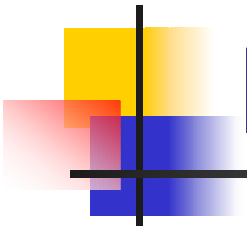
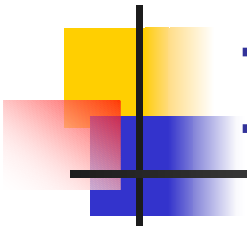


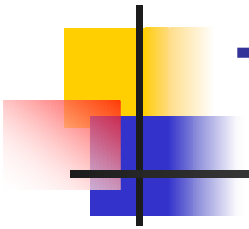
PGP

- PGP – Pretty Good Privacy
- di Bruno Quinzi



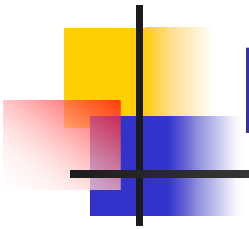
Introduzione

- Posta elettronica
- Lacune della rete
- Possibili attacchi da parte di un hacker



Tipologie di attacco

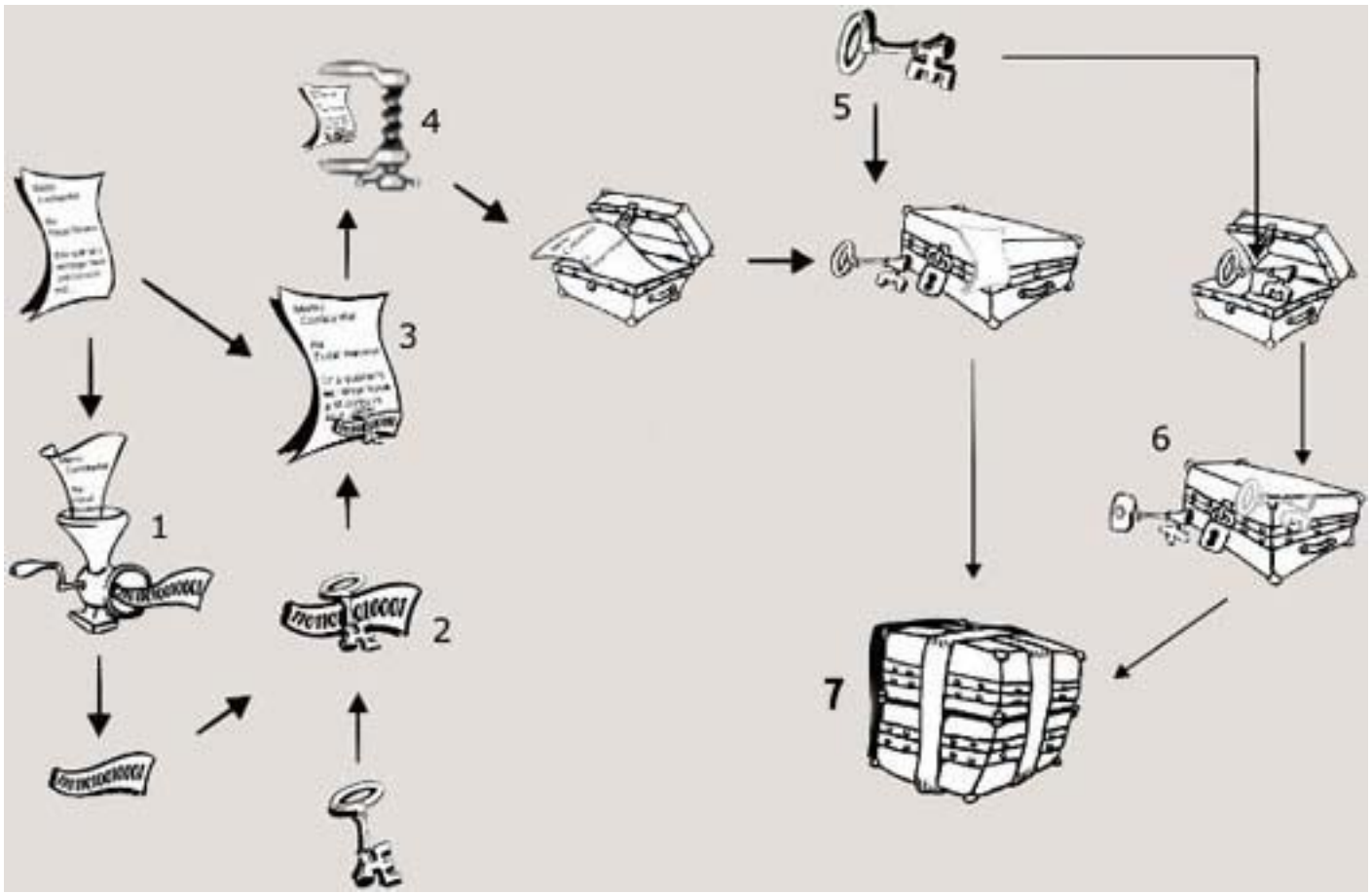
- Attacchi ATTIVI
  - Interruzione
  - Modifica
  - Inserimento
- Attacchi Passivi
  - Intercettazione



PGP – Pretty Good Privacy

- Phil Zimmermann
- Problemi per la sua diffusione
- Senate Bill 266 del 1991

Come funziona (invio)



1.Message Digest

Message Digest

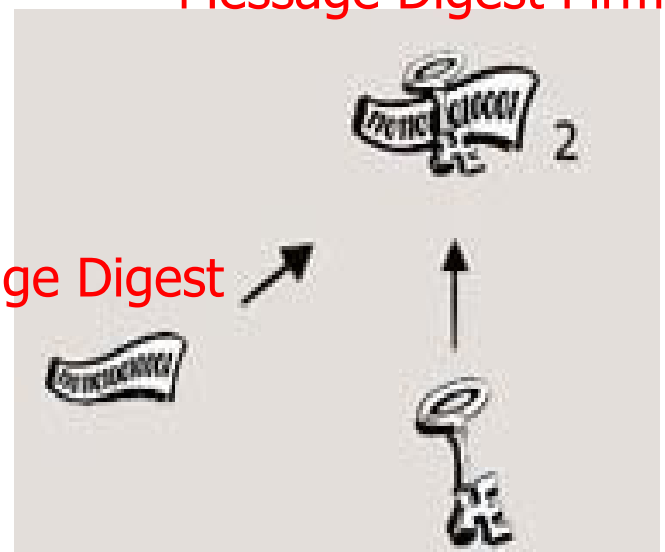
Rappresentazione del messaggio che vogliamo inviare, di lunghezza univoca (128 bit).
Serve ogni qual volta è richiesta la firma del messaggio

MD5

Algoritmo che prende come input un testo di lunghezza arbitraria e applicandogli una funzione hash rimanda come output un Message digest a 128 bit

2.Firma del mittente

Message Digest Firmato



Message Digest

Chiave privata mittente

Message Digest Firmato

AUTENTICAZIONE

Garantisce l'identità dei partecipanti coinvolti

il digest viene codificato con la chiave privata di chi produce il messaggio in modo che il ricevente può stabilire la fonte del testo

3.Firma del messaggio

Messaggio Firmato

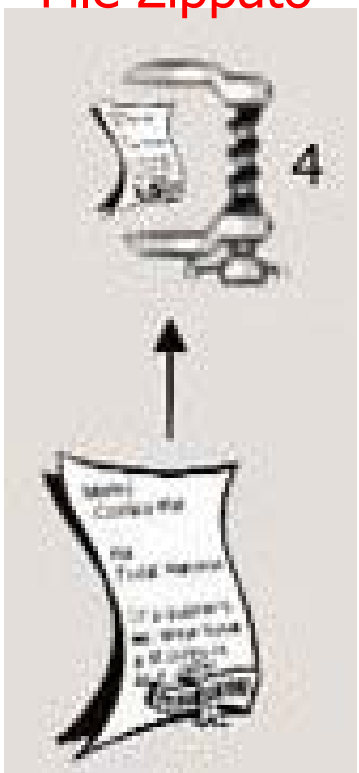
Testo in chiaro

Message Digest Firmato

Il Digest Firmato viene applicato al messaggio in chiaro

4.Compressione

File Zippato



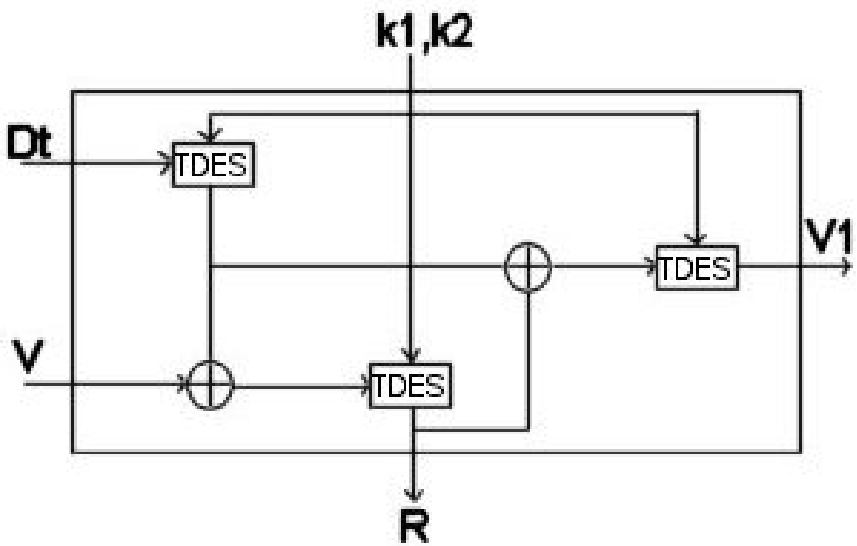
Messaggio Firmato

File Compresso

COMPRESSIONE
Viene utilizzato lo standard commerciale
Zip che garantisce buone prestazioni
dell' intero sistema e rendendo la
Crittoanalisi più difficile visto che un messaggio compresso
ha meno ridondanze di quello originario

Generazione Session Key

ANSI X9.17



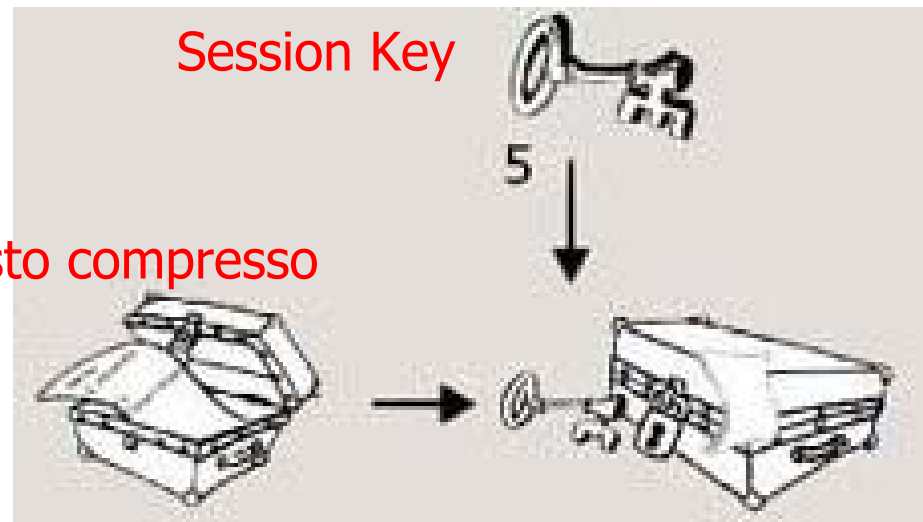
Session Key

Con l'utilizzo dell'ANSI X9.17 otteniamo la chiave con cui cifrare il nostro messaggio al prossimo passaggio

ANSI X9.17

Prende come input un valore seme, la data e l'ora in bit e due chiavi. Attraverso l'uso di 3 TDES combinati mediante l'or-esclusivo elabora questi dati e rimanda come output un valore seme da utilizzare al prossimo passaggio se servisse e la Session Key per cifrare il messaggio

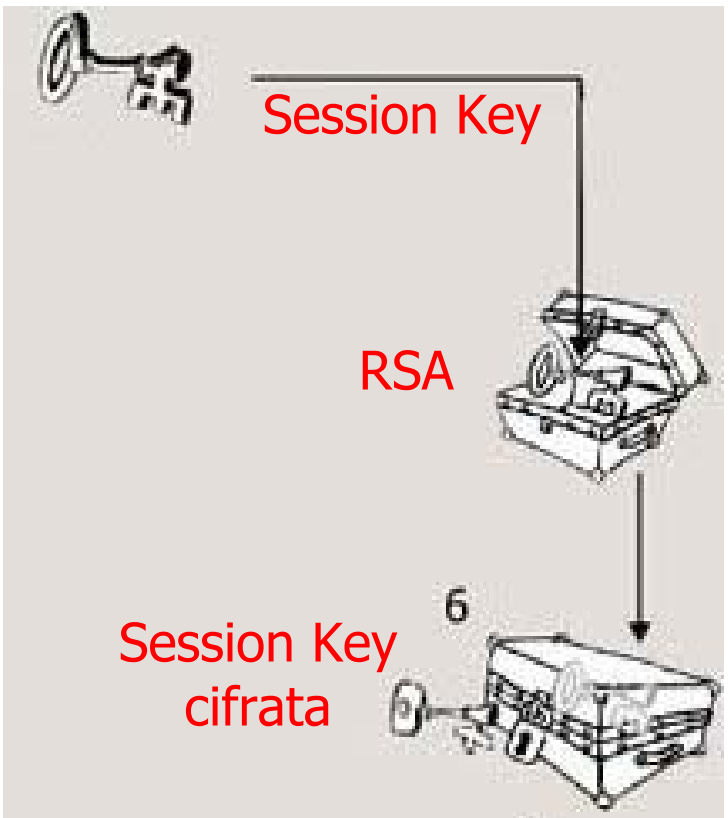
5.Cifratura del Testo



Algoritmo IDEA

Il testo viene cifrato mediante l'algoritmo simmetrico IDEA che utilizza una chiave a 128 bit, Session Key.
Un algoritmo molto difficile da attaccare

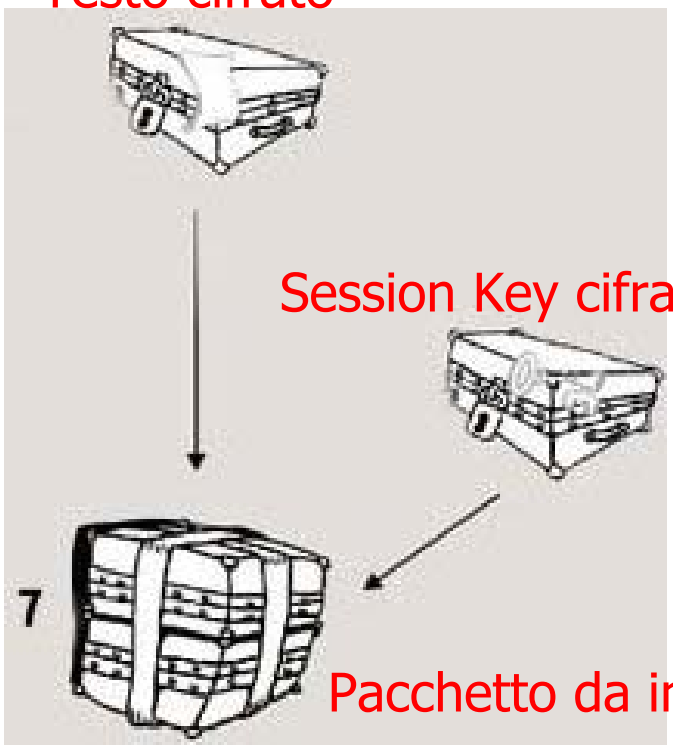
6.Cifratura della Session Key



RSA

Attraverso questo algoritmo asimmetrico viene cifrata la Session Key con l'utilizzo della chiave pubblica del destinatario. Una volta effettuato questo passaggio sarà impossibile anche per il mittente decifrare la Session Key.

7.Invio

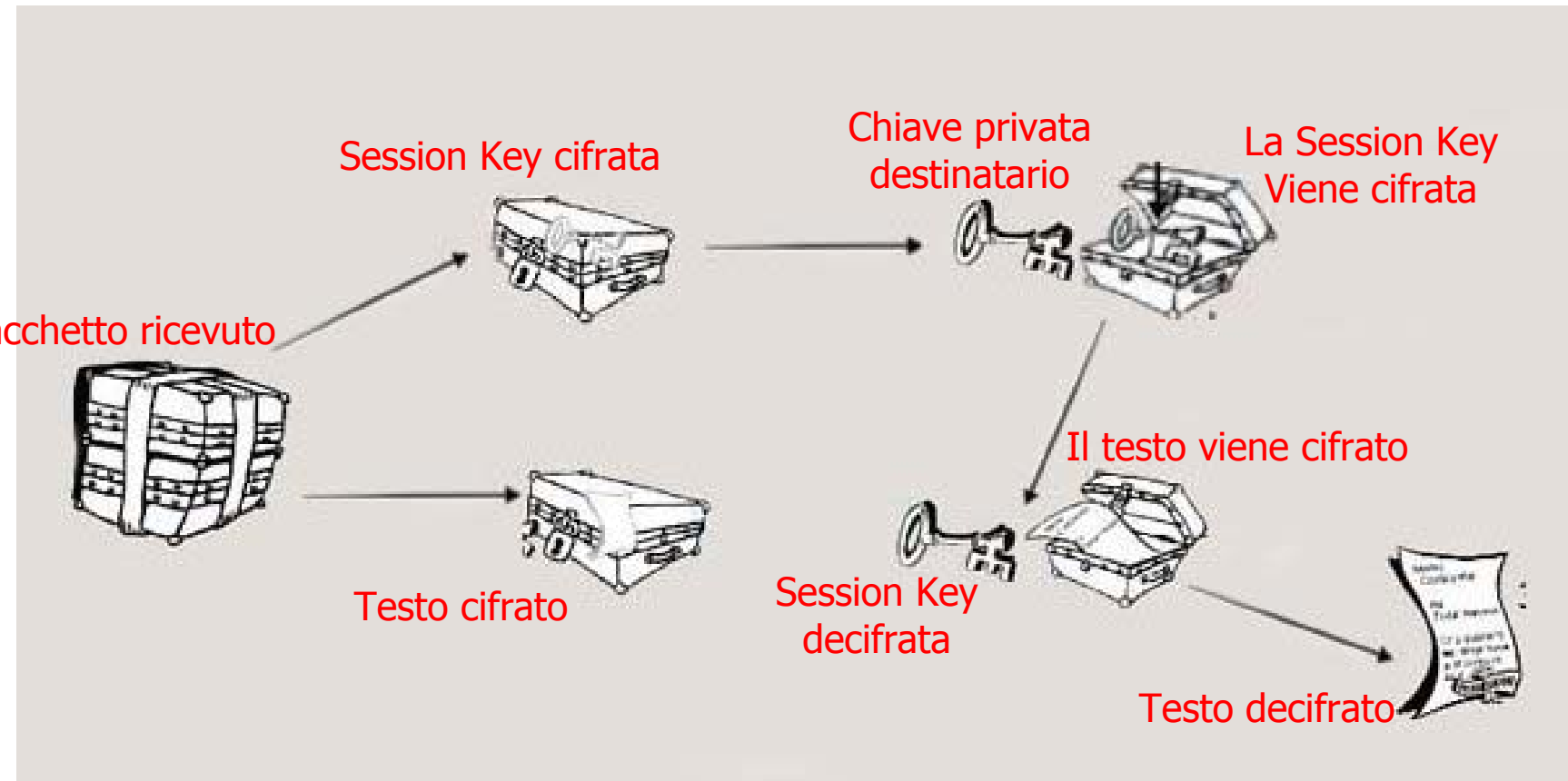


RADIX64

COMPATIBILITA'

Bisogna garantire la compatibilità con gli standard e per questo il messaggio binario viene convertito in una sequenza di caratteri ASCII. L'algoritmo prende 3 byte e li trasforma in 4 caratteri ASCII con un aumento delle dimensioni del 33%, un danno compensato dalla precedente compressione.

Come funziona (ricezione)



Algoritmi utilizzati dal PGP

- MD5
- ZIP
- TDES (TRIPLE DES) – nell'ANSI X9.17
- IDEA, RSA
- RADIX-64