento del TSL è suddivisibile in 3 fasi principali:

1. Negoziazione fra le parti dell'algoritmo da utilizzare;
2. Scambio delle chiavi e autenticazione;
3. Cifratura simmetrica e autenticazione dei messaggi.

Il client e il server negoziano il protocollo di cifratura che sarà utilizzato nella comunicazione, il protocollo per lo scambio delle chiavi e l'algoritmo di autenticazione (generalmente a chiave pubblica, o nel caso di TLS-PSK, fanno uso di una chiave precondivisa, Pre-Shared Key).

TPSIT
(dal sistema binario a decimale)

La decifrazione di Enigma e l'invenzione di Colossus avrebbe portato alla più grande rivoluzione delle comunicazioni: l'informatica moderna. Questo salto in avanti si appoggiò sullo sviluppo si codifica che permise di stabilire comunicazioni efficaci e rapide fra una vasta rete articolata intorno a due agenti fondamentali: i computer ed i loro utenti, cioè noi. Alla base di questa rivoluzione tecnologica si trova il sistema binario. Questo codice, formato da due caratteri, 0 e 1, è il più usato in informatica per la sua capacità di esprimere funzioni logiche, mediante le quali è possibile l'interazione con i circuiti elettronici di computer ed altri apparati. Ogni 0 e ogni 1 è chiamato bit (termine derivato dall'inglese binari digit, cioè "cifra binaria").

Il sistema numerico binario è un sistema numerico posizionale in base 2. Esso utilizza solo due simboli, di solito indicati con 0 e 1, invece delle dieci cifre utilizzate dal sistema numerico decimale. Ciascuno dei numeri espressi nel sistema numerico binario è definito "numero binario".

In informatica il sistema binario è utilizzato per la rappresentazione interna dell'informazione dalla quasi totalità degli elaboratori elettronici, in quanto le caratteristiche fisiche dei circuiti digitali rendono molto conveniente la gestione di due soli valori, rappresentati fisicamente da due diversi livelli di tensione elettrica. Tali valori assumono convenzionalmente il significato numerico di 0 e 1 o quelli di vero e falso della logica booleana.

Nel corso della storia, l'uomo, seppe inventare mezzi pratici che gli permisero di disegnare molti numeri con pochi simboli. A tal fine gli fu necessaria una "scala convenzionale" di simboli, che ora noi chiamiamo "base", per classificare numeri sempre più grandi. È da qui che nasce il sistema decimale in base 10 (1, 2, 3, 4, 5, 6, 7, 8, 9).

Se ad esempio vogliamo convertire dal sistema binario a quello decimale il numero 1001001 dobbiamo utilizzare l'algoritmo della moltiplicazione:

Primo passaggio: $(1 * 2^0 = 1) + (0 * 2^1 = 0) + (0 * 2^2 = 0) + (1 * 2^3 = 8) + (0 * 2^4 = 0) + (0 * 2^5 = 0) + (1 * 2^6 = 64)$

Secondo passaggio: $1 + 0 + 0 + 8 + 0 + 0 + 64 = 73$

Quindi il mio numero corrisponde a 73 espresso nel sistema decimale.

Questo per far capire che il computer (mediante la CPU) esegue milioni, se non miliardi, di questi calcoli in un solo secondo.