ICPPA

Lezione 5

Sicurezza - Privacy

1

Dichiarazione di copyright

Dichiarazione di copyright

L'utilizzo dei contenuti della lezione sono riservati alla fruizione personale degli studenti iscritti ai corsi dell'Università di Camerino. ***Sono vietate*** *la diffusione intera o parziale di video o immagini della lezione, nonché la modifica dei contenuti senza il consenso, espresso per iscritto, del titolare o dei titolari dei diritti d'autore e di immagine.*

Copyright notice

The contents of this lesson are subject to copyright and intended only for personal use by students enrolled in courses offered by the University of Camerino. For this reason, any partial or total reproduction, adaptation, modification and/or transformation of the contents of this lesson, by any means, without the prior written authorization of the copyright owner, is strictly prohibited.

2

Protezione dei dati

presupposto

I messaggi di posta elettronica sono come delle cartoline, che possono essere lette da tutti.

Che accadrebbe se tutti pensassero che i cittadini onesti usano solo cartoline per la loro posta?

Fortunatamente tutti proteggono la maggior parte della loro posta chiudendola in una busta.

Sarebbe giusto se tutti usassero abitualmente la crittografia per la loro posta elettronica.

Privacy: D.L. 30/6/2003 n 156 ("Legge sulla privacy").

https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2003-07-29&atto.codiceRedazionale=003G0218

3

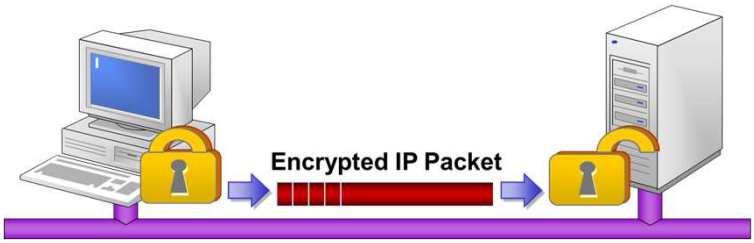
3

La crittografia

La crittografia:
Scrittura convenzionale segreta, decifrabile solo da chi sia a conoscenza del codice.

La crittografia è l'arte di **progettare algoritmi** (o cifrari) per crittografare un messaggio rendendolo **incomprensibile** a tutti tranne al suo destinatario

Il destinatario, con un **algoritmo simile** deve essere in grado di codificarlo, attraverso un parametro segreto detto **chiave** (usato in precedenza anche dal mittente per la cifratura).



4

4

Tipi di chiavi

Key type	Description
 Symmetric	• **La stessa chiave è usata per cifrare e decifrare i dati** • **Protegge i dati dall'intercettazione**
 Asymmetric	• **Consiste in una chiave pubblica e una privata** • **La chiave privata è protetta e confidenziale, la chiave pubblica è liberamente distribuibile** • **Se viene usata la chiave privata per cifrare dei dati, gli stessi possono essere decifrati esclusivamente con la corrispondente chiave pubblica, e vice versa**

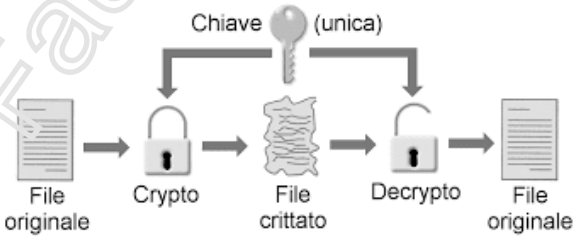
5

5

Tecniche di crittografia

➢ **Crittografia a chiave singola (c. simmetrica)**

- La stessa chiave codifica e decodifica i messaggi.



Symmetric encryption:

- ✓ Usa la stessa chiave per cifrare e decifrare
- ✓ E' spesso referenziata come bulk encryption
- ✓ E' intrinsicamente vulnerabile per il concetto di "Shared secret": la chiave è condivisa

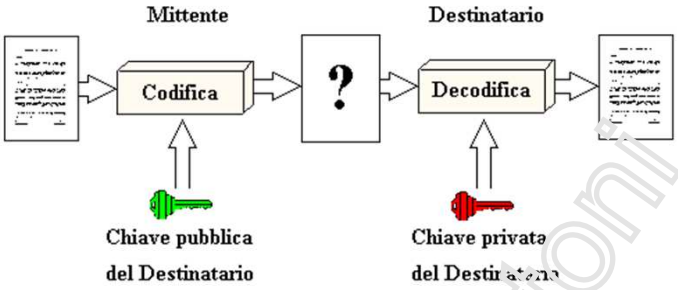
6

6

Tecniche di crittografia

➢Crittografia a chiave pubblica (c. asimmetrica)

- Una chiave pubblica e una privata cifrano e decifrano i messaggi, in modo che nemmeno il mittente può decifrare il proprio messaggio, una volta codificato



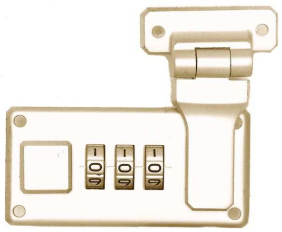
7

7

Lunghezza della chiave

La lunghezza della chiave utilizzata è uno dei fattori più importanti per la segretezza del resto:
evita infatti che possa essere decifrato per tentativi

Provare tutte le possibili combinazioni di caratteri che potrebbero formare una chiave è un problema che gli analisti definiscono a complessità computazionale esponenziale: **brute force**
basta aggiungere una sola lettera alla chiave per aumentare in modo vertiginoso il numero di possibili combinazioni che possono essere ottenute.



8

8

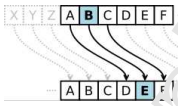
Il cifrato di Cesare

Per comunicare con i sui generali, Giulio Cesare sostituiva ad ogni lettera del messaggio un'altra lettera un certo numero di posizioni più avanti nell'alfabeto.

Per l'esattezza utilizzava la chiave "3",
tutte le lettere venivano scalate di tre cifre:
la A diventava D, la B diventava E, la C diventava F e così via.

Con questo metodo la frase:

PROVA DI CIFRATURA
diventa
SURYD GL FLIUDWXUD



https://www.codingcreativo.it/cifrario-di-cesare-online/

9

9

Il cifrario di Atbash

Il cifrario di Atbash è uno dei primi cifrari a **sostituzione monalfabetica**:
la prima lettera dell'alfabeto viene sostituita con l'ultima, la seconda con la penultima, e così per tutte le altre lettere. Si tratta essenzialmente dell'inversione dell'alfabeto.

10

10

Crittografia a chiave segreta

Tutti i sistemi di cifratura visti fino a questo punto sono detti a chiave segreta ed utilizzano la stessa chiave sia per cifrare che per decifrare.

Le due parti devono riuscire in qualche modo a **scambiarsi la chiave** con la certezza che nessuno ne venga a conoscenza, un problema non indifferente.

La soluzione a questo tipo di problema fu proposta nel 1975 da Whitfield Diffie e Martin Hellman, che ebbero un'intuizione che rivoluzionò il mondo della crittografia

11

11

Le chiavi asimmetriche

Diffie ed Hellman pensarono ad un **sistema asimmetrico**, basato su l'uso di due chiavi:
generate in modo che sia impossibile ricavarne una dall'altra.

Le due chiavi vengono chiamate **pubblica e privata**:

la prima serve per cifrare e la seconda per decifrare.

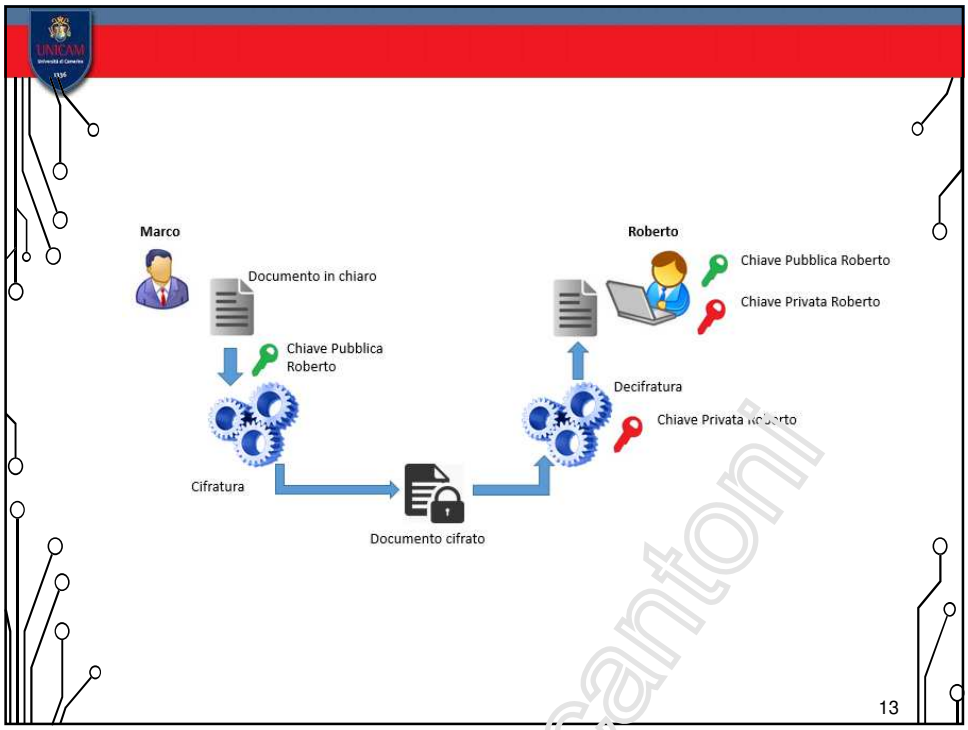
Ogni persona con questo sistema possiede quindi **una coppia di chiavi**:

quella pubblica può essere tranquillamente distribuita e resa di pubblico dominio perché consente solo di cifrare il messaggio

quella privata deve essere conosciuta solo da una persona consente di decifrare il messaggio

12

12



13

Cryptographic hash function

Una funzione hash crittografica (cryptographic hash function, CHF) è un algoritmo matematico che mappa i dati («messaggio») di dimensione arbitraria su una matrice di bit di dimensione fissa (il «valore hash» o «hash value», «hash» o «digest del messaggio»). È una funzione unidirezionale, cioè una funzione che è praticamente impossibile invertire.

Alcune applicazioni di «cryptographic hash function»

- ✓ Verifica dell'integrità di messaggi (copia/trasmissione)
- ✓ Generazione e verifica della firma digitale (pec)
- ✓ Verifica della password (password hashing)
- ✓ Proof-of-work (criptovalute)
- ✓ Identificatore di file o dati (git)

14

14

Verifica dell'integrità di messaggi e file

Un'importante applicazione degli hash sicuri è la verifica dell'integrità dei messaggi e file. Ad esempio: prima e dopo la trasmissione/copia (via rete, da un dispositivo di storage ad un altro…)

- Viene calcolato il digest del messaggio/file prima della trasmissione/copia
- Viene calcolato il digest del messaggio/file ricevuto/copiato
- Confrontando i due digest è possibile determinare se sono state apportate modifiche al messaggio/file

Cryptographic hash algorithms
MD5, SHA-1, SHA-2, SHA-3 …

15

15

Esempio MD5

https://emn178.github.io/online-tools/md5.html

https://it.wikisource.org/wiki/Divina_Commedia/Inferno/Canto_I

16

16

La firma digitale

La firma digitale viene da molti considerata uno dei migliori mezzi possibili per ridurre drasticamente i problemi di sicurezza relativi alla trasmissione di documenti per via telematica.
Tale sistema permette di semplificare sia i rapporti tra imprese e/o privati che quelli tra cittadini e pubblica amministrazione.

La legge la definisce il risultato di una procedura informatica – validazione – che attraverso un procedimento crittografico a chiavi asimmetriche, permette di identificare il reale mittente di un documento informatico verificandone l'autenticità.

17

17

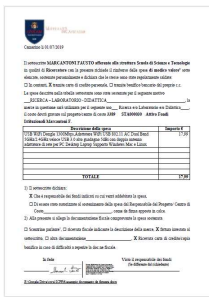
Firma di un documento

esempio documento da firmare

MS Word

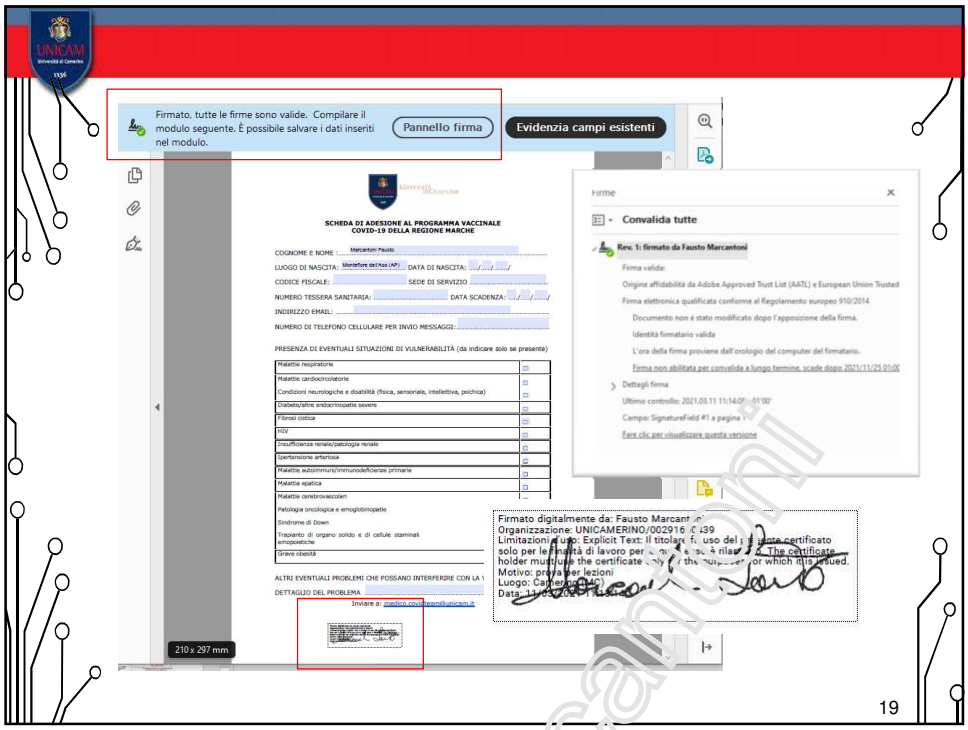
PDF

PDF firmato



18

18



19

19

Messaggi a firma digitale

Messaggi a firma digitale

Come viene inviato un messaggio? Tre diversi modi:

il mittente in possesso della chiave pubblica del destinatario cifra con essa il messaggio; il destinatario attraverso la propria chiave privata può decifrarlo;

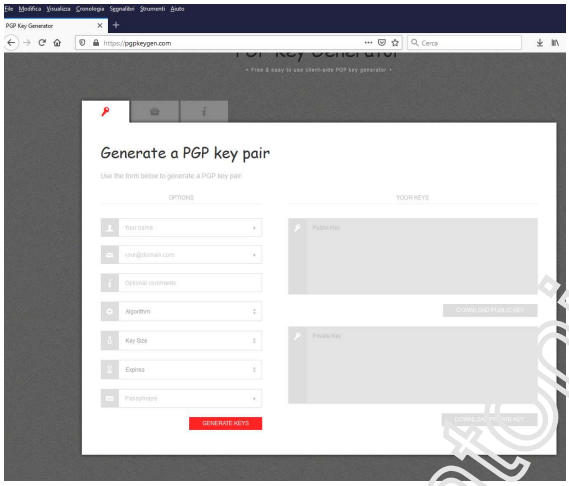
è il mittente a rendere cifrato il messaggio con la propria chiave privata, in questo caso chiunque sia in possesso della chiave pubblica del mittente può decifrarlo (in questo modo viene assicurata la reale identità del mittente);

il mittente cifra il proprio messaggio con la chiave pubblica del destinatario e con la propria chiave privata; il ricevente dovrà decifrare il testo sia con la propria chiave privata che con quella pubblica del mittente. In questo modo oltre alla segretezza del messaggio dovrebbe essere garantita anche l'autenticità della provenienza.

20

20

Creare chiave PGP

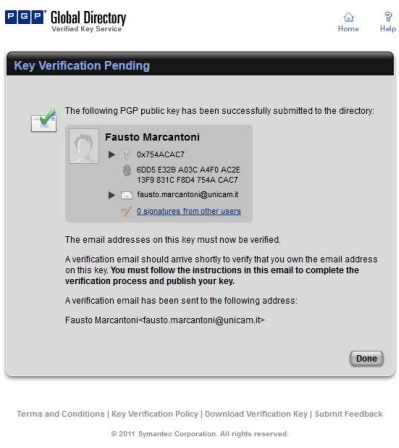


https://pgpkeygen.com/

21

21

Pubblicare chiavi PGP

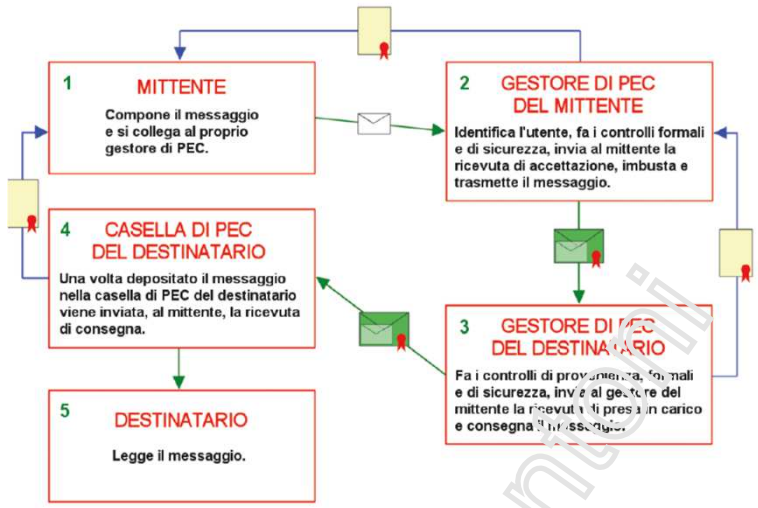


https://keyserver.pgp.com/vkd/GetWelcomeScreen.event

22

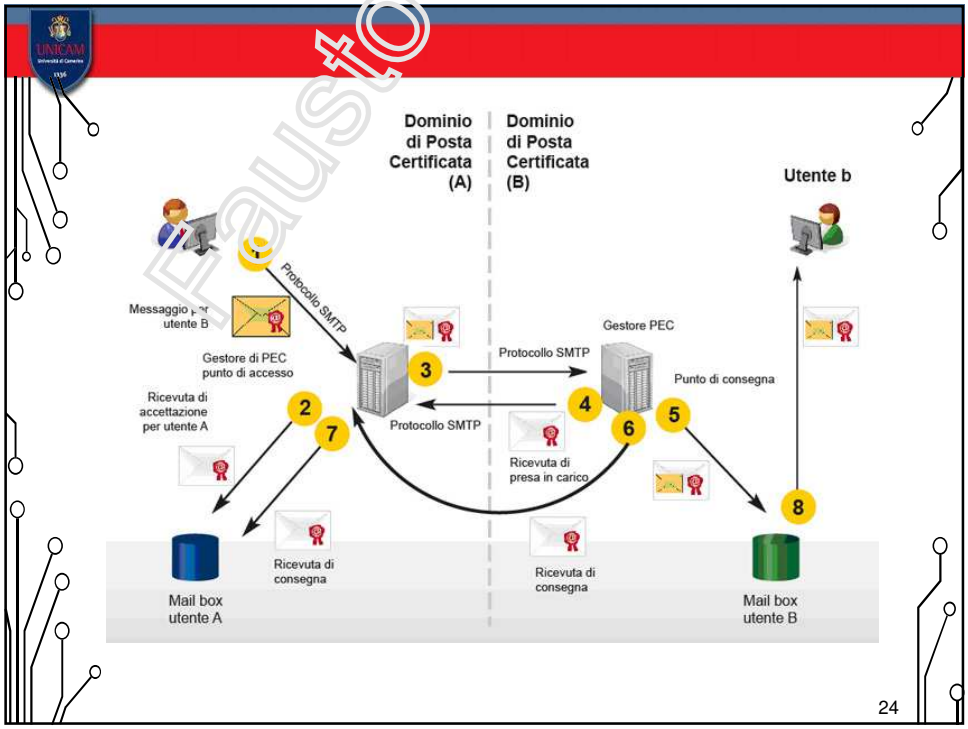
22

PEC: Posta Elettronica Certificata



23

23



24

24

1 - Il mittente (utente A) invia un **messaggio** al destinatario attraverso il **server di Posta Elettronica Certificata** del suo gestore (punto di accesso), previa verifica delle credenziali di accesso.

2- Il gestore provvede a inviare nella casella del mittente (utente A) una ricevuta di accettazione o di non accettazione, sulla base dei controlli formali effettuati sul messaggio pervenuto. Le ricevute riportano la data e l'ora dell'evento, l'oggetto del messaggio e i dati del mittente e del destinatario e l'eventuale causa di non accettazione.

3- Il messaggio viene quindi imbustato all'interno di un altro messaggio (chiamato busta di trasporto) di tipo S/MIME firmato digitalmente dal gestore e inviato al punto di ricezione (gestore del destinatario).

4- Il punto di ricezione effettua il **controllo della firma del gestore mittente** e verifica la validità del messaggio: in caso di esito positivo provvede a inviare al server del gestore mittente una **ricevuta di presa in carico del messaggio** e invia il messaggio verso il punto di consegna.

5- 8 Il punto di consegna rende disponibile il messaggio nella casella del destinatario (utente B), e questo punto il destinatario (utente B) è in grado di **leggere il messaggio di Posta Elettronica Certificata** (punto 8).

6-Il **punto di consegna** invia al gestore mittente una **ricevuta di avvenuta consegna**.

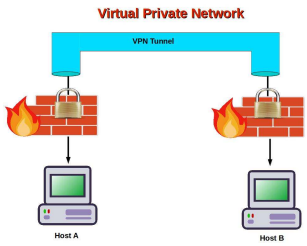
7- Il gestore mittente rende disponibile la **ricevuta di avvenuta consegna** nella casella del mittente (utente A)

25

25

Virtual Private Network

Una VPN (Virtual Private Network) consente di creare una rete privata virtuale che garantisce privacy, anonimato e sicurezza dei dati attraverso un canale di comunicazione riservato tra dispositivi che non necessariamente devono essere collegati alla stessa LAN.

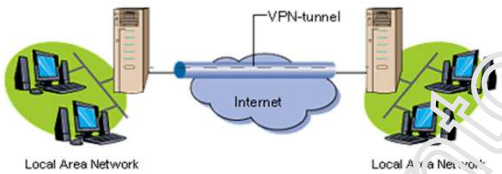


26

26

Virtual Private Network

Una VPN è un servizio di comunicazione "logico" sicuro e affidabile fra due o più apparecchiature, realizzata sopra una infrastruttura di rete pubblica potenzialmente non sicura, che rispetta i principi di **riservatezza, integrità e autenticazione**. Una connessione VPN si può rappresentare graficamente come un "**tunnel**" tra due terminali della VPN stessa (endpoint) dietro cui sono attestati gli host che comunicano.



27

27

Virtual Private Network

- ✓ Le VPN migliorano le comunicazioni, in quanto gli utenti remoti si possono connettere alle risorse aziendali in sicurezza da qualunque luogo 24 ore su 24.
- ✓ Sono flessibili e scalabili, in quanto un'infrastruttura VPN può adattarsi con facilità alle necessità di cambiamento delle reti.
- ✓ Sono sicure ed affidabili, in quanto le connessioni VPN sono protette da meccanismi di autenticazione, crittografia e protezione dell'integrità dei dati.
- ✓ Sono indipendenti dagli standard tecnologici dei primi due livelli della pila OSI. Questo garantisce che una rete non sia vulnerabile alle caratteristiche di debolezza (insicurezza) dei primi due livelli.

28

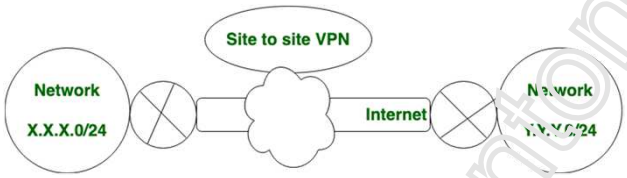
28

Virtual Private Network

Site-to-site VPN

I collegamenti che vengono fatti tra due sedi, aziendali e non, possono essere di due tipi:

- **Intranet VPN** quando uniscono sedi della stessa azienda, scuola, ufficio, ecc.
- **Extranet VPN** quando uniscono aziende, scuole, uffici, ecc. diverse che devono condividere delle informazioni tra di loro



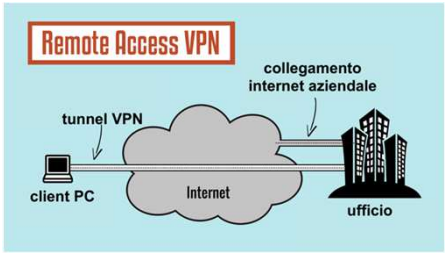
29

29

Virtual Private Network

VPN per accesso remoto

Le connessioni VPN di accesso remoto consentono agli utenti che **lavorano da casa** o **in movimento** di accedere a un server su una rete privata utilizzando l'infrastruttura resa disponibile da una rete pubblica, ad esempio Internet.
Dal punto di vista dell'utente la VPN è una **connessione Point-to-Point** tra il computer (il client VPN) e il server di un'organizzazione. L'infrastruttura della rete condivisa è irrilevante, inquanto, dal punto di vista logico è come se i dati venissero inviati su un collegamento privato dedicato



30

30

31

32