

# **SICUREZZA in RETE**

# SOMMARIO

## 1. Introduzione

## 2. Firewall

## 3. Crittografia

- Crittografia a chiave segreta
- Crittografia a chiave pubblica
- Hashing

## 4. Applicazioni

- Firma digitale e certificati
- IPSec, SSL
- Virtual Private Network

# Requisiti di sicurezza in un sistema informativo distribuito:

- Protezione dei dati da
  - Accessi non autorizzati
  - Danni (intenzionali o accidentali)
- Protezione del sistema da attacchi esterni che possono causare interruzione del servizio (*Denial-of-Service*)
- Protezione dei dati comunicati tramite la rete

### Osservazione

La sicurezza non è una proprietà binaria. Per ogni sistema informativo è necessario definire:

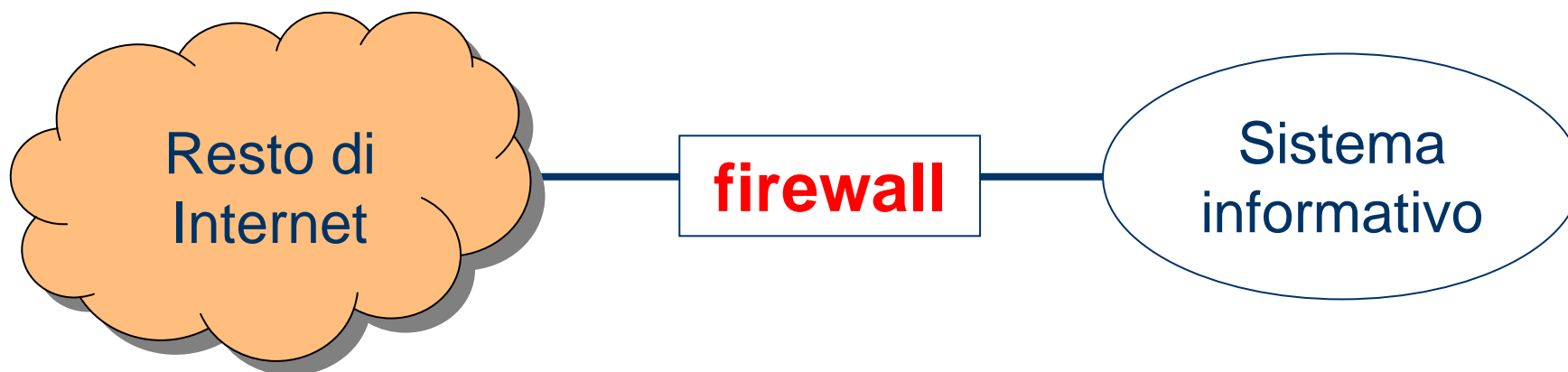
- Politica di sicurezza
- Valore dell'informazione

### Strumenti di base per la protezione dei dati:

- Uso di **password** (fissando regole per la scelta della password e frequenza di aggiornamento)
- Assegnazione di **privilegi di accesso** ai dati in scrittura/lettura, distinti in base al ruolo dell'utente
- Uso di **sistemi di back-up** e sistemi di memoria secondaria che offrono protezione dei dati (ad es. **RAID**)
- Uso di **antivirus**

# FIREWALL

Router che collega il sistema informativo al resto della rete (ad es. Internet) e filtra il traffico che lo attraversa e in particolare il traffico in ingresso al sistema informativo



### Cosa è utile filtrare?

- Traffico diretto a host o servizi (cioè programmi server) ai quali non si vuole permettere l'accesso dall'esterno
- Traffico proveniente da indirizzi o domini indesiderati (ad esempio noti come generatori di SPAM, virus, o denial-of-service attacks)
- Traffico contenente parole o frasi specifiche (ad es. Viagra)

### Come funziona un firewall?

**Filter based:** è configurato con una tabella che mantiene una lista di quadruple:

<Source-IPaddr, Source-Port, Dest-IPaddr, Dest-Port>

che rappresentano connessioni di livello transport (TCP/UDP) proibite o permesse. E' possibile filtrare anche nomi (mnemonici) di domini, o pacchetti contenenti parole o frasi specifiche

**Proxy-based:** è inserito in modo trasparente tra un client esterno al sistema informativo e un server interno al sistema informativo (ad es. web-server) e filtra selettivamente le richieste, piuttosto che impedire completamente l'accesso al servizio



### Requisiti per la sicurezza delle comunicazioni:

- **PRIVACY:** evitare che i dati inviati da un soggetto A a un soggetto B vengano conosciuti da un terzo soggetto (male intenzionato) C. Es. Numero della carta di credito
- **AUTHENTICATION:** accertare l'identità di chi manda o riceve i dati (evitare cioè che un intruso si spacci per chi non è).
- **MESSAGE INTEGRITY:** verificare che i dati ricevuti siano conformi a quelli inviati (evitare cioè che un intruso intercetti e alteri i dati durante la trasmissione).

## Crittografia

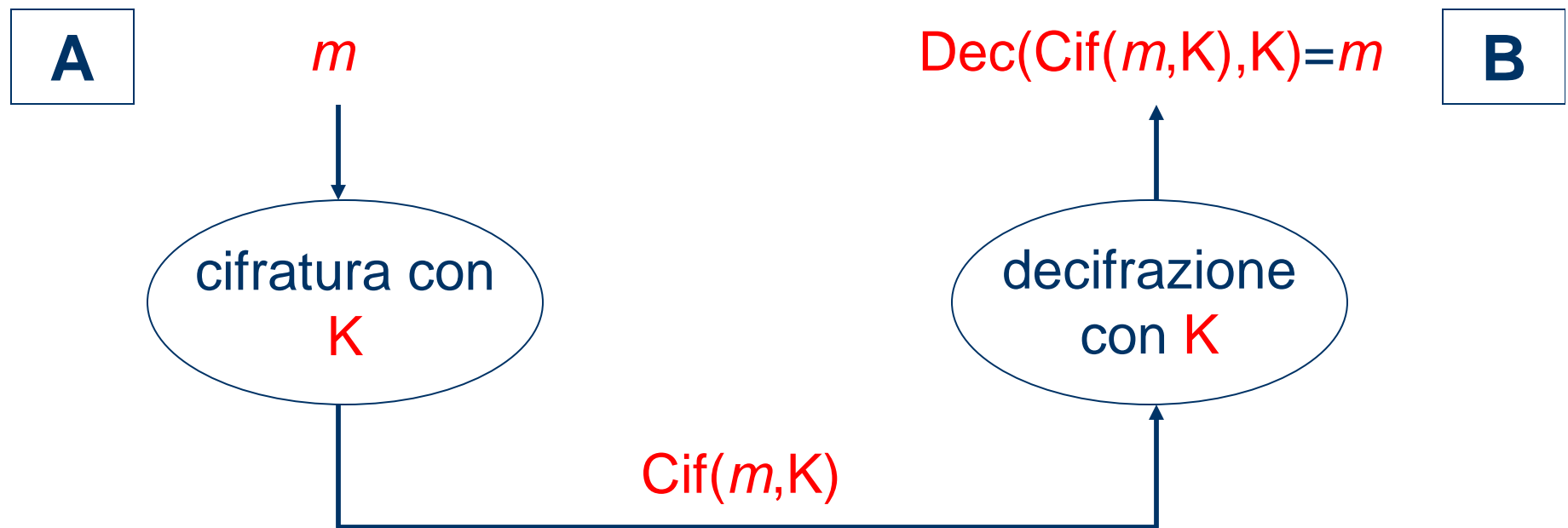
---

Lo strumento di base usato per realizzare i requisiti di sicurezza nelle comunicazioni è la **crittologia**, ovvero lo studio di tecniche per la cifratura e decifrazione di messaggi.

- **Crittografia:** (“scrittura nascosta”) insieme di tecniche per la cifratura di messaggi. Obiettivi:
  - Cifratura (computazionalmente) facile
  - Decifrazione (computazionalmente) difficile se non si conosce un'apposita chiave
- **Crittoanalisi:** insieme di tecniche per la decifrazione di messaggi cifrati, senza conoscere la chiave di cifratura

### Crittografia a Chiave Segreta

I due soggetti (A e B) usano una stessa chiave  $K$  per cifrare e decifrare un messaggio  $m$

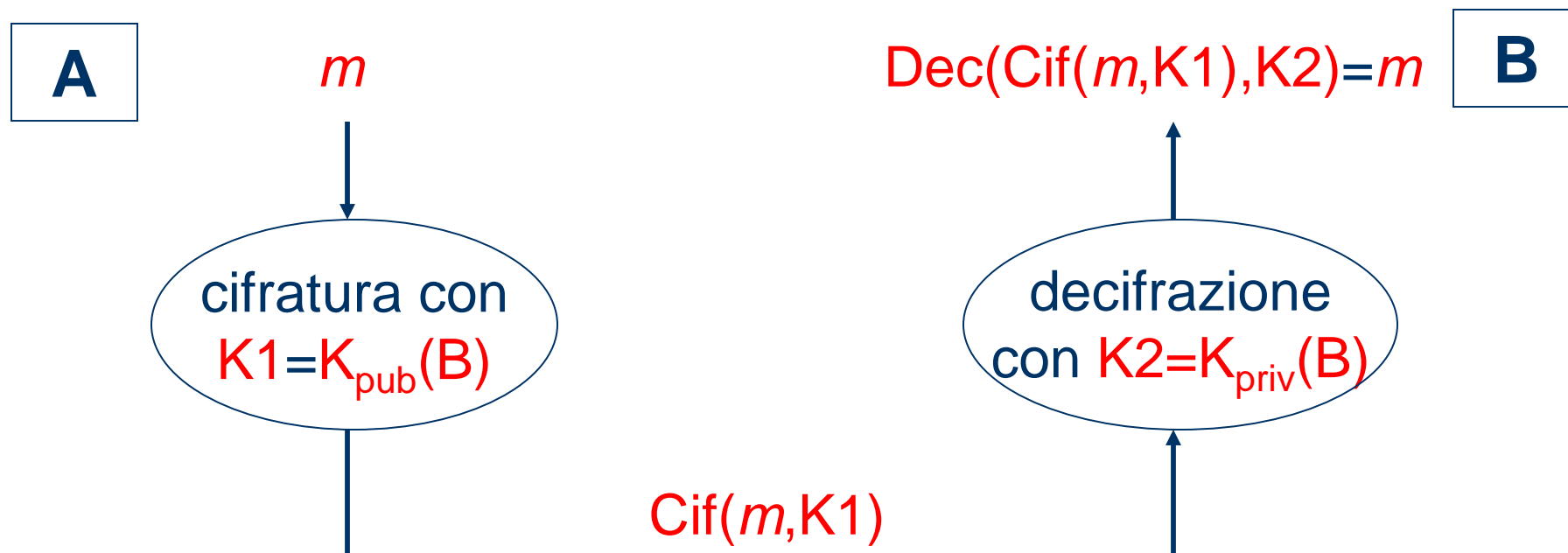


**Osservazione:** Privacy e authentication sono assicurate dalla segretezza della chiave

# Crittografia a Chiave Pubblica

Ogni soggetto  $S$  ha una propria *chiave pubblica*  $K_{\text{pub}}(S)$ , nota a tutti, e una propria *chiave privata*  $K_{\text{priv}}(S)$  nota solo a lui. I dati cifrati con una delle due chiavi possono essere decifrati SOLO con l'altra chiave.

### Implementazione della privacy:

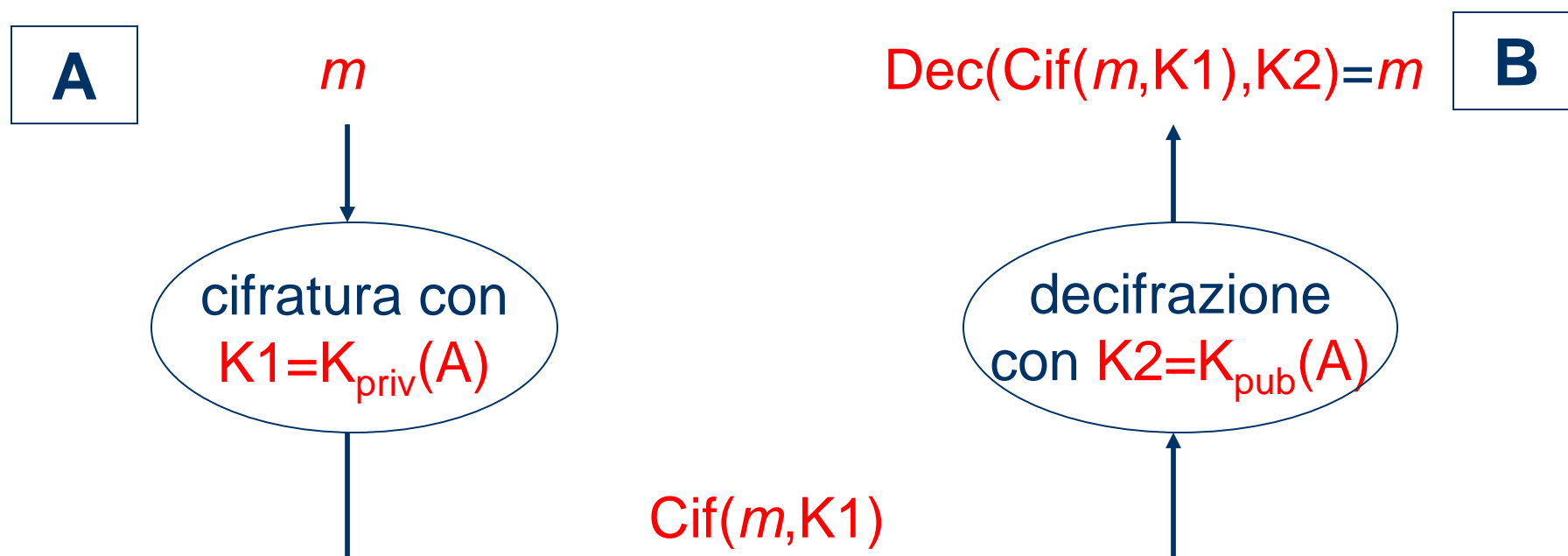


**Osservazione:** la privacy è assicurata in quanto *solo B* può determinare  $m$  da  $Cif(m, K1)$ .

**N.B.:** L'implementazione della privacy tramite crittografia a chiave pubblica è esposta ad attacchi di tipo *chosen plain-text* :

Se i possibili messaggi che A può inviare a B sono pochi e tutti noti a un intruso C, e se C conosce  $K_{pub}(B)$ , allora C può facilmente decifrare un messaggio inviato da A a B confrontando esaustivamente la sua codifica con le codifiche di tutti i messaggi inviabili da A a B.

### Implementazione dell'autentication:



**Osservazione:** l'autentication si realizza in quanto solo A può produrre  $\text{Cif}(m, K1)$ . In questo caso però non c'è privacy

### Sicurezza:

- Per decifrare un messaggio è necessario conoscere la chiave con la quale esso è stato cifrato (nel caso di crittografia a chiave segreta) o la chiave a abbinata alla chiave di cifratura (nel caso di crittografia a chiave pubblica)
- I metodi noti per i due tipi di crittografia basano la loro sicurezza sul fatto che per ricavare la chiave di decifrazione senza conoscerla *non si sa fare meglio* di una ricerca esaustiva tra tutte le possibili chiavi, il che richiederebbe un tempo di computazione troppo elevato ai fini pratici (milioni-miliardi di anni)



### Hashing

Una funzione hash è una one-way function che mappa una sequenza di bit  $s$  in una sequenza di bit  $h(s)$ , di solito molto più corta

Per garantire l'integrità di un messaggio  $m$  tramite l'uso di una funzione hash  $h$ , potenzialmente di dominio pubblico, si utilizzano due metodi

1. Insieme a  $m$  viene inviato  $h(m+k)$  dove “+” rappresenta l'operatore di concatenazione e  $k$  è una chiave segreta nota solo ai due soggetti che comunicano
2. Insieme a  $m$  viene inviata la cifratura di  $h(m)$  con la chiave privata del mittente

In entrambi i casi è difficile per un intruso modificare il messaggio  $m$  senza che il ricevente se ne accorga

# APPLICAZIONI

# FIRMA DIGITALE

Deve essere:

- Univocamente associata al firmatario
- Univocamente associata al documento firmato
  - Documento non alterabile
  - Firma non riutilizzabile
- Non falsificabile
- Non ripudiabile

## Applicazioni: firma digitale

---

Firma di un documento  $m$  da parte di un soggetto  $S$  e verifica da parte di un soggetto  $S' \neq S$ :

$K_{\text{priv}}(S), K_{\text{pub}}(S)$  = chiavi (pubblica e privata) di  $S$

$h$  = funzione hash

### Protocollo 1:

**Firma:**  $m \rightarrow \text{Cif}(m, K_{\text{priv}}(S))$

**Verifica:**  $\text{Dec}(\text{Cif}(m, K_{\text{priv}}(S)), K_{\text{pub}}(S)) \rightarrow m$

**Oss:** Intervenendo su  $\text{Cif}(m, K_{\text{priv}}(S))$  è possibile alterare il documento  $m$  senza che  $S'$  se ne accorga, a meno che non conosca a priori il contenuto di  $m$ .

### Protocollo 2:

**Firma:**  $m \rightarrow \text{Cif}(m, K_{\text{pub}}(S')) + \text{Cif}(h(m), K_{\text{priv}}(S))$

**Verifica:**  $\text{Dec}(\text{Cif}(m, K_{\text{pub}}(S')), K_{\text{priv}}(S')) \rightarrow m$

$h(m) = \text{Dec}(\text{Cif}(h(m), K_{\text{priv}}(S)), K_{\text{pub}}(S))$

**Oss.** E' il metodo più diffuso e garantisce anche la privacy

## Applicazioni: certificati

---

**CERTIFICATO:** Documento emesso da una **Certification Authority (CA)** che assegna una chiave pubblica a un certo soggetto. Il certificato è firmato (con firma digitale) dalla CA.

Es. Certificato per il soggetto **S** emesso dalla CA **A**:

$$m_A(S) = (A, S, K_{\text{pub}}(S), \text{periodo di validità})$$

$$\text{Cert}_A(S) = \text{Cif}(m_A(S), K_{\text{priv}}(A))$$

**Oss:** Conoscendo  $K_{\text{pub}}(A)$  si può accertare l'identità di **S** e acquisirne la chiave pubblica.

## Applicazioni: certificati

---

A volte è necessario fornire una sequenza di certificati per comunicare la propria chiave pubblica

Es. Comunicazione di  $K_{\text{pub}}(S)$

$$\text{Cert}_{A_1}(S) = \text{Cif}(m_{A_1}(S), K_{\text{priv}}(A_1))$$

$$\text{Cert}_{A_2}(A_1) = \text{Cif}(m_{A_2}(A_1), K_{\text{priv}}(A_2))$$

...

...

...

$$\text{Cert}_{A_k}(A_{k-1}) = \text{Cif}(m_{A_k}(A_{k-1}), K_{\text{priv}}(A_k))$$

**Oss:** Conoscendo  $K_{\text{pub}}(A_k)$  e risalendo la catena di certificati si può accertare l'identità di  $S$  e acquisirne la chiave pubblica.

### Sicurezza a livello del protocollo IP

**IPSec:** insiemi di protocolli che forniscono diversi servizi di sicurezza (ad es. privacy, authentication) alle comunicazioni IP. Può essere visto come un'alternativa all'implementazione dei requisiti di sicurezza a livello più alto



## Applicazioni: SSL

---

**Secure Socket Layer (SSL):** Protocollo inserito tra il livello application e il livello transport che aggiunge

- Privacy
- Authentication
- Message integrity



ai servizi offerti dal livello transport

**Esempio: HTTPS (Secure HTTP):** combinazione dei protocolli HTTP e SSL

## Applicazioni: SSL

---

Comunicazione sicura tra un client C e un server S tramite il protocollo SSL:

- C si accorda con S sugli algoritmi di crittografia da usare
- S invia a C il proprio certificato
- C verifica la corretta identità di S, ottiene  $K_{pub}(S)$ , e invia a S un pre-master secret cifrato con  $K_{pub}(S)$
- C ed S costruiscono, a partire dal pre-master secret:
  - Chiave segreta K1 da utilizzare per l'algoritmo a chiave segreta (ad es. DES)
  - Chiave K2 da utilizzare insieme alla funzione hash

## Applicazioni: SSL

---

Invio di un messaggio  $m$  previsto dal protocollo applicativo (es. HTTP):

- suddivisione di  $m$  in blocchi  $b_1, b_2, \dots$
- per ogni  $b_i$ :
  - $b_i \rightarrow \langle b_i, h(b_i + K_2) \rangle \rightarrow \text{Cif}(\langle b_i, h(b_i + K_2) \rangle, K_1)$
  - invio di  $\text{Cif}(\langle b_i, h(b_i + K_2) \rangle, K_1)$

Dove:

$h \equiv$  funzione hash scelta

### Virtual Private Network

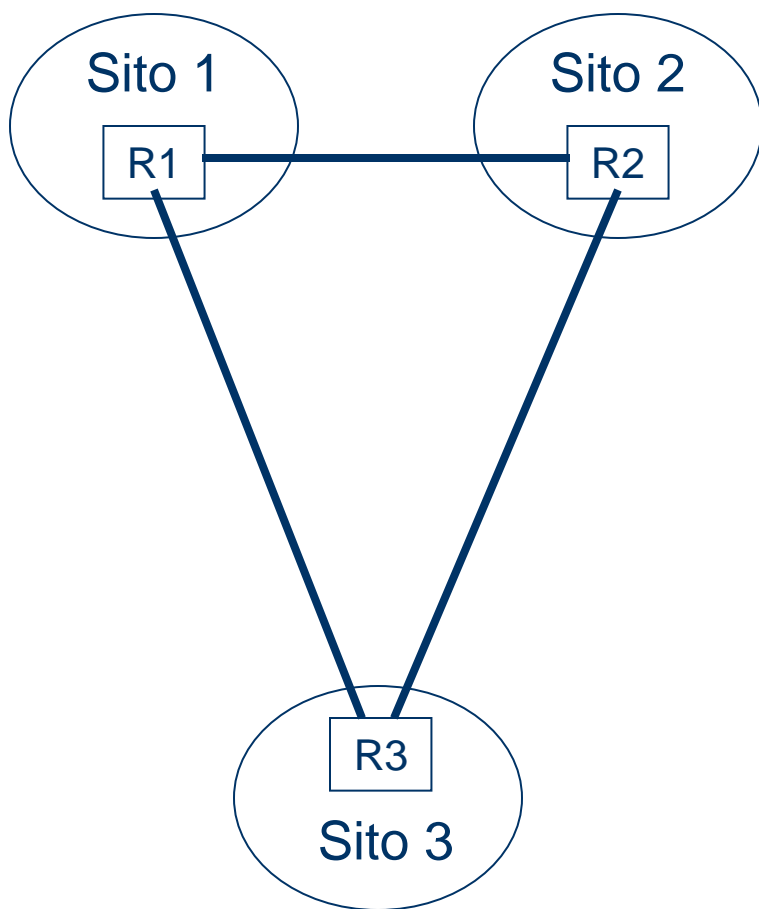
**Problema:** si vuole creare una intranet collegando reti fisiche dislocate su siti diversi (ad es. le sedi di una stessa azienda)

#### Opzioni:

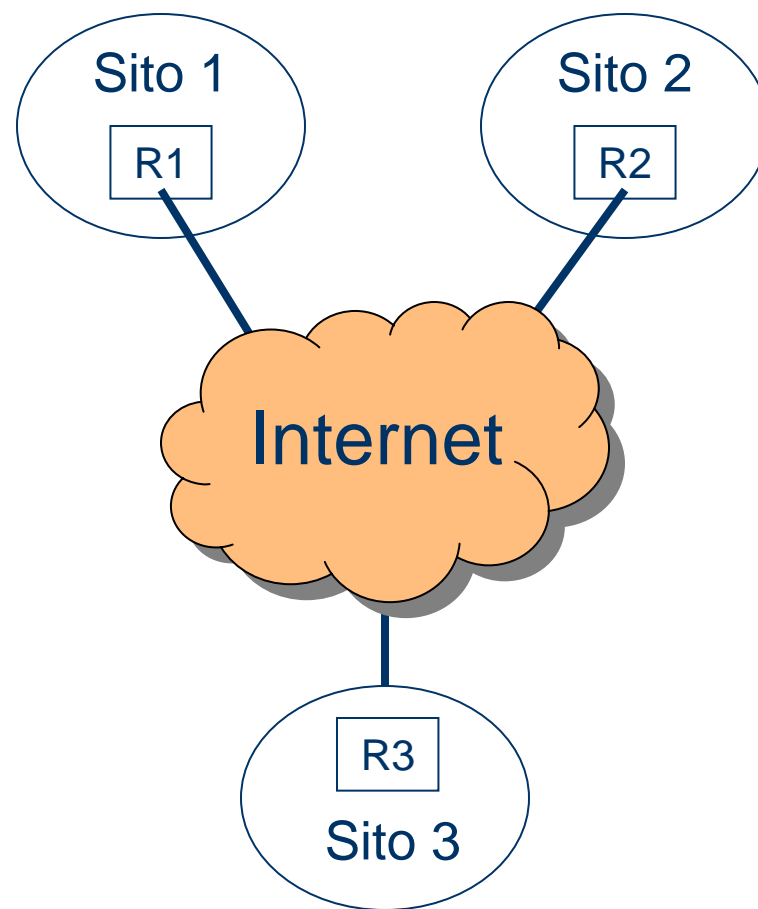
1. Utilizzo di link point-to-point privati (e.g., CDA, CDN) tra i vari siti
2. Creazione di una intranet virtuale (**Virtual Private Network o VPN**) che poggia su Internet

## Applicazioni: VPN

---



Opzione 1



Opzione 2

### Implementazione di una VPN (opzione 2)

- Ogni sito è collegato a Internet tramite un router (VPN router) sul quale gira un software speciale che implementa la VPN a livello IP
- Un VPN router filtra i pacchetti IP e garantisce che tutti i pacchetti in ingresso o in uscita provengano da o siano diretti a un altro VPN router
- La sicurezza è assicurata dall'uso di tecnologie come IPSec
- In questo modo la VPN è di fatto chiusa rispetto a Internet, ma la utilizza per fornire connettività tra i diversi siti, con un risparmio notevole rispetto all'uso di link point-to-point dedicati

## Applicazioni: VPN

---

### Invio di un pacchetto IP $p$ da un host A appartenente al sito i a un host B appartenente al sito j:

- $p$  è inviato da A al VPN router  $R_i$  del sito i (impostato come router di default per tutte le comunicazioni esterne al sito i)
- (TUNNELING)  $R_i$  crea una copia cifrata di  $p$  e la inserisce come dato in un altro pacchetto IP  $q$  che invia al VPN router  $R_j$  del sito j
- $R_j$  riceve  $q$ , estrae e decifra  $p$ , e invia  $p$  a B

