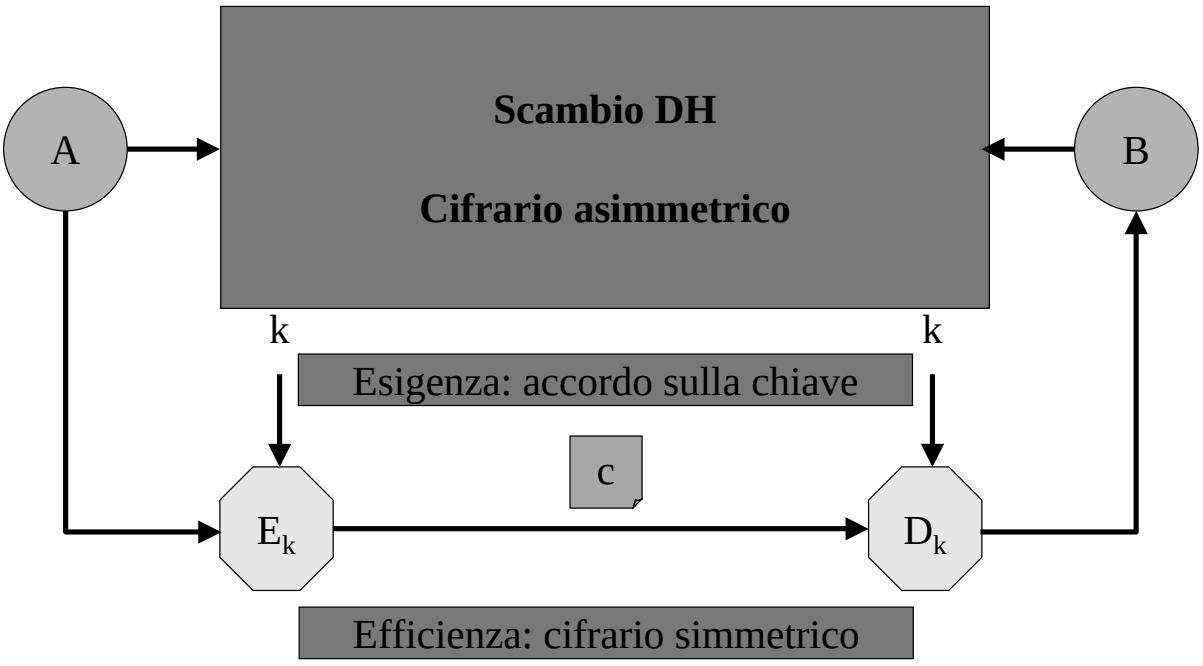
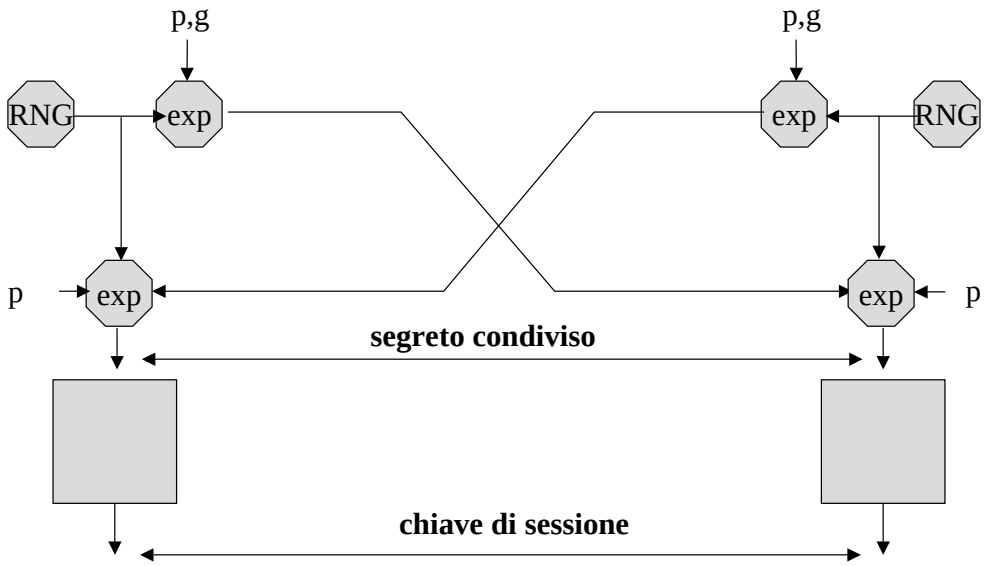
Le tecniche di key agreement

Key Agreement

Problema: A e B vogliono scambiarsi informazioni riservate in assenza di accordi segreti precedenti

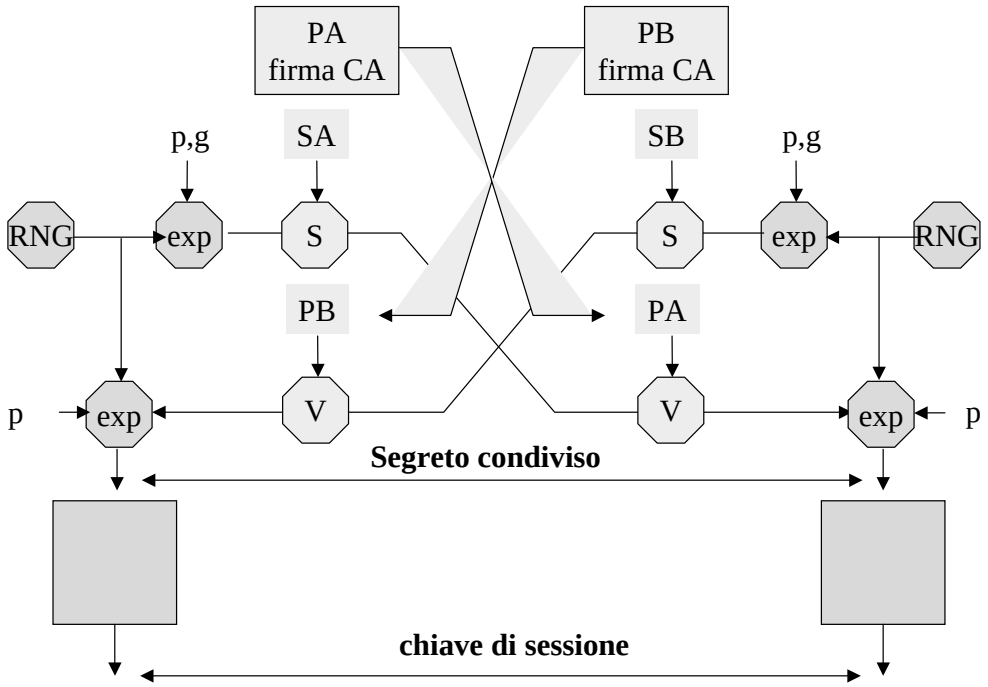


L’accordo sulla chiave: anonimous Diffie-Hellman (pag. 92)

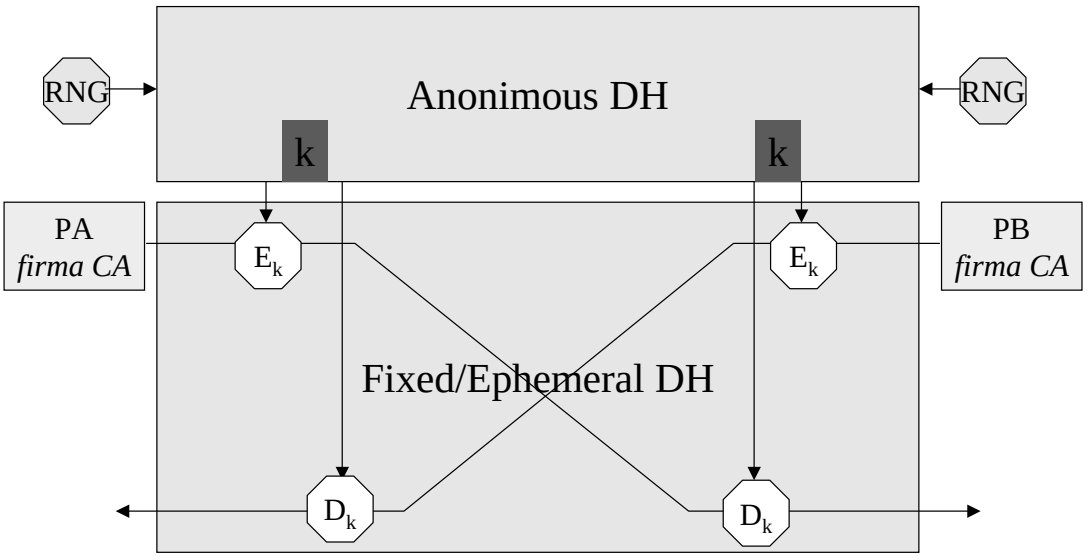


L’accordo sulla chiave: fixed Diffie-Hellman

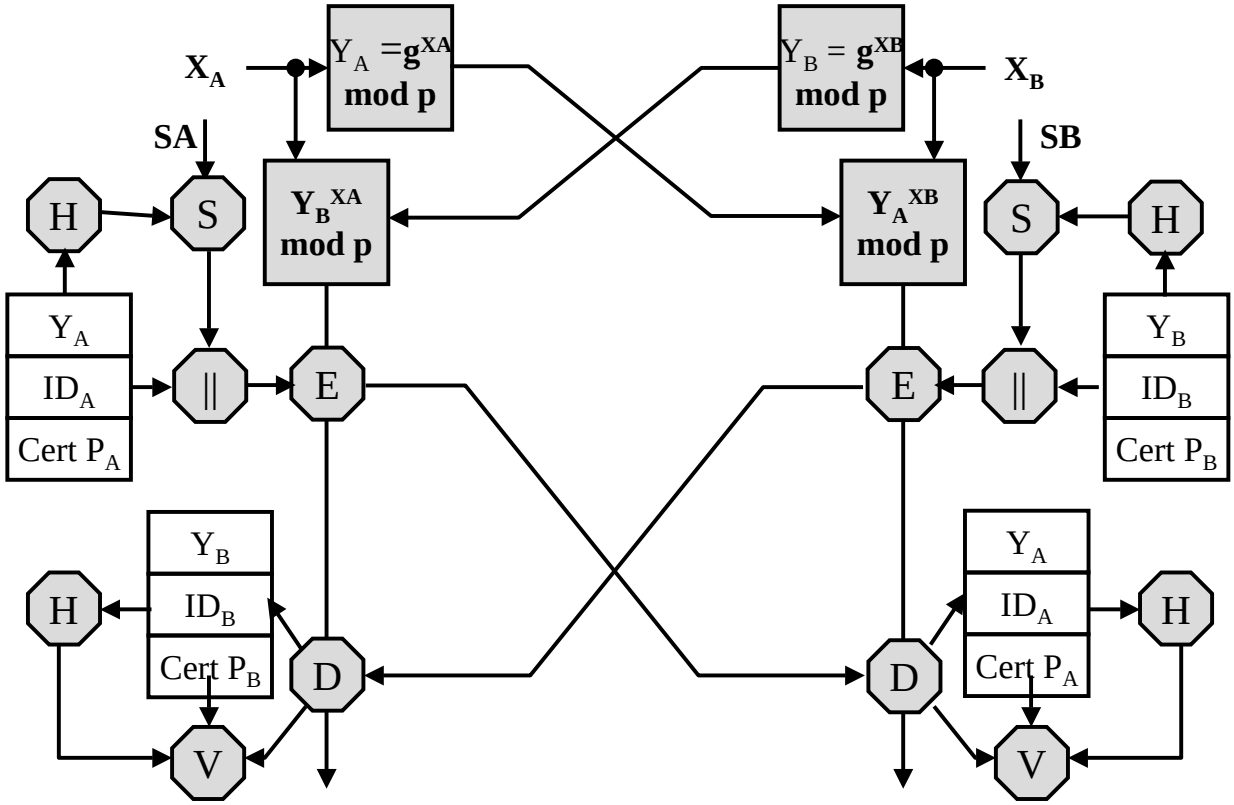
L'accordo sulla chiave: ephemeral Diffie-Hellman



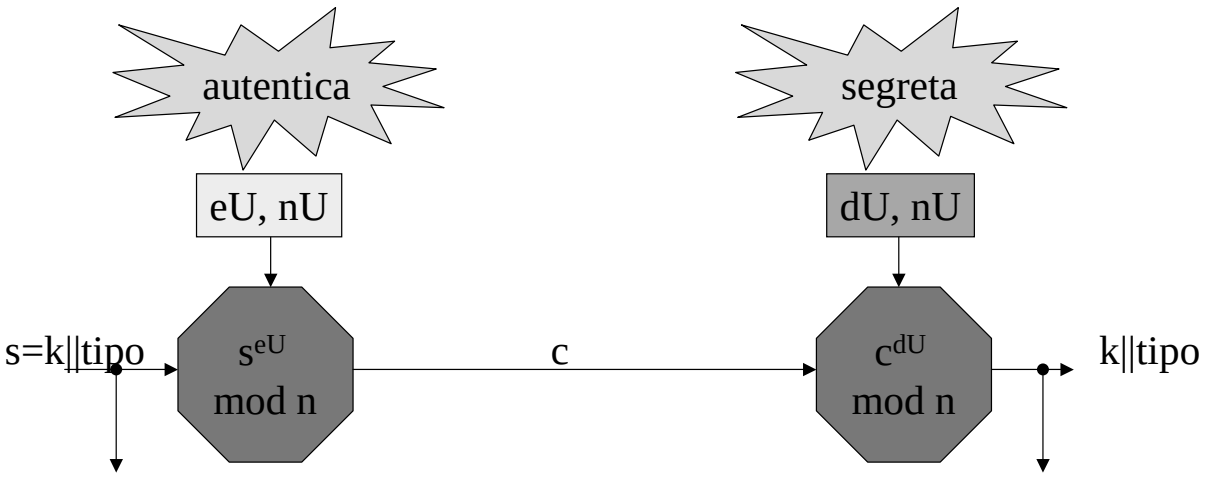
Accordo sul segreto e privacy: IKE (Internet Key Exchange)



IKE: anonimato ed identificazione



Chiave di sessione con RSA



Vulnerabilità: $s^{eU} < n$

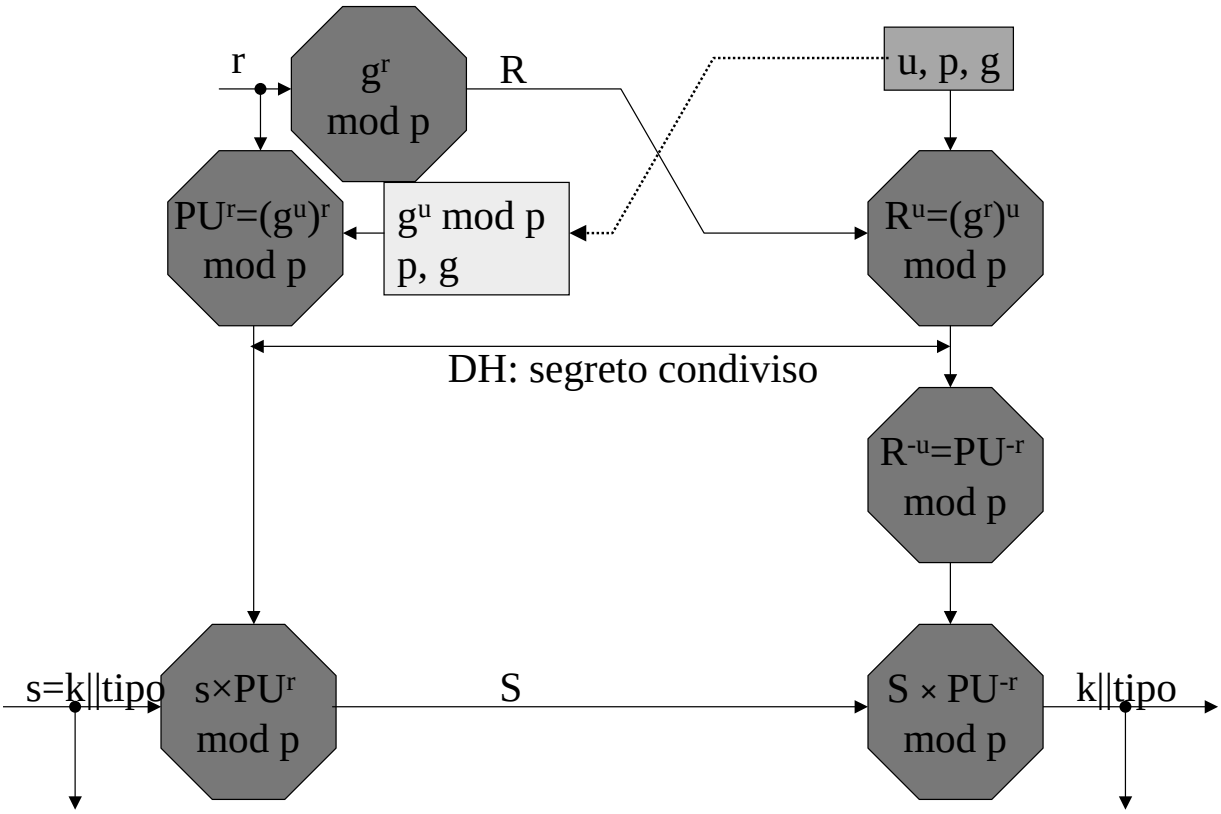
Contromisura

1: A sceglie a caso un R “grande”

2: A cifra R

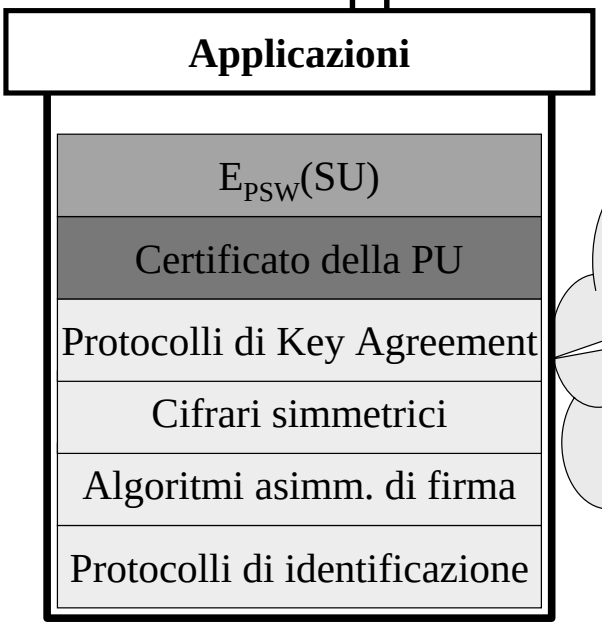
3: A e B impiegano k = H(R)

Chiave di sessione con ElGamal

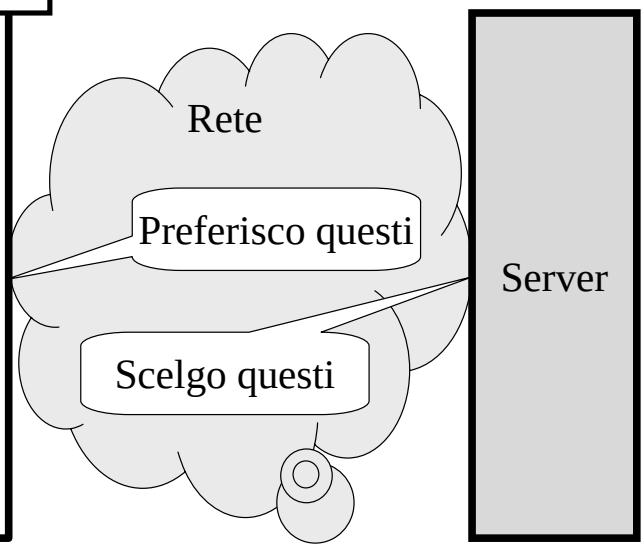


Il protocollo SSL

Servizi di sicurezza condivisi dalle applicazioni di un browser

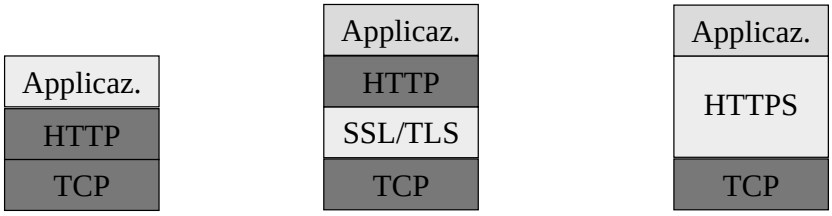


Browser: zainetto da viaggio

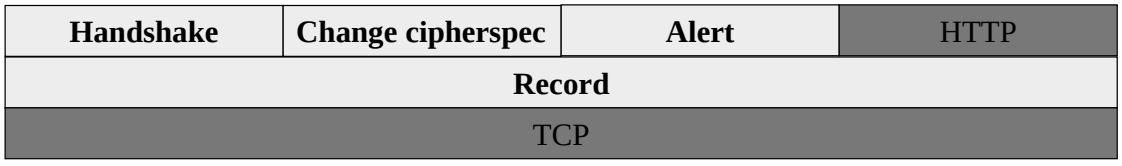


La negoziazione

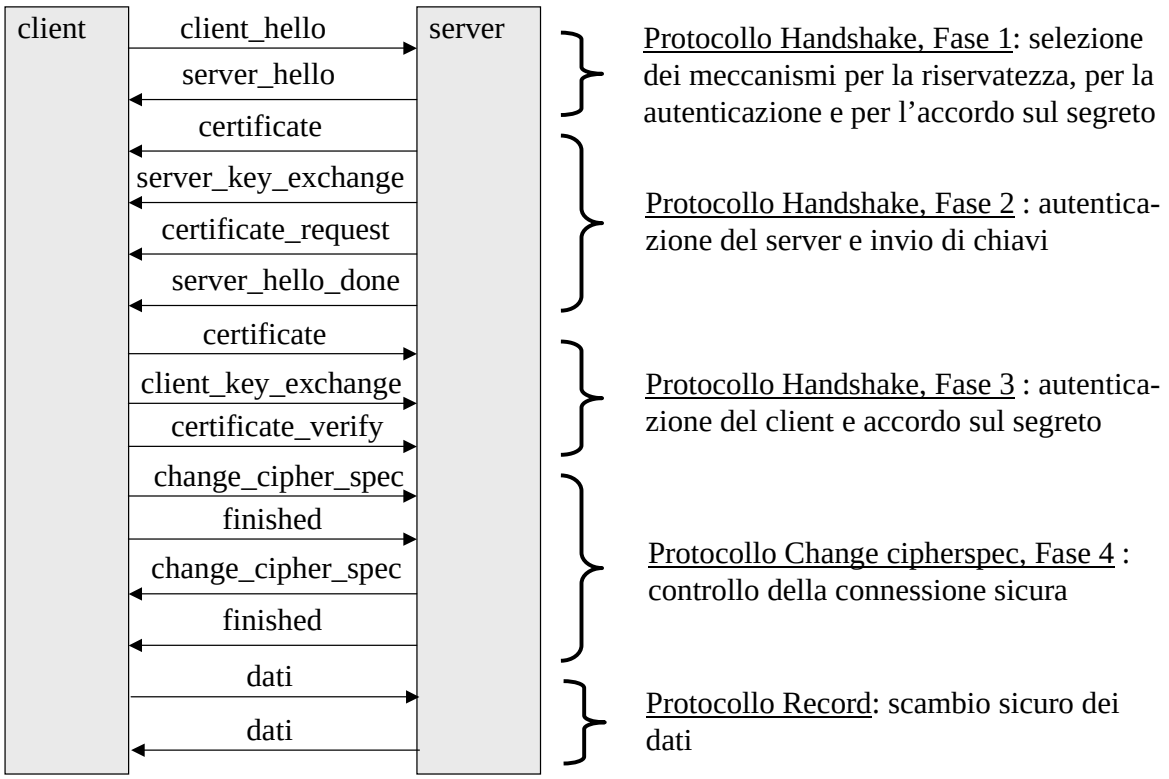
Secure socket layer (SSL) (pag.122) Transport layer security (TLS)

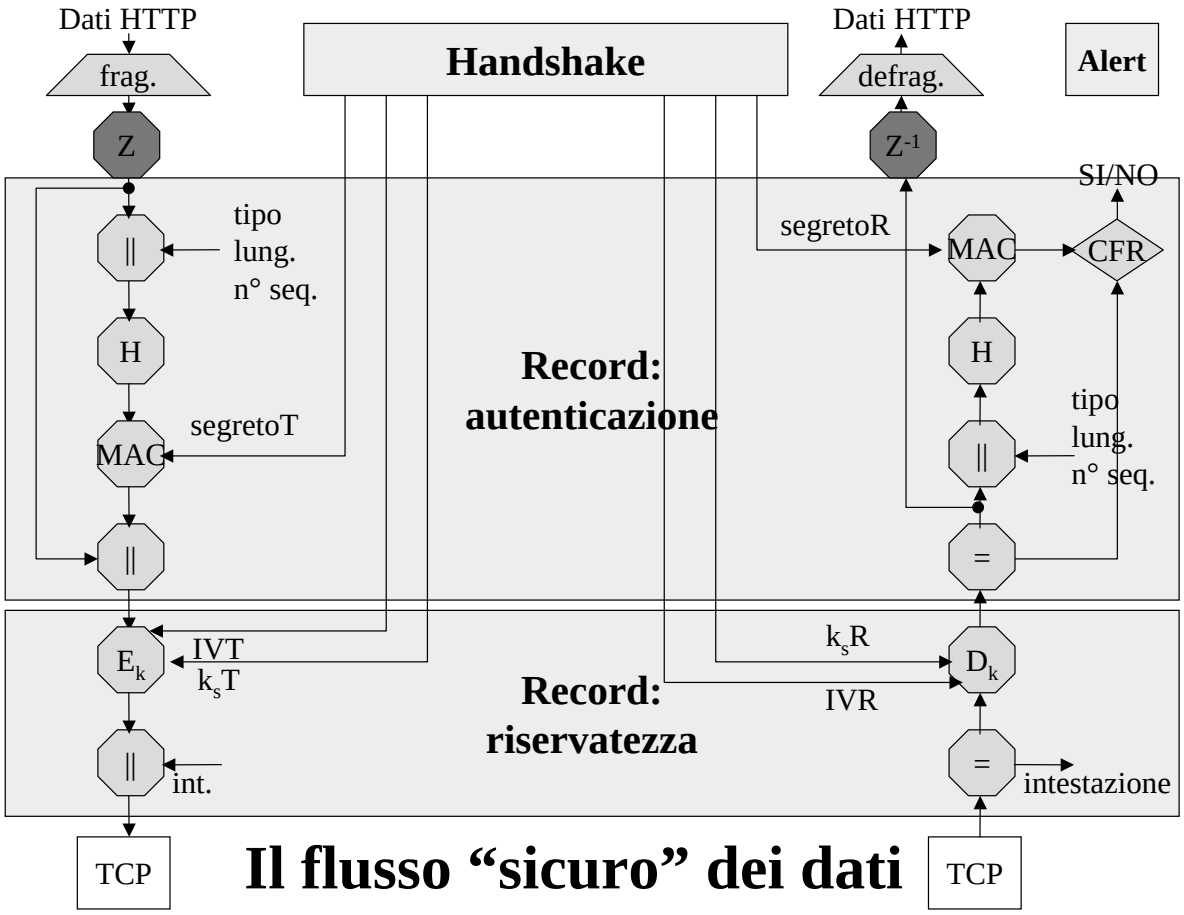


SSL: Netscape
TLS:RFC 2246



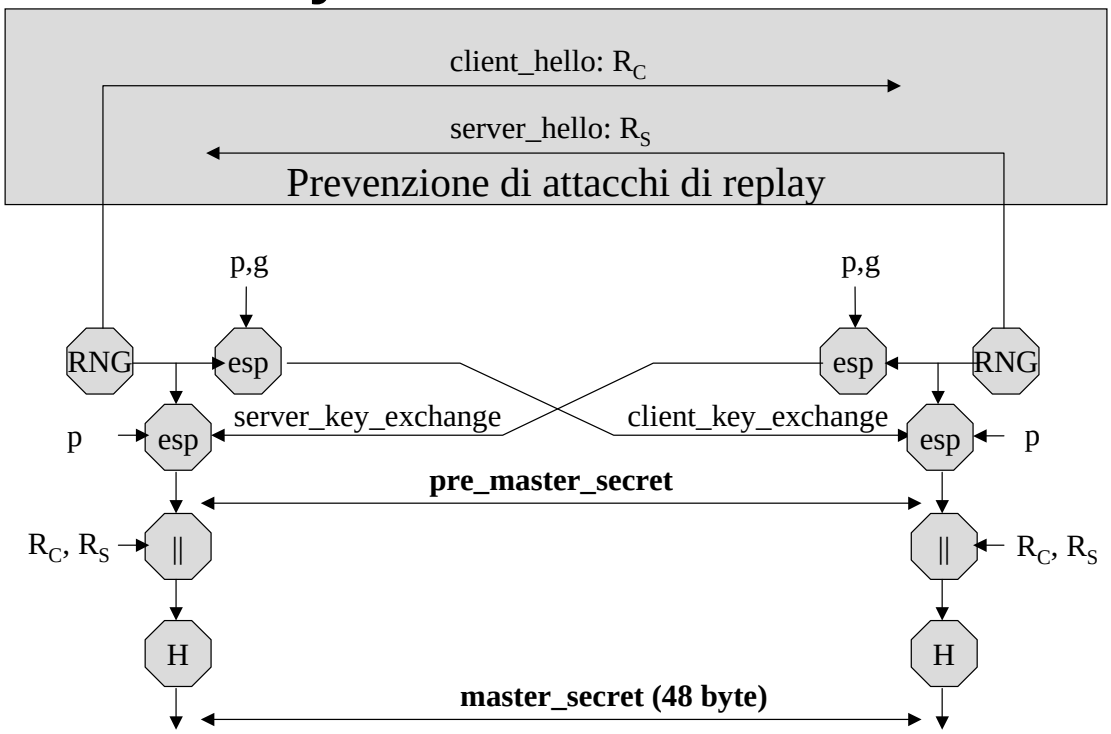
I protocolli Handshake e Record



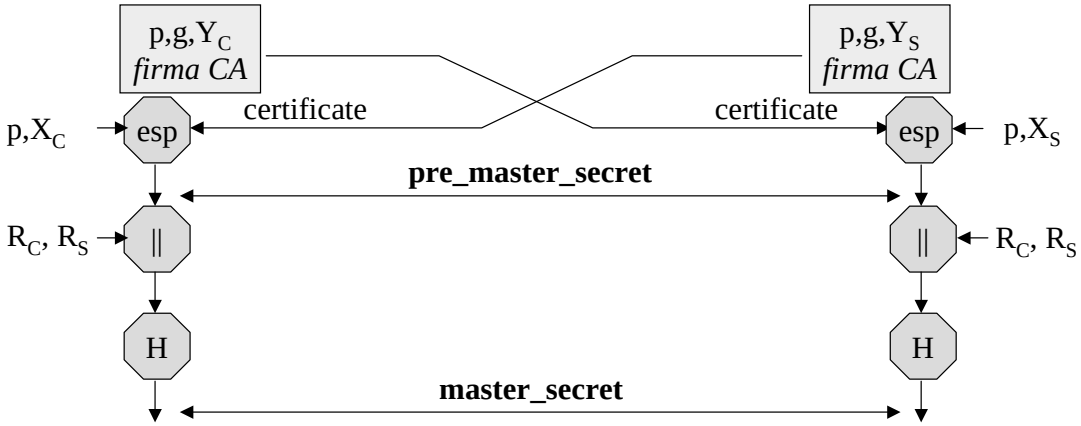


Il flusso "sicuro" dei dati

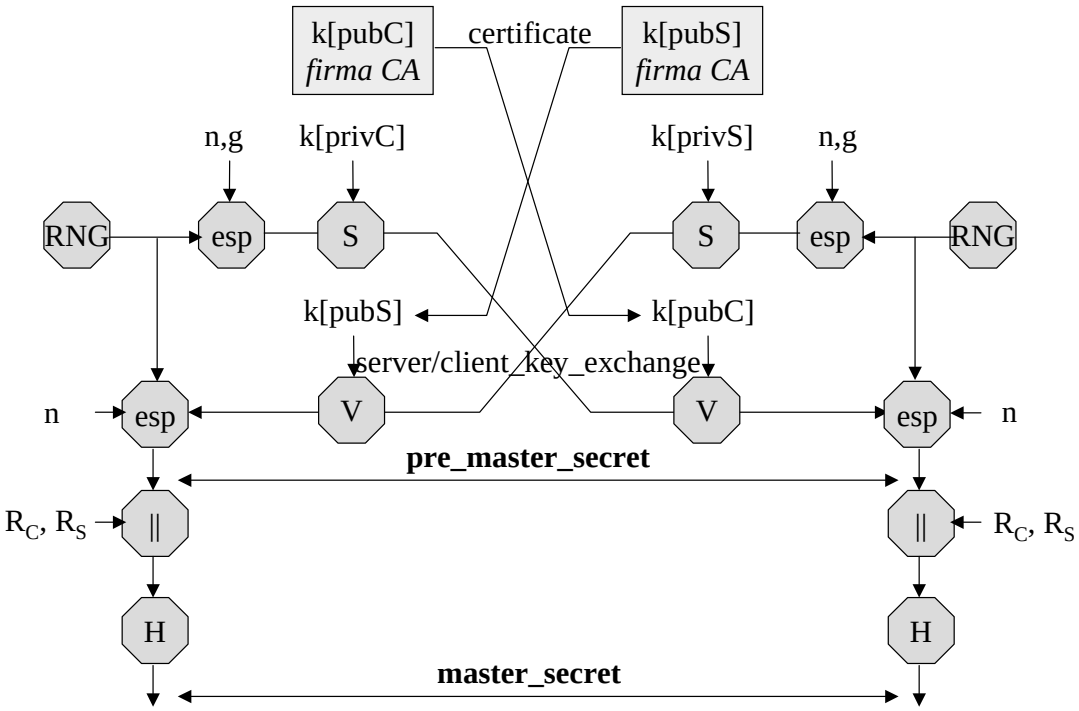
L’accordo sul segreto: anonymous Diffie-Hellman



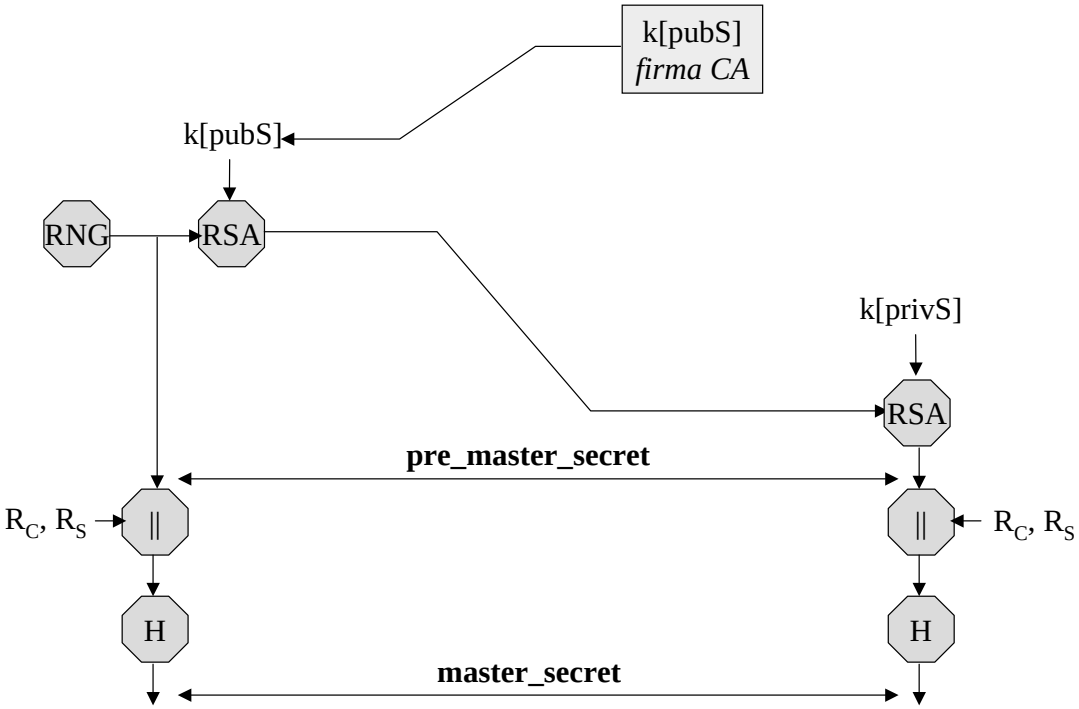
L’accordo sul segreto: fixed Diffie-Hellman



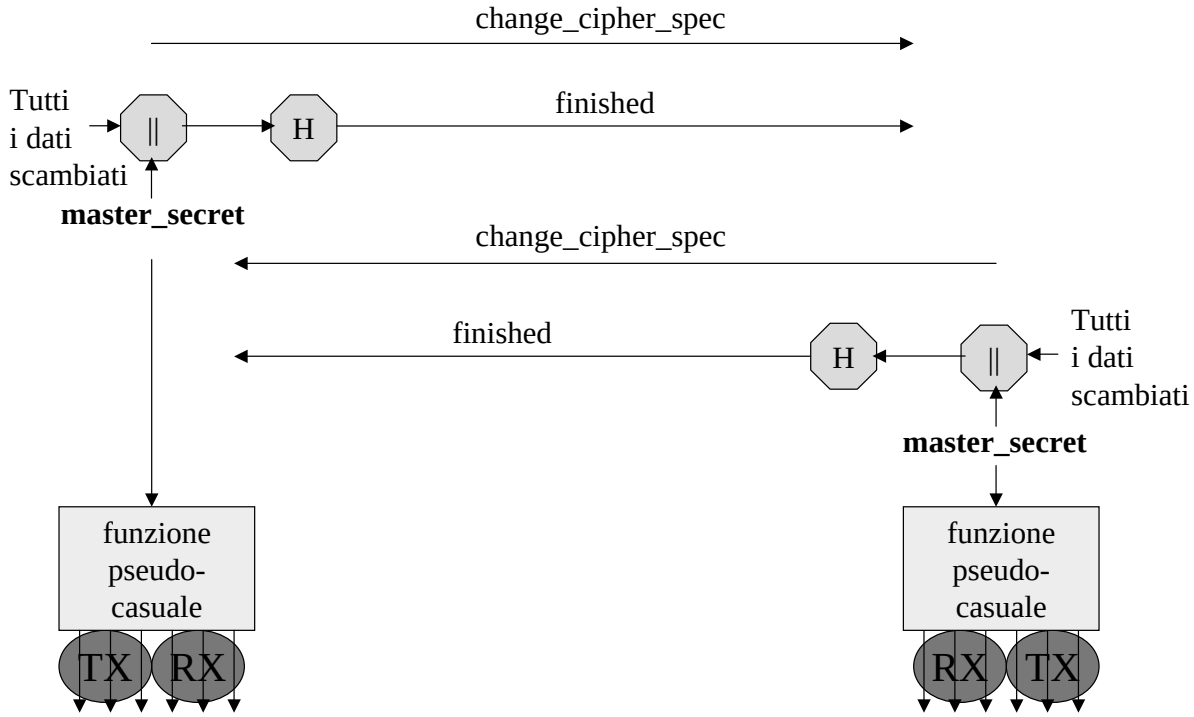
L’accordo sul segreto: ephemeral Diffie-Hellman



L’accordo sul segreto: cifratura asimmetrica



La verifica del segreto e la generazione delle chiavi



Il servizio PGP

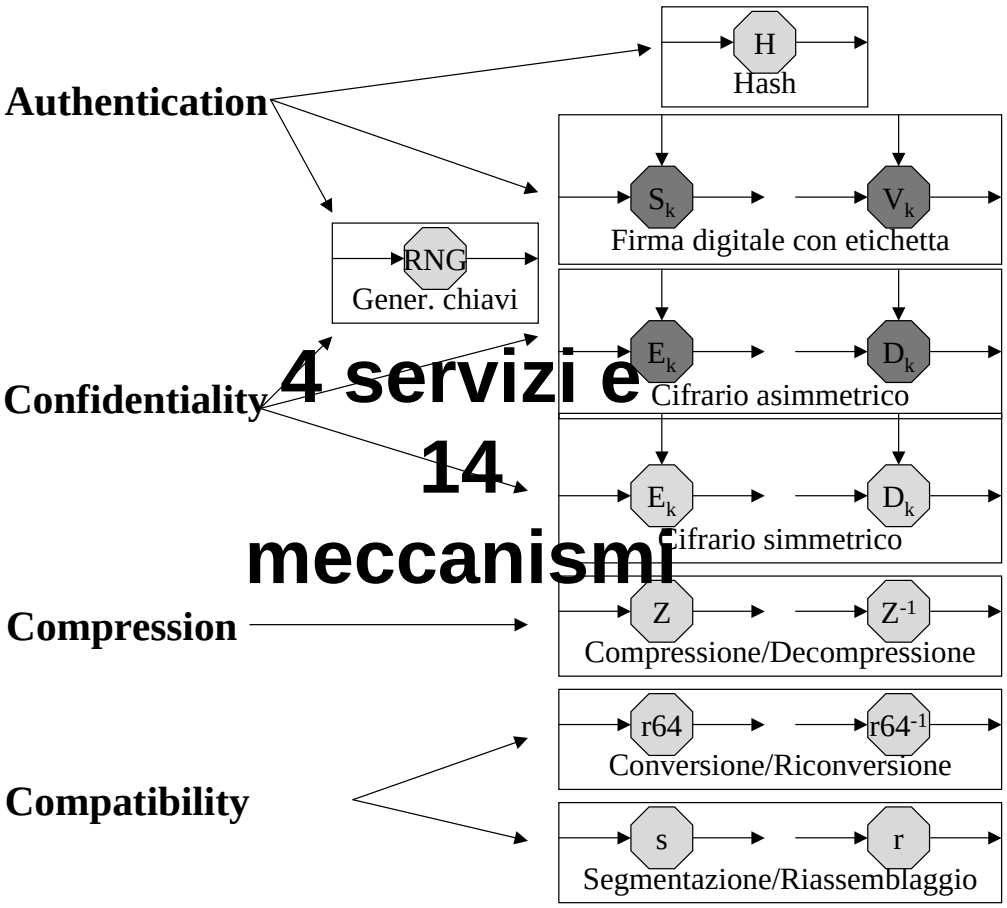
Pretty Good Privacy (pag.117)

- Philip R. Zimmerman is the creator of PGP (1993).

PGP provides
a **confidentiality** and **authentication** service
that can be used for
electronic mail and **file storage** applications.

Confidentiality: the act of keeping something private and secret from all but those who are authorized to see it.

Authentication: to prove genuine by corroboration of the identity of an entity.

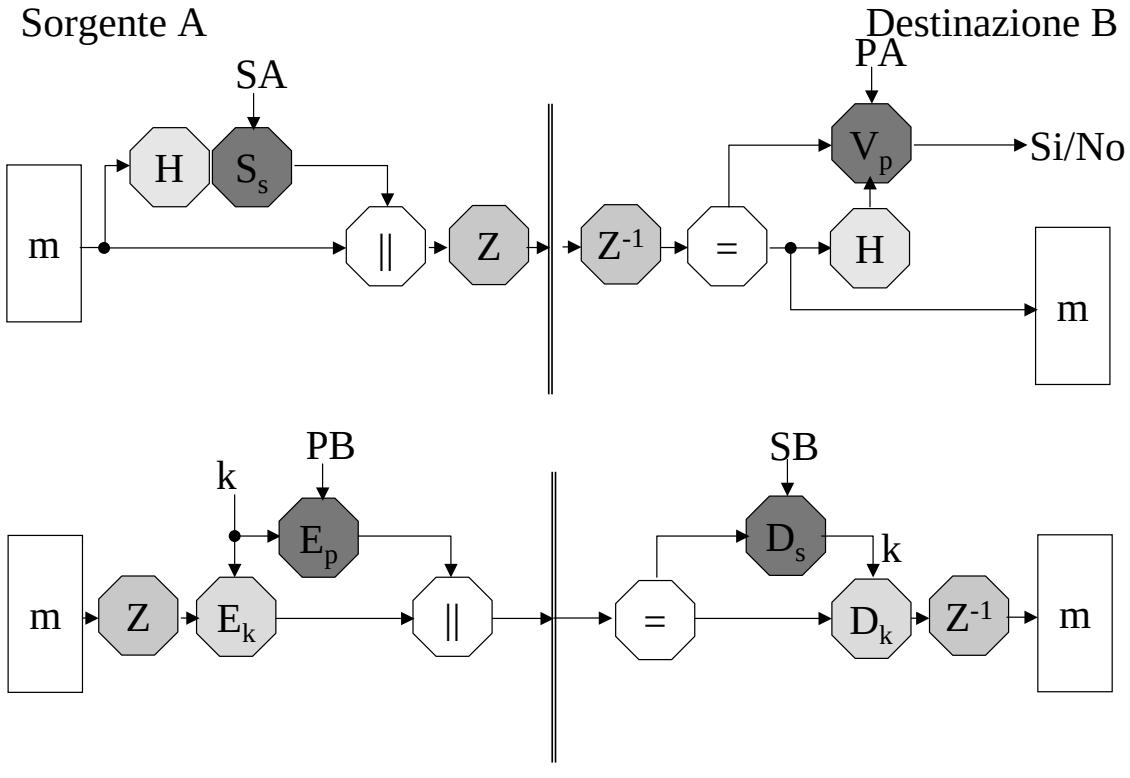


4 servizi e 14 meccanismi

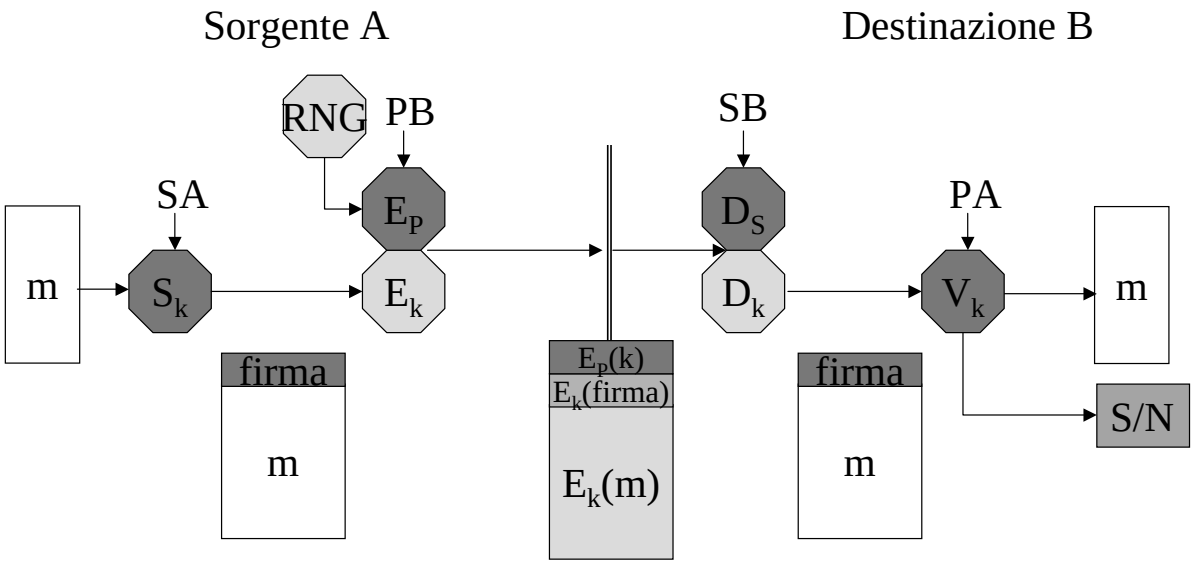
Summary of PGP Services

Function	Algorithm Used
Digital Signature	DSS/SHA or RSA/SHA
Message Encryption	CAST or IDEA or three-key triple DES with Diffie-Hellman or RSA
Compression	ZIP
E-mail Compatibility	Radix-64 conversion
Segmentation	

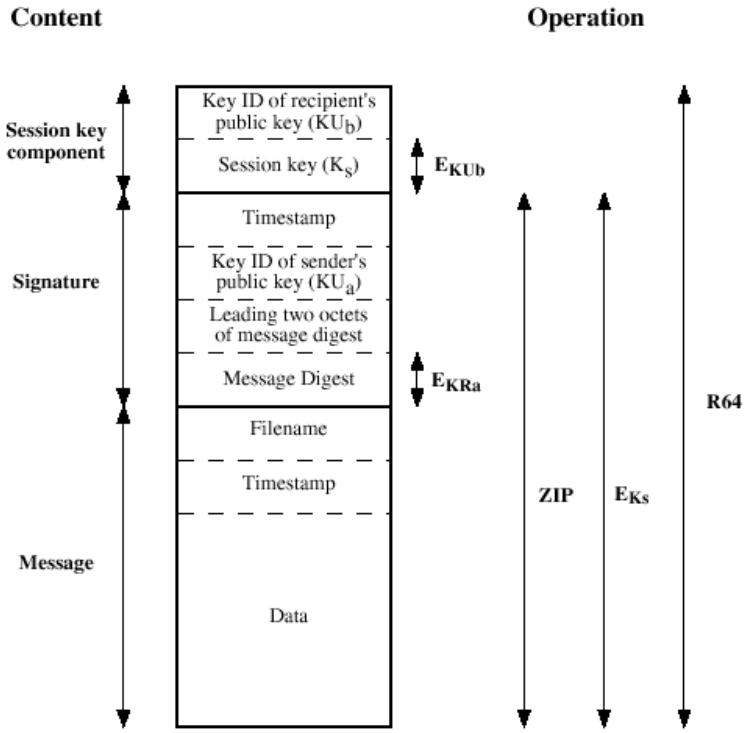
PGP: autenticazione o riservatezza

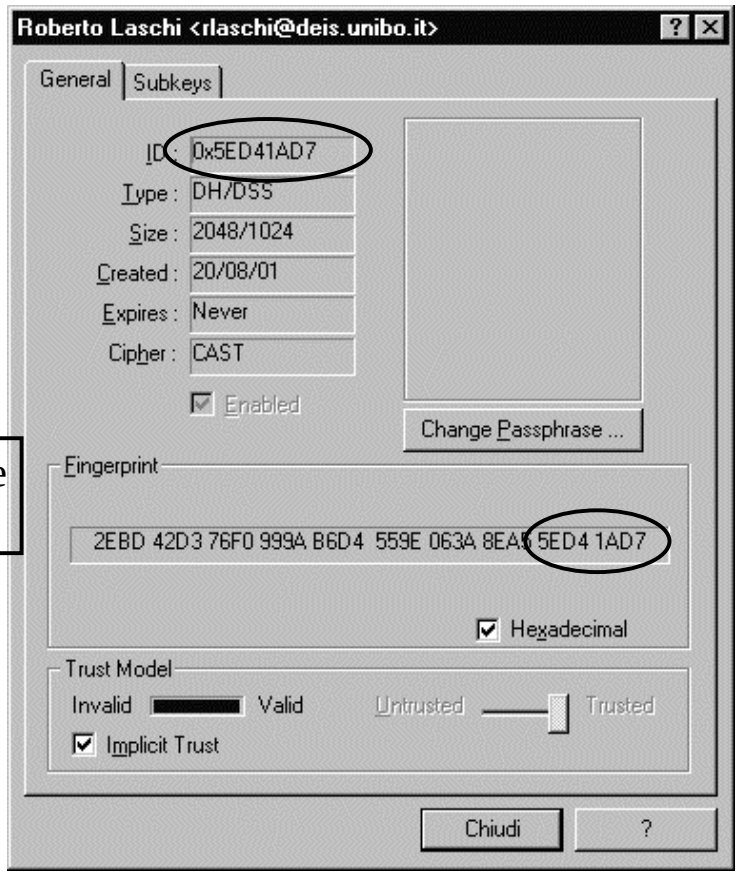


PGP: autenticazione & riservatezza



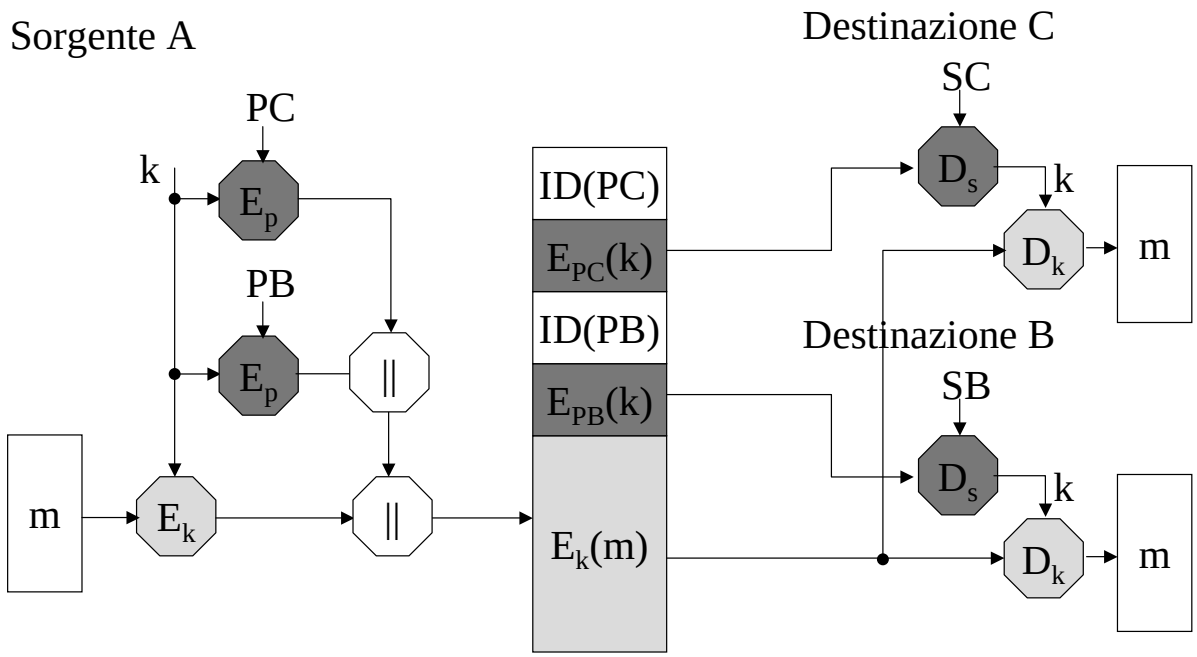
Format of PGP Message



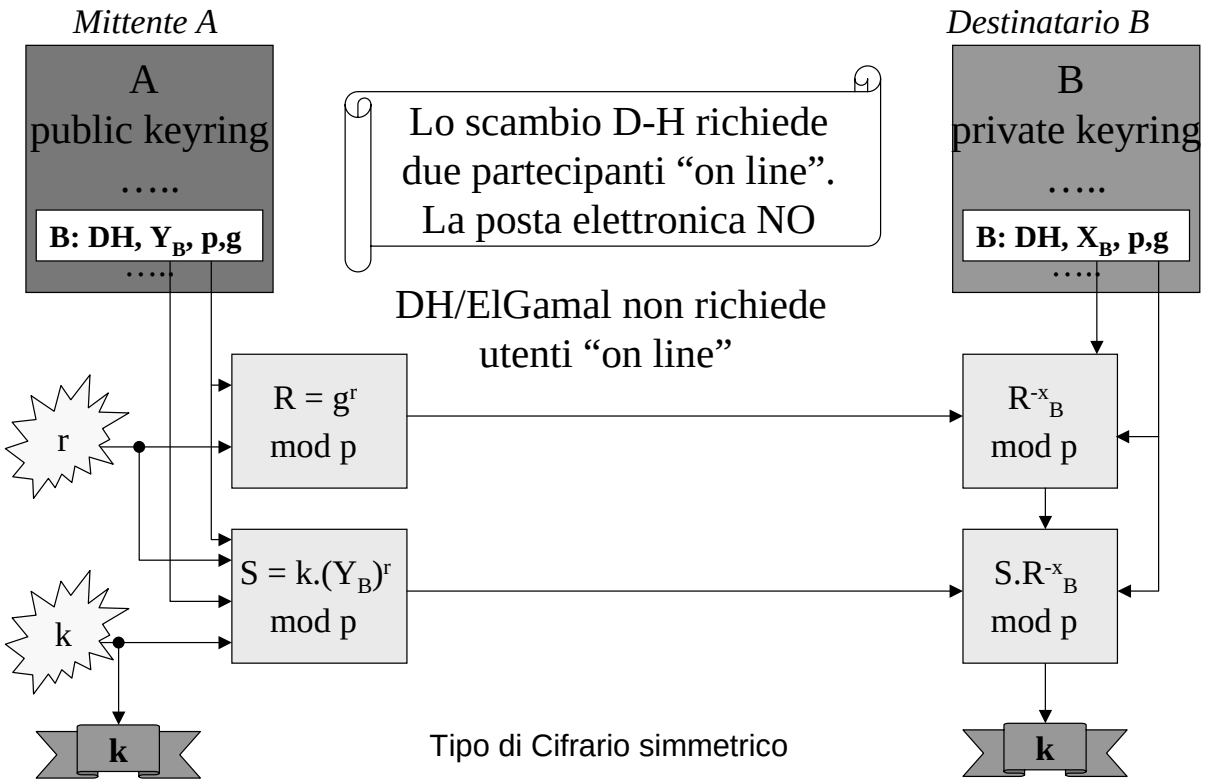


Identificatore di chiave

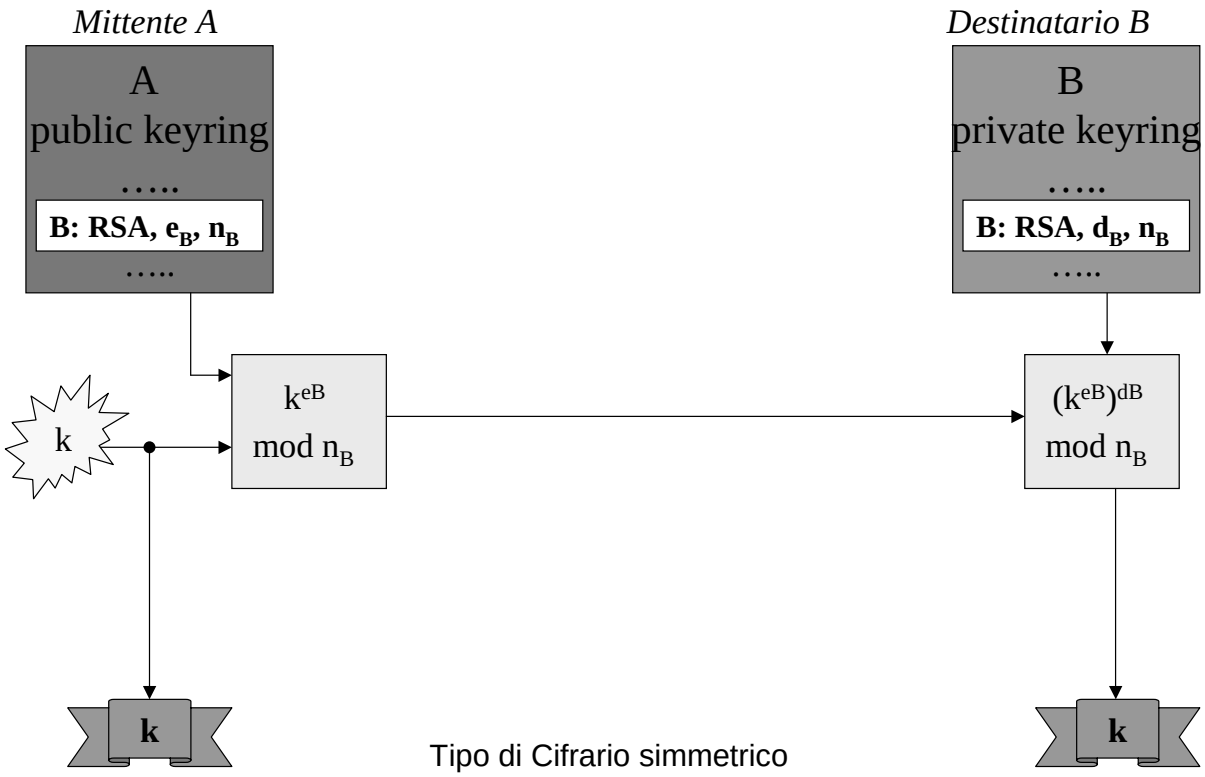
Messaggio riservato per più destinatari



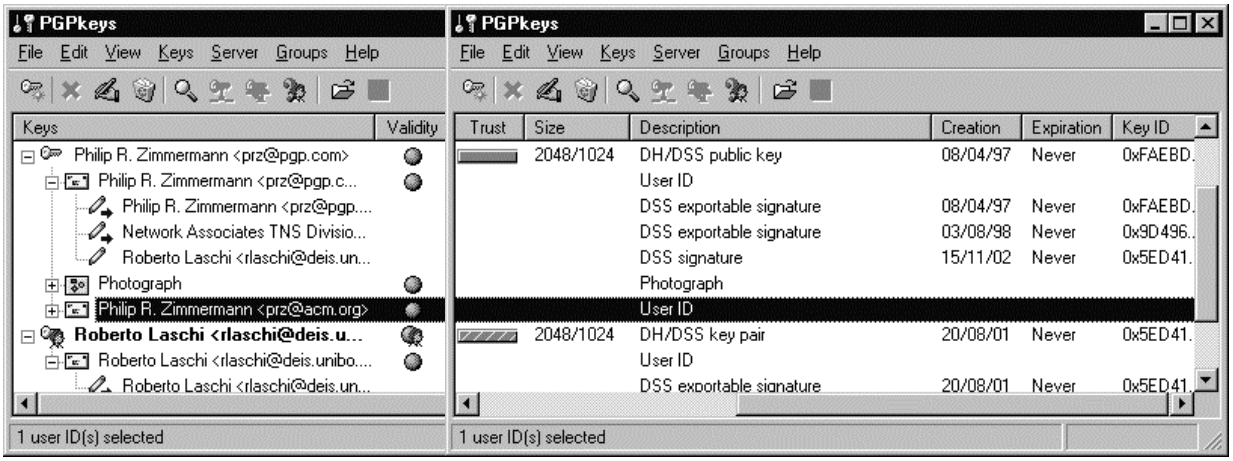
Chiave di messaggio con DH/ElGamal



Chiave di messaggio con RSA



La “vista” del portachiavi pubblico



Struttura dei portachiavi

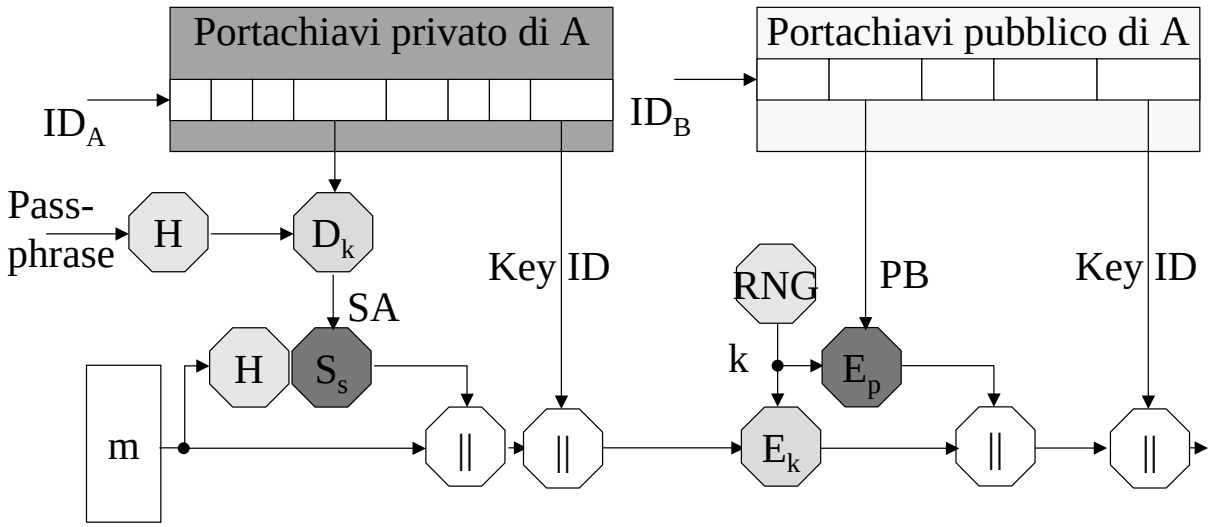
Private Key Ring

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
T_i	$KU_i \bmod 2^{64}$	KU_i	$E_{H(P_i)}[KR_i]$	User i
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

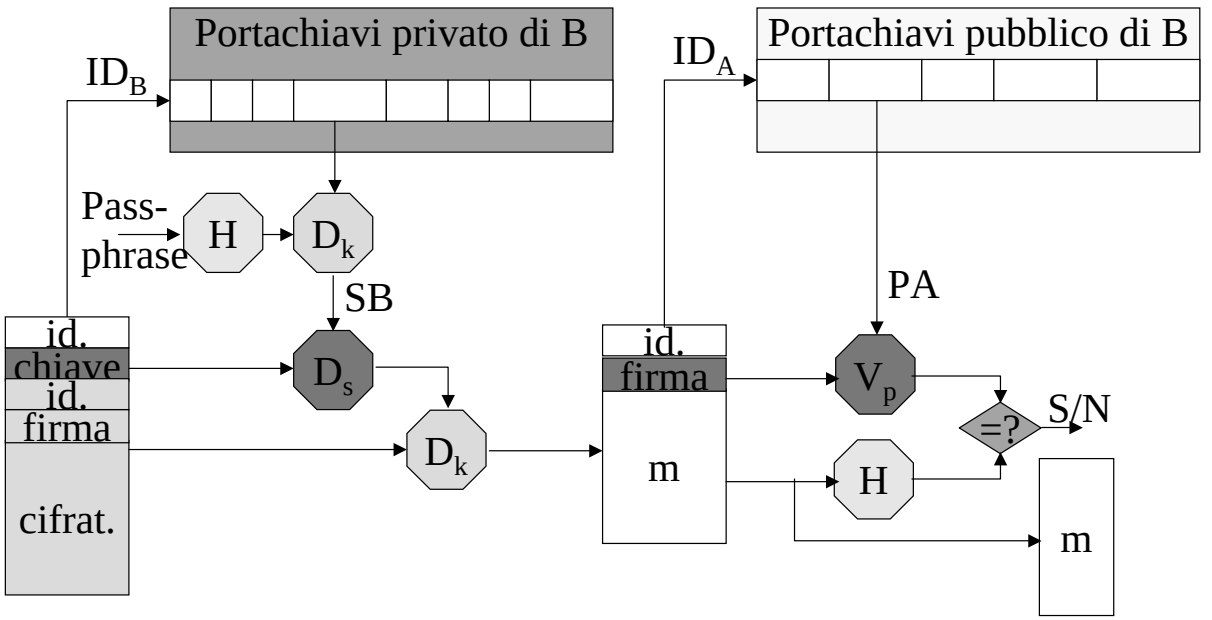
Public Key Ring

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
T_i	$KU_i \bmod 2^{64}$	KU_i	$trust\_flag_i$	User i	$trust\_flag_i$		
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.

Mittente: portachiavi privato e pubblico

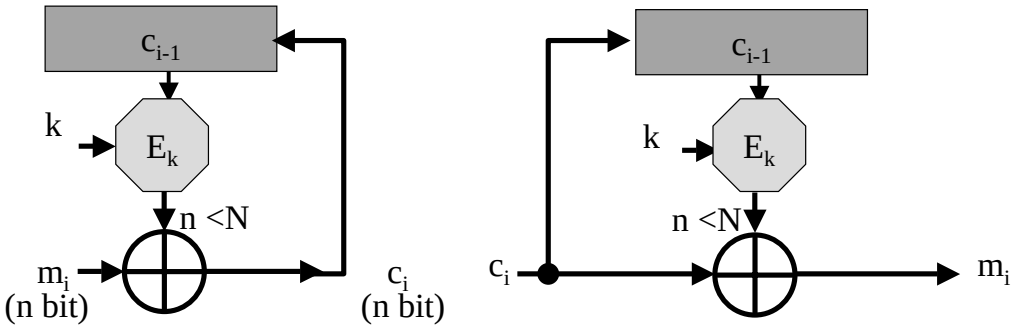


Destinatario: portachiavi privato e pubblico



Modalità di cifratura del PGP

CFB (Chipher Feedback)

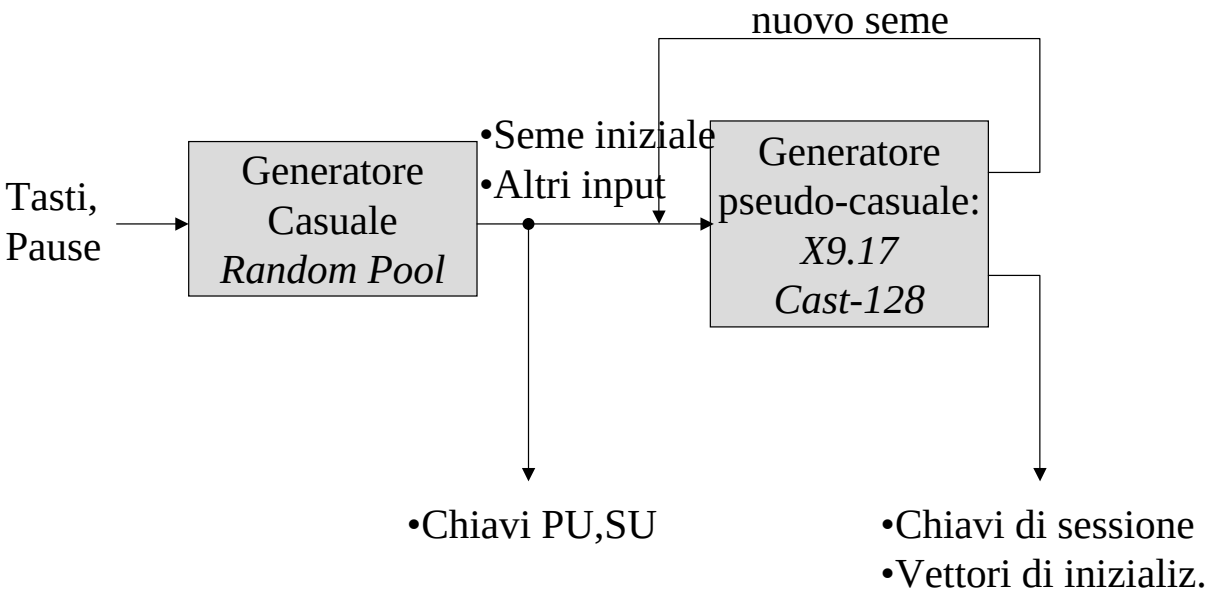


$c_i = m_i \oplus E_k(c_{i-1})$

$m_i = c_i \oplus E_k(c_{i-1})$

N = 64/128 bit
n = 64 bit

RNG e PRNG



radix-64

	000	001	010	011	100	101	110	111
000	A	B	C	D	E	F	G	H
001	I	J	K	L	M	N	O	P
010	Q	R	S	T	U	V	W	X
011	Y	Z	a	b	c	d	e	f
100	g	h	i	j	k	l	m	n
101	o	p	q	r	s	t	u	v
110	w	x	y	z	0	1	2	3
111	4	5	6	7	8	9	+	/