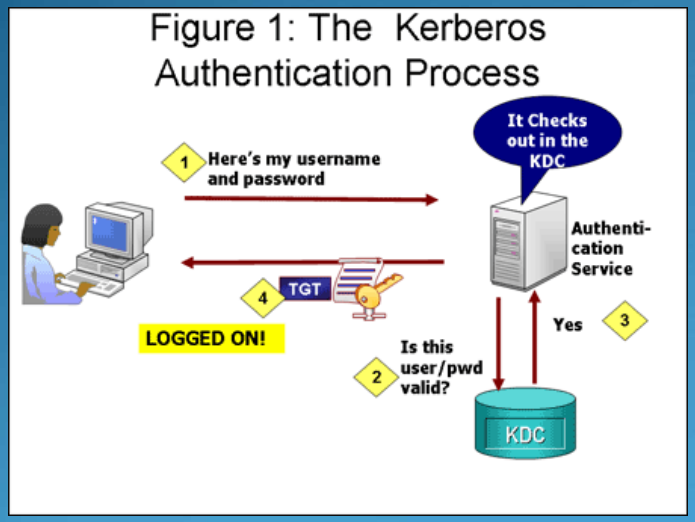
FSE - Formazione in servizio all'innovazione didattica e organizzativa
Con il PNSD nuova governance e didattica a misura di studenti
Modulo: Formazione Team per l'innovazione Modulo 1 – A.S. 2016/17

# Project Work:
# Sicurezza in rete

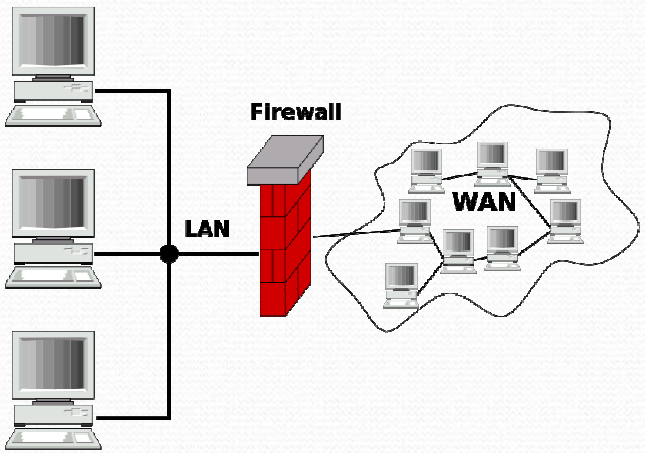

**Team dell'innovazione digitale :**
**Prof.ssa Luongo Maria Teresa**
**I.C. «Rita Levi Montalcini» - S. Giorgio del Sannio (BN)**

# Sicurezza in rete
# AUTENTICAZIONE



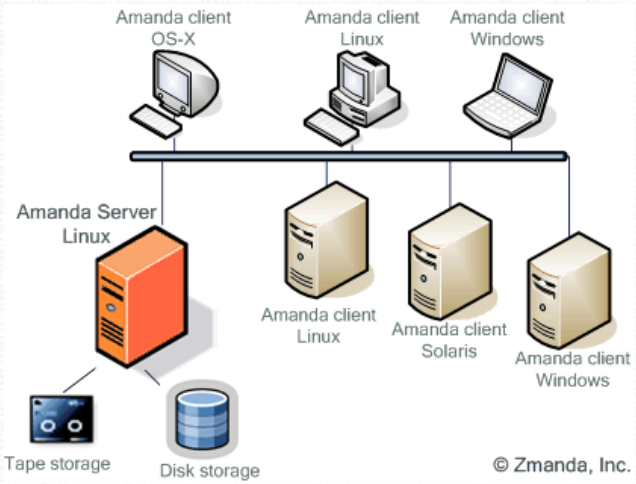

Ogni utente che utilizza la rete sia locale (LAN) sia esterna (WAN) deve autenticarsi tramite le proprie credenziali ed ogni accesso e operazione che avviene sulla rete deve essere loggata e monitorata. A seconda del livello di credenziali l'utente potrà accedere a determinate parti della rete.

# Sicurezza in rete
# Protezione da attacchi esterni




Per evitare attacchi alla rete locale (LAN) provenienti dalla rete esterna (WAN), nella rete bisogna inserire un firewall opportunamente configurato in modo da limitare gli attacchi dall'esterno. Il firewall deve essere configurato per impedire l'accesso verso i siti con note pericolosità di rete. Inoltre, a seconda dell'utente, i siti esterni visibili dovranno essere limitati.

# Sicurezza in rete
# BACKUP




Al fine di evitare la perdita dei dati importanti, la rete deve offrire funzionalità di BACKUP automatico. Con la continua diffusione di CRIPTOLOKER,(software malevoli e silenti che crittografano i dati e chiedono il riscatto per decodificarli), è diventato indispensabile dotare la rete di un sistema di BACKUP efficace ed efficiente.

# Sicurezza in rete
# Esempi di attacchi esterni


La maggior parte delle volte è proprio durante la navigazione in internet che scarichiamo, in modo totalmente inconsapevole, software dannosi…

- **Spyware**= virus che raccoglie informazioni sulla nostra attività on line.
- **Spoofing**= attacco l'utente con la falsificazione dell'indirizzo del mittente.
- **Phishing**= invio di una mail con il logo contraffatto, per es. di un istituto di credito, per chiedere all'utente credenziali e dati riservati.
- **Spamming**= invio di un elevato numero di messaggi di posta indesiderati di tipo promozionale.
- **Defacing**= cambio illecitamente la home page di un sito web per ingannare l'utente.
- **Botnet**= è una rete di computer controllata da un Botmaster (pirata informatico) e usata per diffondere mail con allegati contenenti Trojan (un software dannoso che appare come un software utile o apparentemente sicuro, l'utente lo esegue di sua spontanea volontà facendo avviare anche il virus celato al suo interno…).

# Sicurezza in rete

# Alcuni strumenti per la sicurezza

## Crittografia

Fornisce uno strumento adatto a mantenere segrete tutte quelle informazioni che non si vogliono divulgare pubblicamente, in maniera tale che la possibilità di accedervi sia data solo a persone autorizzate.

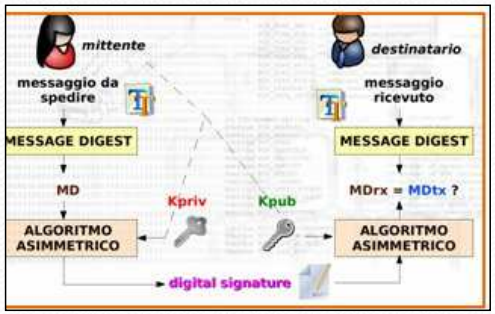
Gli algoritmi basati sull'utilizzo di chiavi si dividono in:

1. A chiave simmetrica, con un'unica chiave per cifrare e decifrare il messaggio.
2. A chiave asimmetrica, con 2 chiavi diverse (una pubblica e una segreta).

Le chiavi di indirizzo di cifratura devono essere lunghe e con caratteri alfanumerici. MAGGIORE COMPLESSITA'= MAGGIORE ROBUSTEZZA.

## Firma Digitale

- E' un meccanismo a chiave pubblica di cifratura che utilizza il sistema a chiave pubblica/chiave segreta.
- E' importante per la validità legale perché identifica il mittente.
- Garantisce l'integrità del documento, ossia che il documento non è stato modificato.
- E' un sistema di autentificazione e di non ripudio.



# Sicurezza in rete

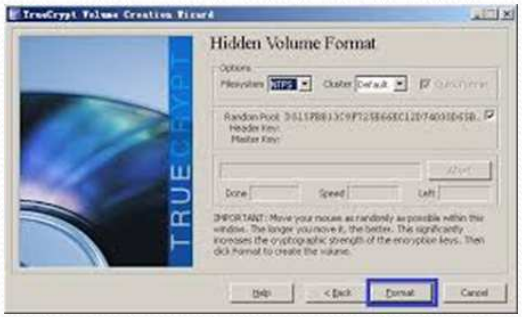
## Strumenti per la sicurezza: Copiare i dati


L'app che ti permette di sincronizzare file e cartelle e di avere più copie dei documenti…

- **Dsynchronize** è un'applicazione gratuita che consente di sincronizzare le cartelle presenti sul disco rigido con quelle poste su Floppy Disk, LAN, USB Key, CD-DVD. Copia i file più recenti e modificati all'interno di una cartella, in questo modo si ottengono facilmente copie dei documenti (per es. una sul pc di casa, una sulla chiavetta USB, una sul pc di scuola) e ciò contribuisce a evitarne la perdita in caso di guasti o virus. E' possibile specificare con esattezza l'ora e i giorni in cui si vuole sincronizzare le varie cartelle, è anche possibile impostare dei filtri di selezione dei file.

# Sicurezza in rete

## Strumenti per la sicurezza: Cifrare i dati





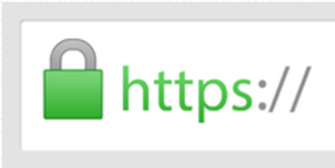
- **Truecrypt** è un'applicazione gratuita che permette di creare all'interno del disco rigido ed anche su supporti rimovibili USB Key, CD, DVD, ecc., *Volumi* (dischi fissi) *Virtuali* da usare come un contenitore di cifratura su cui salvare i nostri documenti e file. E' virtuale perché rappresenta un file criptato che, una volta installato, viene letto dal pc come un'unità fisica. Il disco virtuale può essere «montato» e «smontato» in pochi secondi rendendo disponibile o no il contenuto, che smontato è protetto da sistemi molto sofisticati di crittografia avanzata da selezionare fra oltre una dozzina. Per accedere ai file cifrati occorre inserire una password di accesso.

# Sicurezza in rete
# Navigare sicuri

## Quando un sito web è sicuro?

- Quando viene visualizzato il lucchetto accanto alla barra degli indirizzi del browser, si può essere sicuri che **una serie completa di operazioni di sicurezza** è stata eseguita con successo.
- Insieme al lucchetto, verrà visualizzata anche la scritta **https://** nella barra degli indirizzi del browser, all'inizio dell'indirizzo del sito Web al quale ci si è collegati.

Se poi il Certificato SSL del server Web è di tipo **Extended Validation** (EV), il browser lo evidenzierà chiaramente, solitamente in verde, sempre nella barra degli indirizzi. Ciò rappresenta l'assicurazione che il proprietario del sito Web **ha subìto controlli molto più ampi e approfonditi** di quelli normali, per ottenere appunto il Certificato SSL.




## Alcune estensioni per navigare sicuri.

Dalla barra di Impostazioni di Google Crome è possibile scaricare una serie di estensioni per migliorare la sicurezza in rete. Per esempio:

-  **AdBlock** permette di eliminare i contenuti pubblicitari in molte pagine web;
-  **Ghostery** protegge la privacy da quei siti che tracciano la navigazione (il tracking).
-  **Safe Search** blocca dei contenuti espliciti su Google, (è utile per tutelare i minori dalla visualizzazione di risultati di ricerca non appropriati su smartphone, tablet o computer).

E' comunque sempre consigliabile installare sul Pc due browser in modo da avere sempre garantita la possibilità di navigare, nel caso uno dei due venga attaccato da malware...

# Sicurezza in rete

# Educazione ai social media: i docenti


Docenti in rete… come comportarsi?

**LA QUESTIONE:** *Noi docenti possiamo commentare o esternare le nostre idee, impressioni o modi di essere sui social?*

**I RISCHI:**

- perdita di autorevolezza;
- dubbi sulla capacità di operare correttamente;
- fraintendimenti e sospetti da parte dell'utenza (alunni/genitori).

Nella funzione di Giudizio, Gestione, Comparazione degli studenti, il docente ha l'obbligo di essere equo e di apparire equo. = Chi viene valutato non deve mai avere l'impressione di essere stato soggetto ad un effetto/idea collaterale…

**LA SOLUZIONE:** per es. avere un profilo Facebook ASETTICO da parte del docente.

Ogni post deve essere MOTIVATO ASETTICAMENTE dal docente per non inficiare l'immagine e la valenza di EQUITA' della sua valutazione.

# Educazione ai social media: i minori e la privacy


E' on Line la guida del Garante per la protezione dei dati personali dedicata alla scuola. Consultabile al sito: www.garanteprivacy.it

**Ciò che pubblichiamo in rete… rimane nella rete!**

- Su Facebook e sui Social in generale

*NON si devono pubblicare immagini di alunni minorenni in modo che siano riconoscibili,* (e questo anche nel caso di fatti di rilevanza pubblica se prima non si è acquisito il consenso dei genitori). Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese e fare incorrere il responsabile in sanzioni ed in eventuali reati.

Basti pensare che, nel momento in cui viene pubblicato on line, il contenuto di foto e video cessa di essere di proprietà dell'utente per divenire oggetto del web… perdendone così per sempre il suo controllo. Ciò è tanto più rilevante se si tratta di immagini di minori!

Tale diffusione può arrecare non solo un pregiudizio alla riservatezza individuale, ma incrementare anche il rischio che le persone interessate possano subire abusi, come il cosiddetto furto di identità, o perfino che le loro foto vengano modificate ed utilizzate per produrre immagini pedopornografiche.

## Modulo: Formazione Team per l'innovazione Modulo 1 – A.S. 2016/17

## Project Work: Sicurezza in rete

**A cura del Team dell'innovazione digitale : Prof.ssa Luongo Maria Teresa**

**I.C. «Rita Levi Montalcini» - S. Giorgio del Sannio (BN)**


Fine presentazione