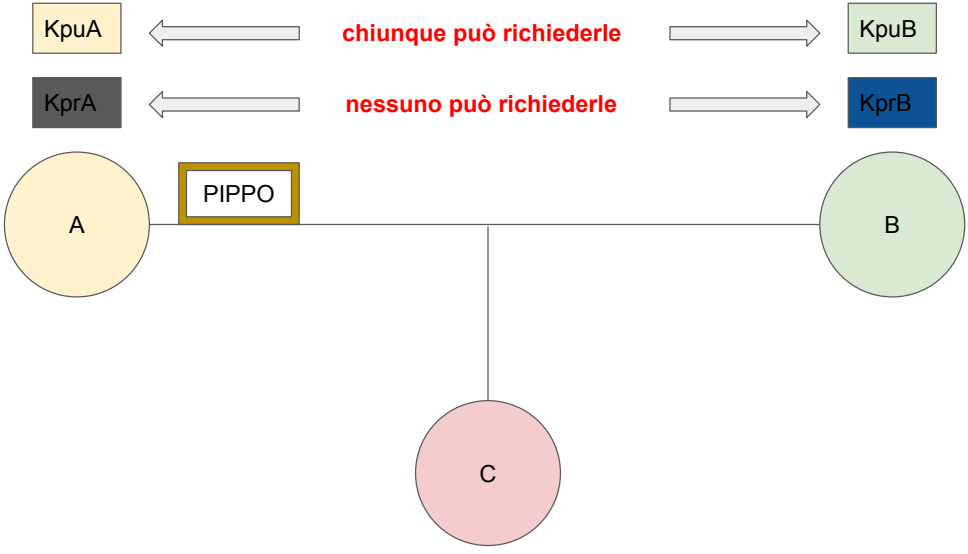
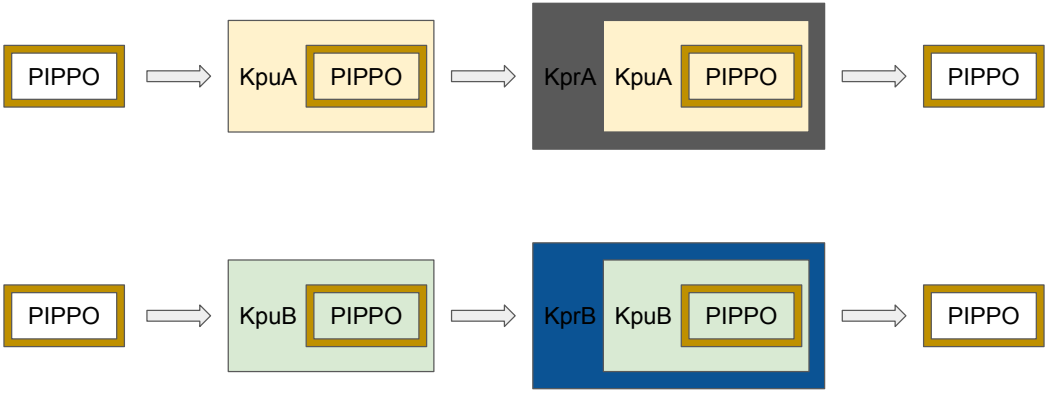
MODELLO RSA

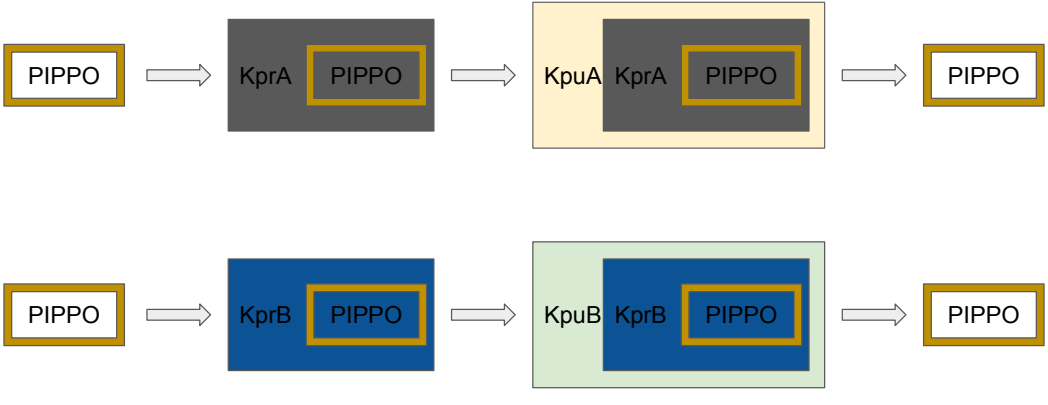
crittografia a chiave asimmetrica


KpuA
chiunque può richiederle
KpuB
KprA
nessuno può richiederle
KprB
A
PIPPO
B
C

CHIAVI

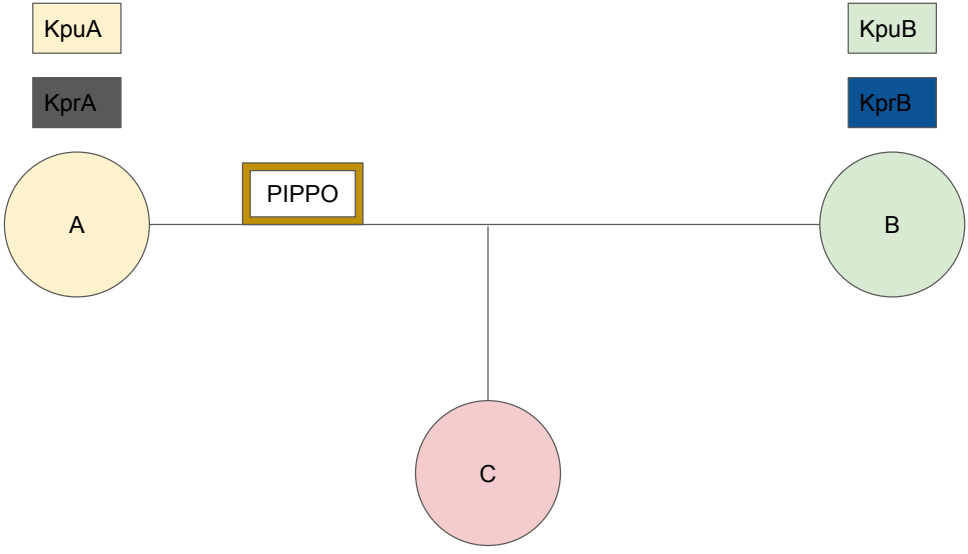
chiavi pubbliche e chiavi private

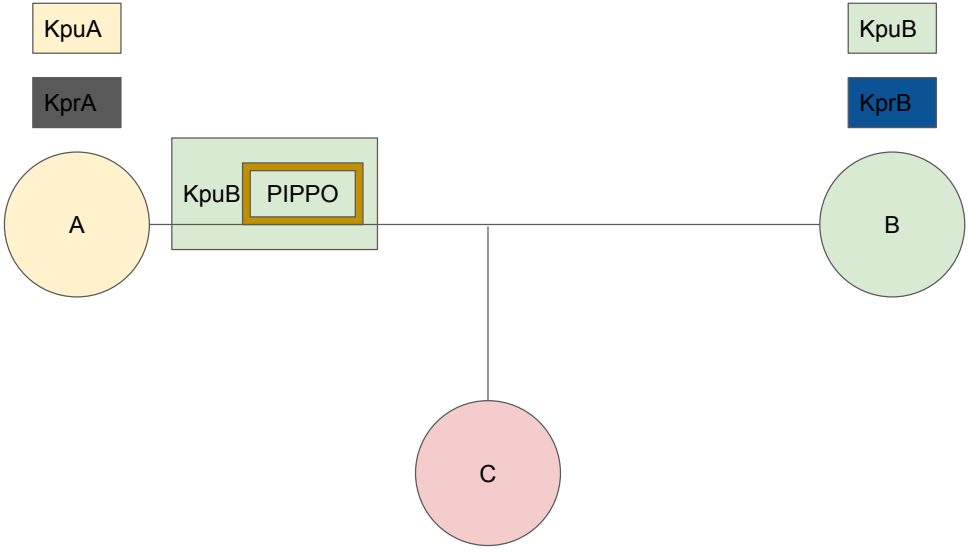

PIPPO
KpuA
PIPPO
KprA
KpuA
PIPPO
PIPPO
PIPPO
KpuB
PIPPO
KprB
KpuB
PIPPO
PIPPO

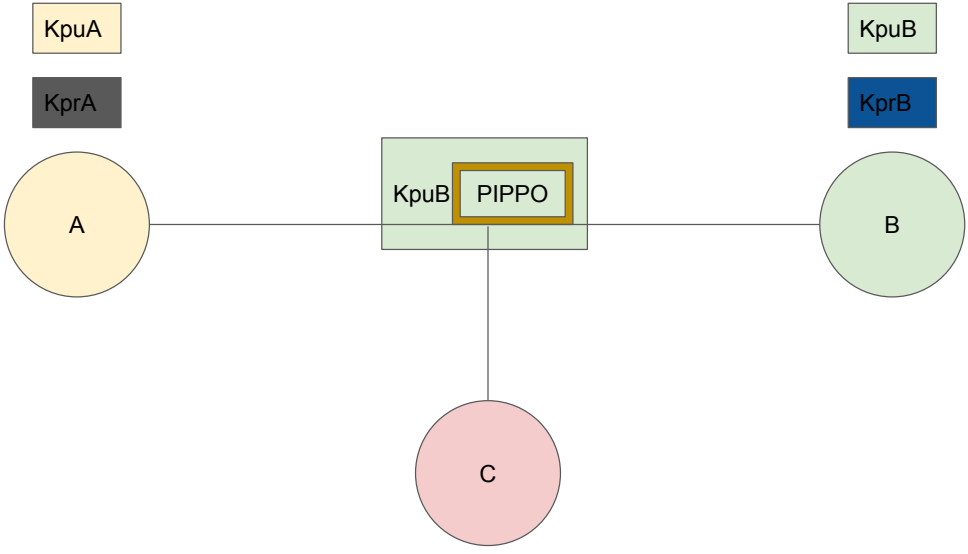

PIPPO
KprA
PIPPO
KpuA
KprA
PIPPO
PIPPO
PIPPO
KprB
PIPPO
KpuB
KprB
PIPPO
PIPPO

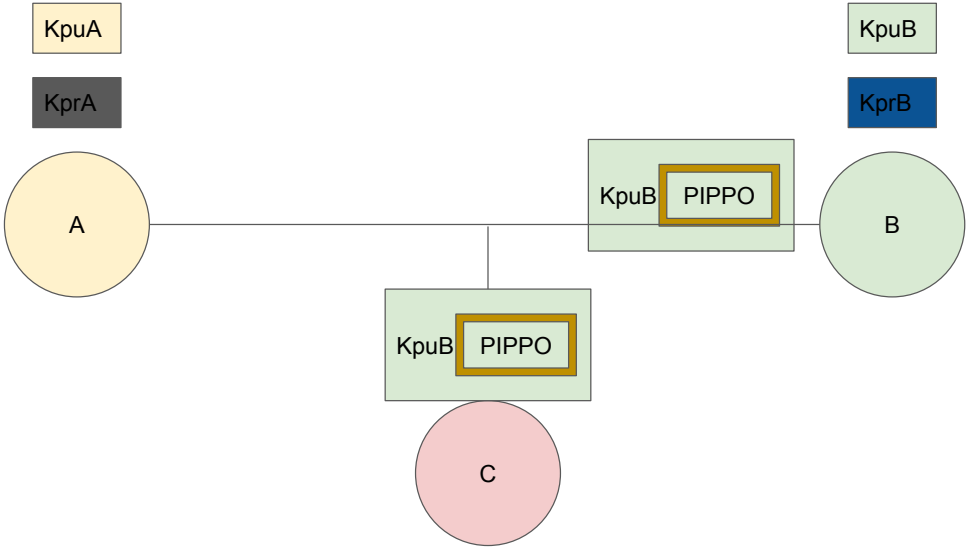
CONFIDENZIALITÀ

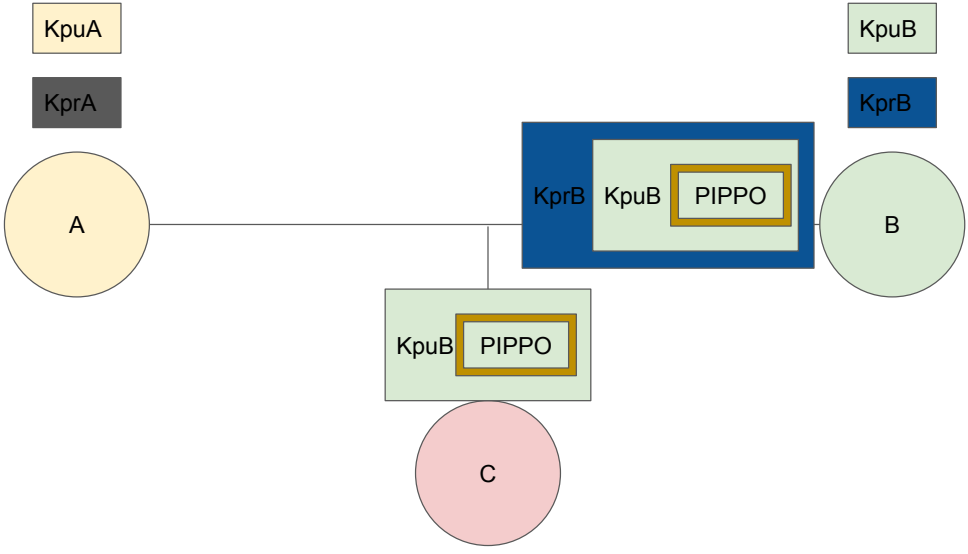
garantire la riservatezza di un messaggio

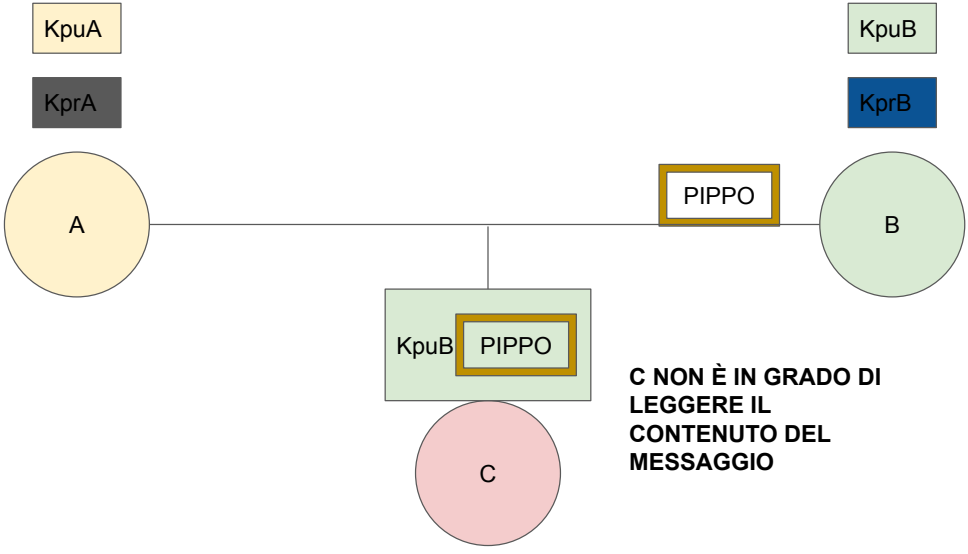

KpuA
KprA
KpuB
KprB
A
PIPPO
B
C

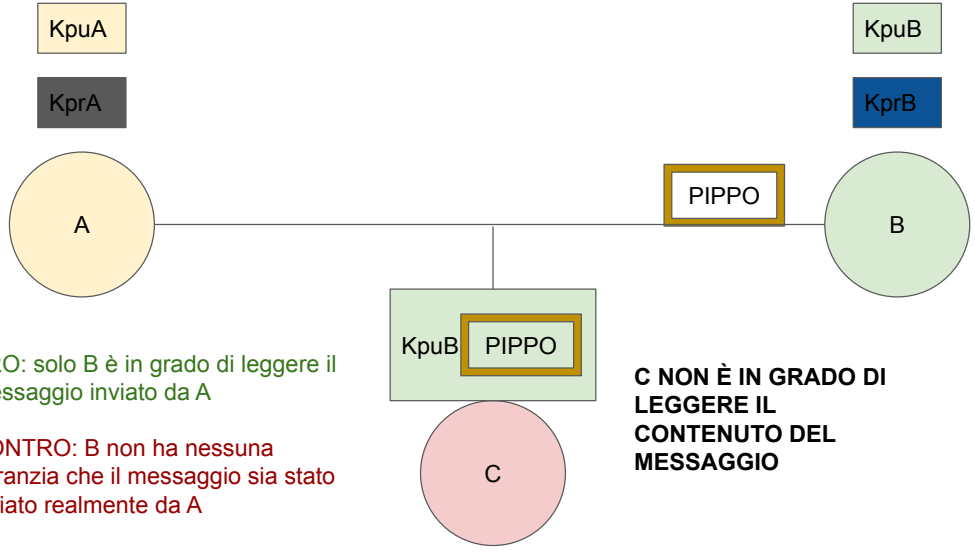

KpuA
KprA
KpuB
KprB
A
KpuB
PIPPO
B
C


KpuA
KprA
KpuB
KprB
KpuB
PIPPO
A
B
C


KpuA
KprA
KpuB
KprB
A
KpuB
PIPPO
B
KpuB
PIPPO
C


KpuA
KprA
KpuB
KprB
A
KprB
KpuB
PIPPO
B
KpuB
PIPPO
C


KpuA
KprA
KpuB
KprB
A
PIPPO
B
KpuB
PIPPO
C
C NON È IN GRADO DI LEGGERE IL CONTENUTO DEL MESSAGGIO



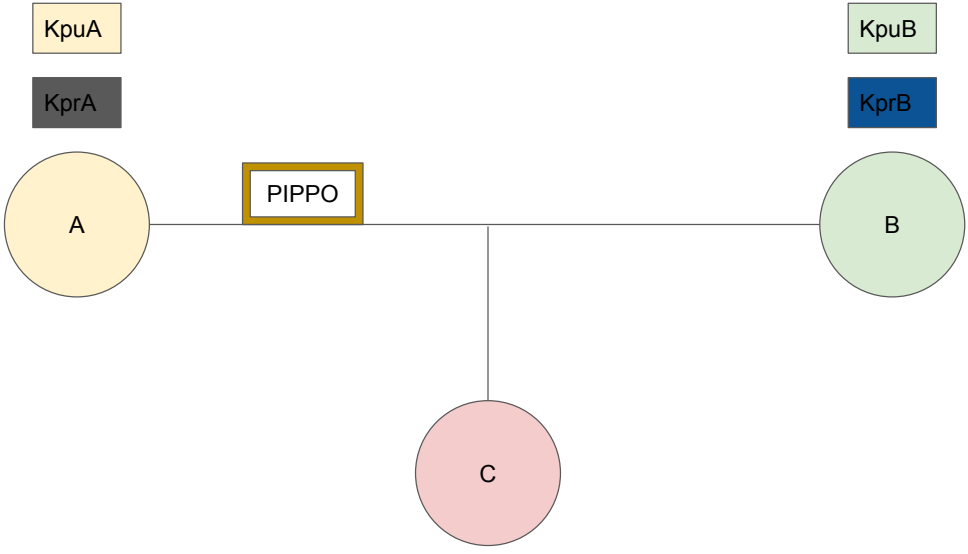
PRO: solo B è in grado di leggere il messaggio inviato da A

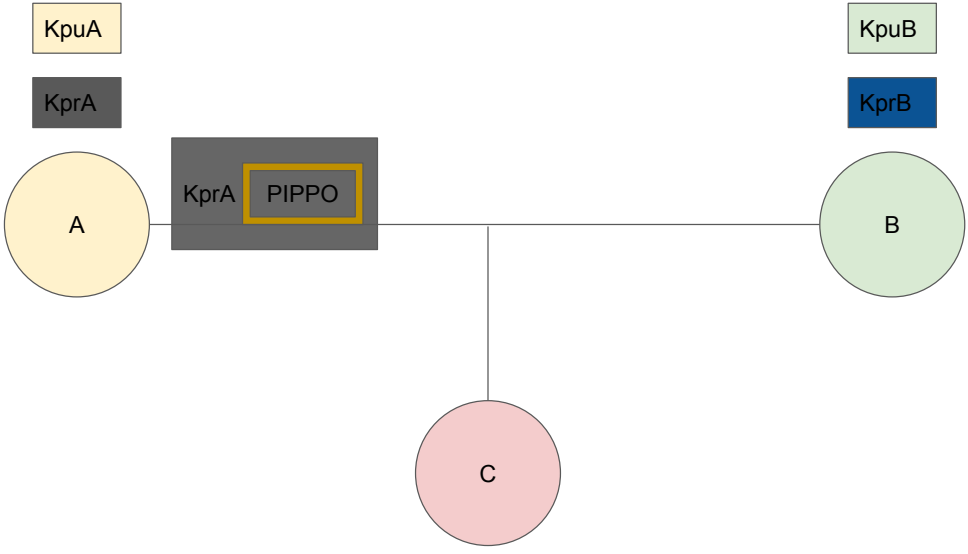
CONTRO: B non ha nessuna garanzia che il messaggio sia stato inviato realmente da A

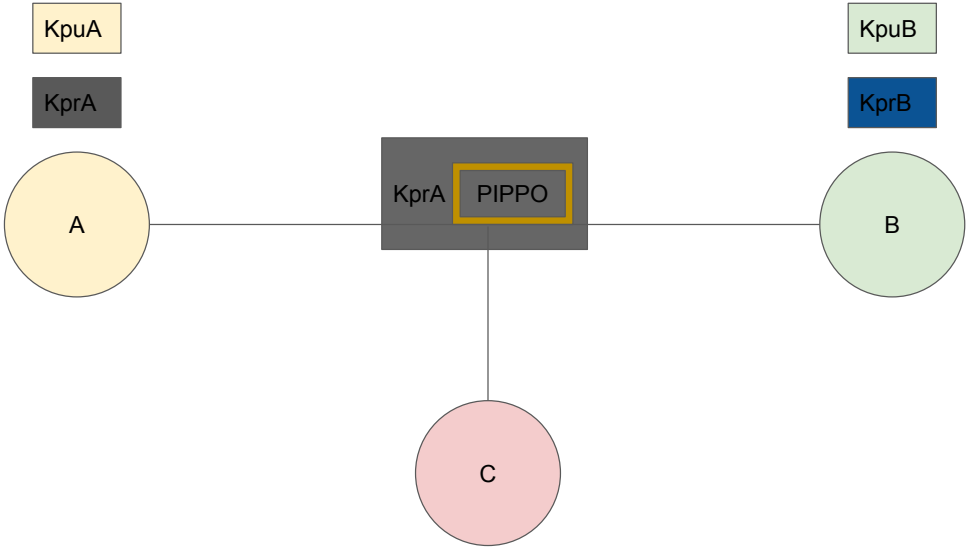
C NON È IN GRADO DI LEGGERE IL CONTENUTO DEL MESSAGGIO

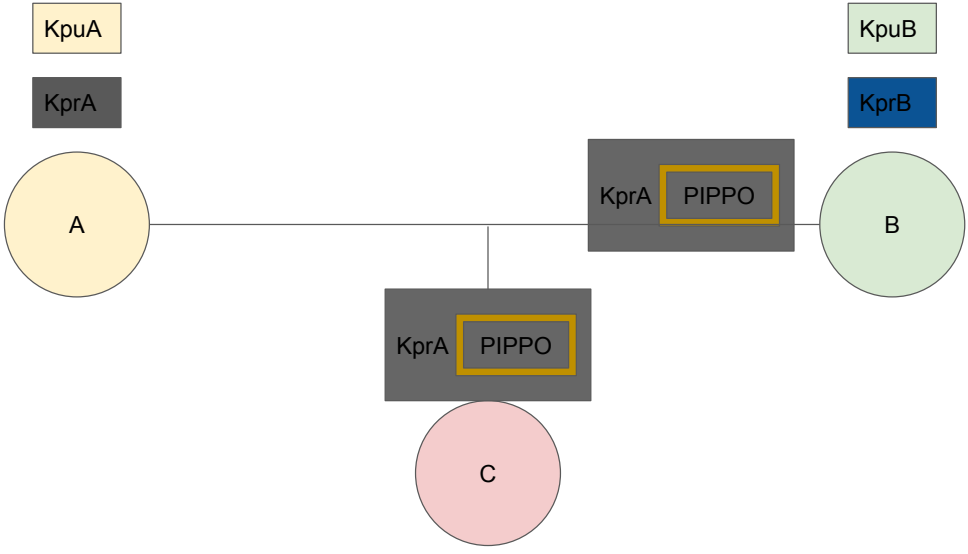
AUTENTICITÀ

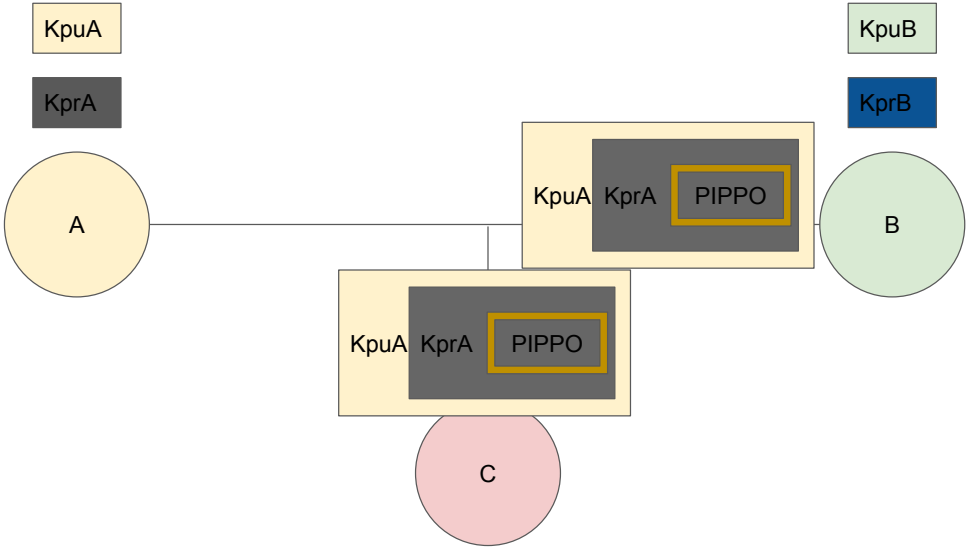
firma digitale

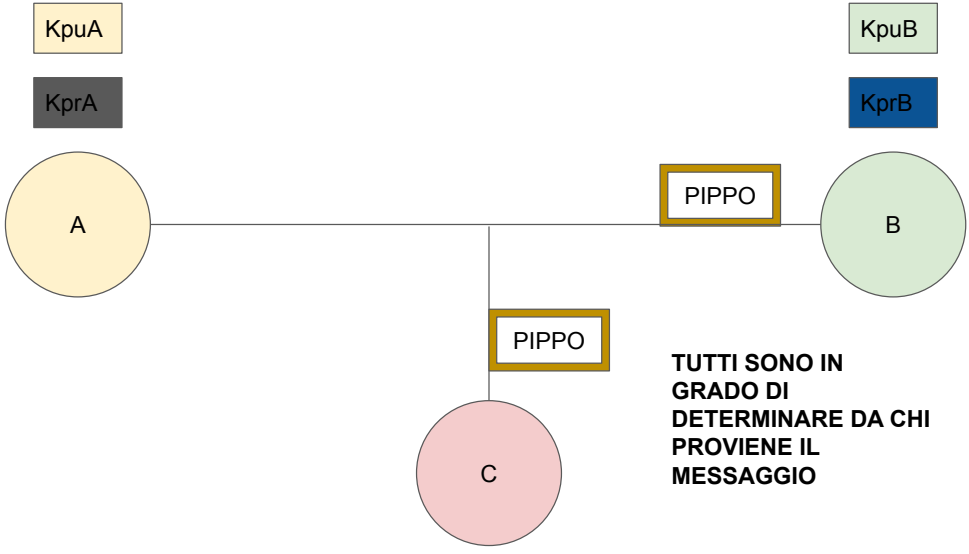

KpuA
KprA
KpuB
KprB
A
PIPPO
B
C

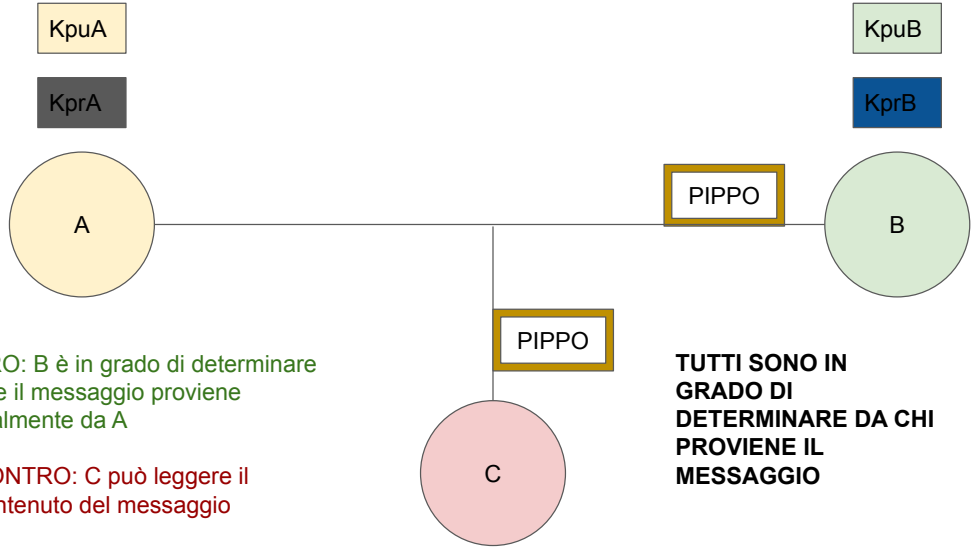

KpuA
KprA
KprA
PIPPO
A
B
C
KpuB
KprB


KpuA
KprA
KprA
PIPPO
KpuB
KprB
A
B
C


KpuA
KprA
KpuB
KprB
A
KprA
PIPPO
B
KprA
PIPPO
C


KpuA
KprA
KpuB
KprB
A
KpuA
KprA
PIPPO
B
KpuA
KprA
PIPPO
C


KpuA
KprA
KpuB
KprB
A
PIPPO
B
PIPPO
C
TUTTI SONO IN GRADO DI DETERMINARE DA CHI PROVIENE IL MESSAGGIO



PRO: B è in grado di determinare che il messaggio proviene realmente da A

CONTRO: C può leggere il contenuto del messaggio

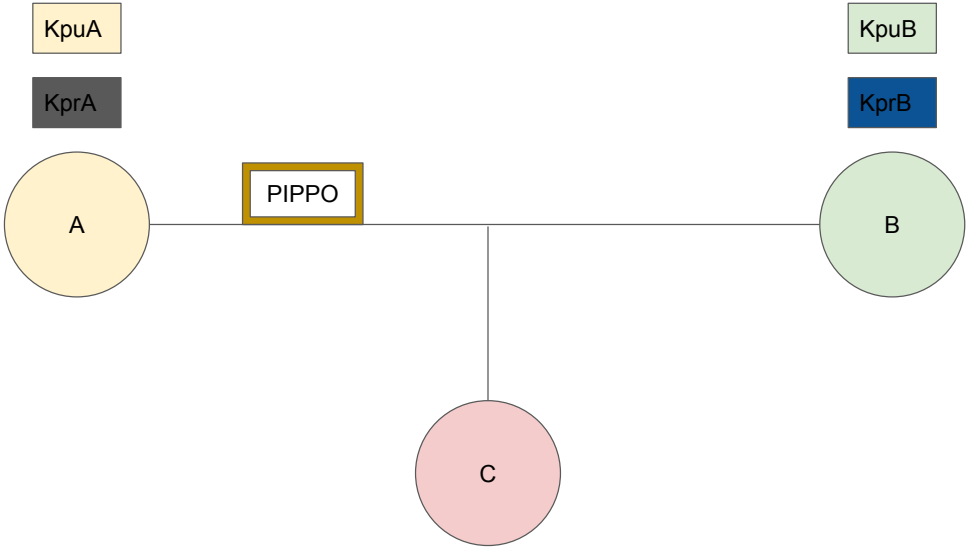
TUTTI SONO IN GRADO DI DETERMINARE DA CHI PROVIENE IL MESSAGGIO

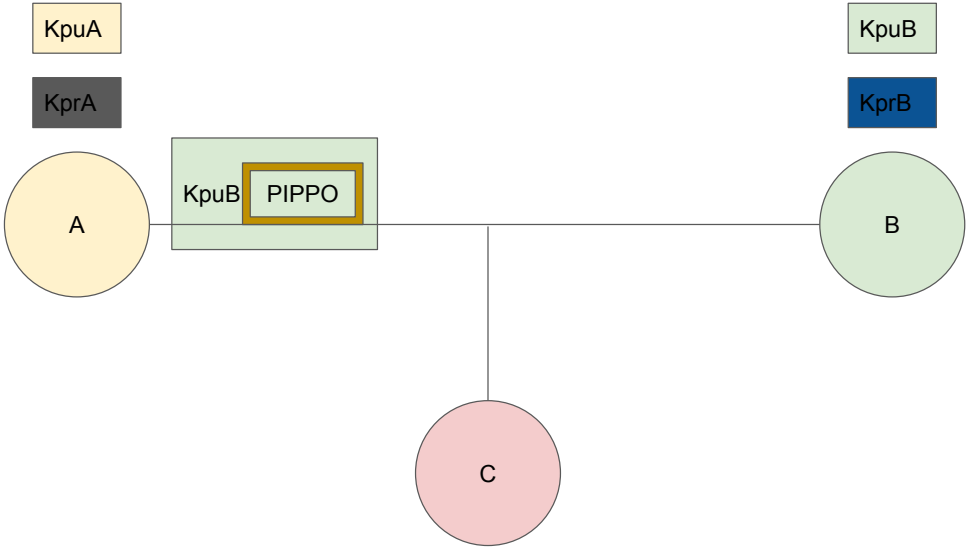
INTEGRITÀ

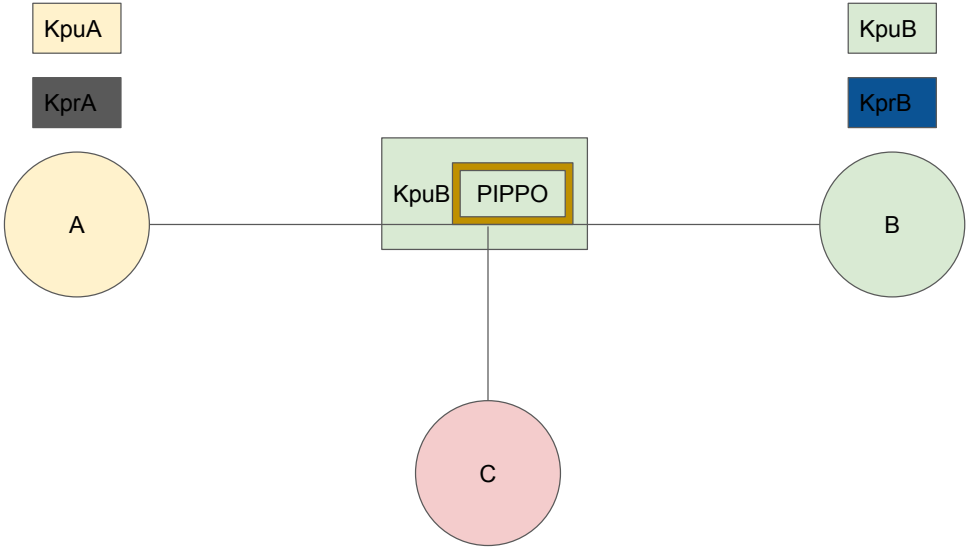
garantire la non modificabilità di un messaggio

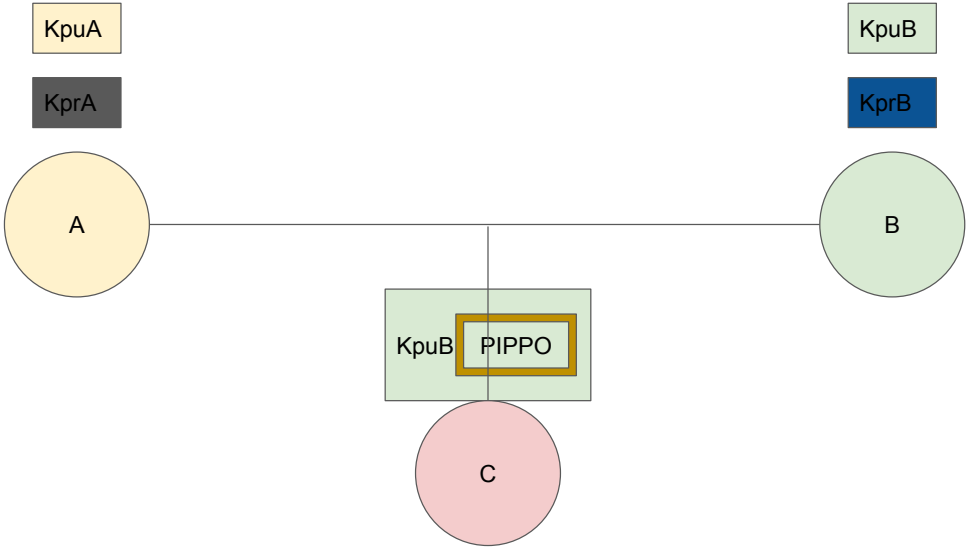
PROBLEMA

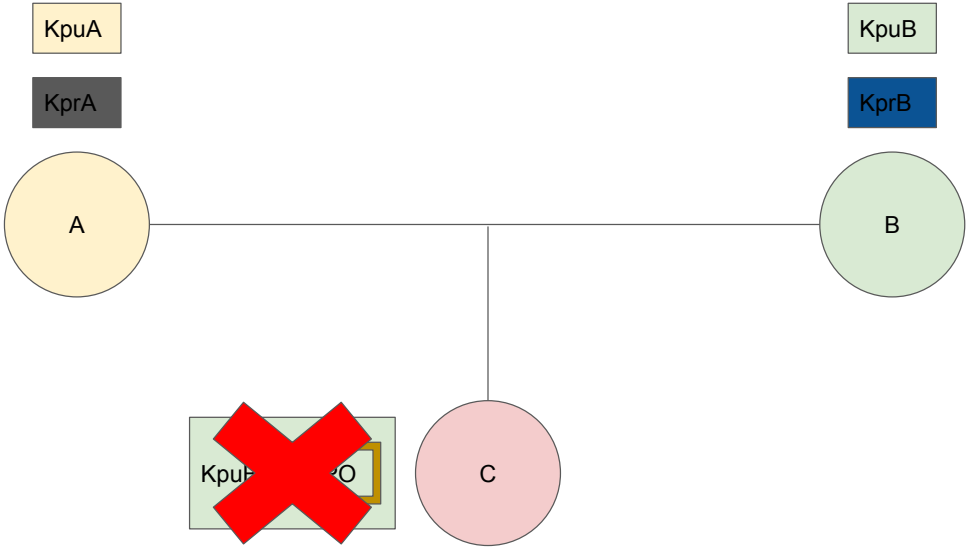
possibile attacco all’integrità di un messaggio

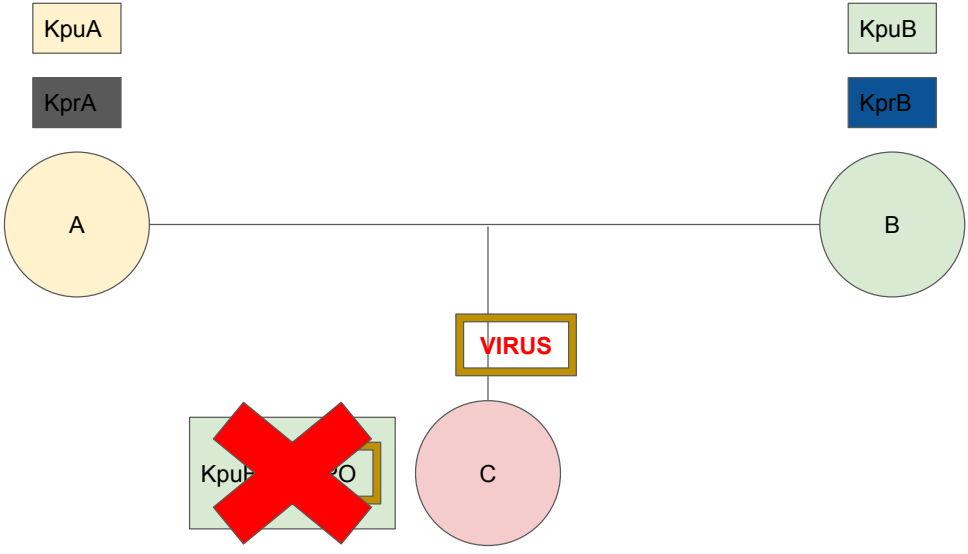

KpuA
KprA
KpuB
KprB
A
PIPPO
B
C

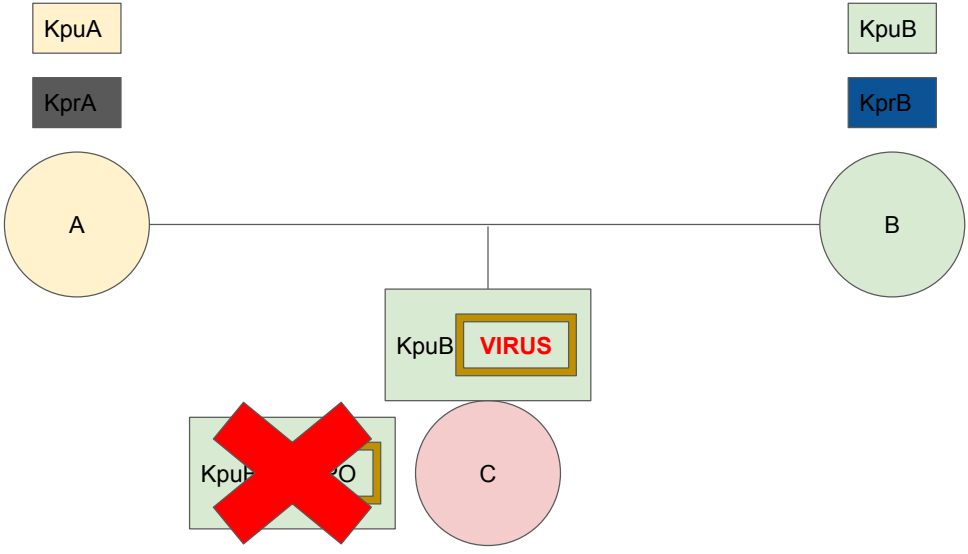

KpuA
KprA
KpuB
KprB
A
KpuB
PIPPO
B
C

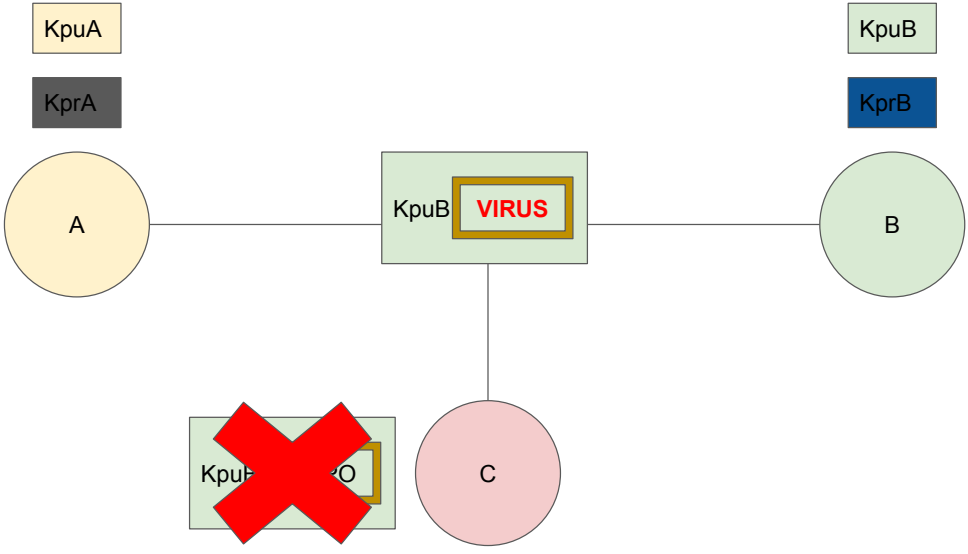

KpuA
KprA
KpuB
KprB
KpuB
PIPPO
A
B
C

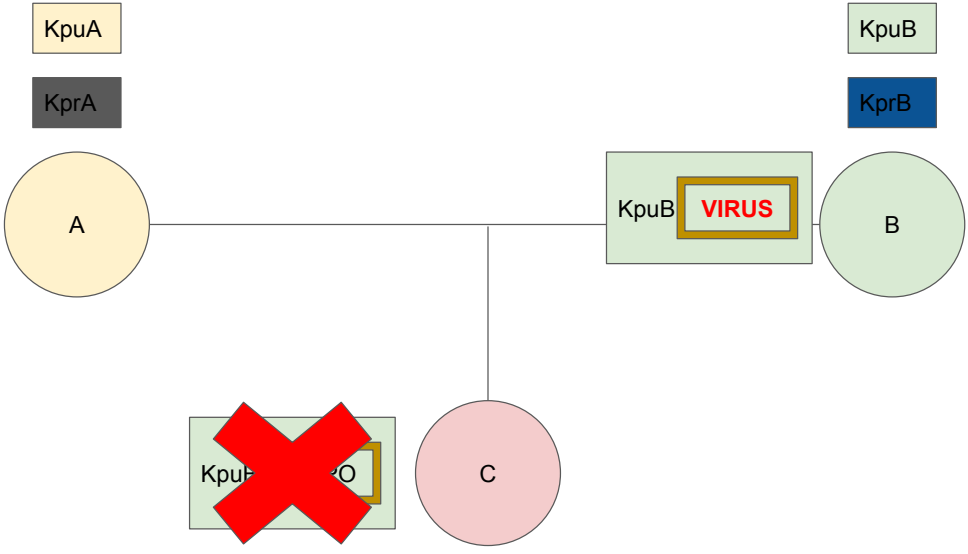

KpuA
KprA
KpuB
KprB
A
B
KpuB
PIPPO
C

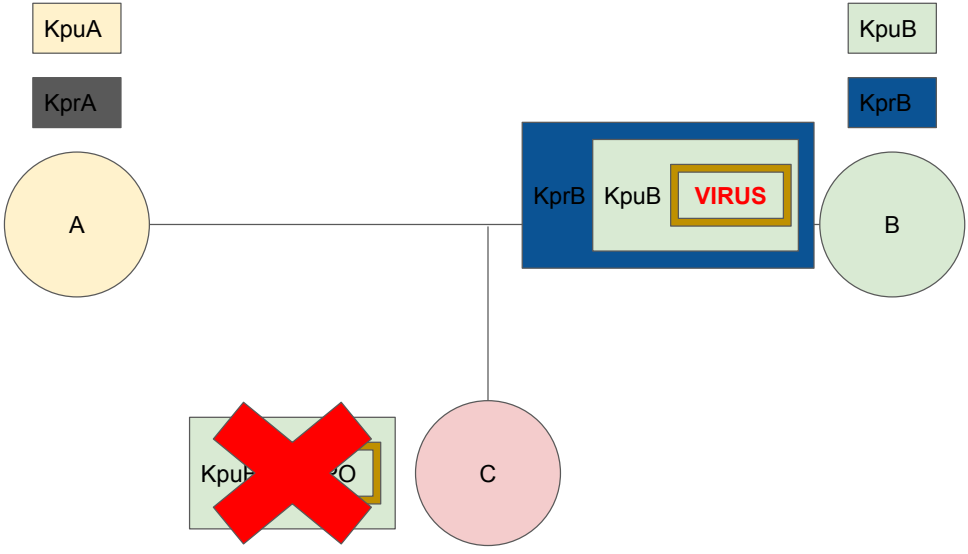

KpuA
KprA
KpuB
KprB
A
B
C

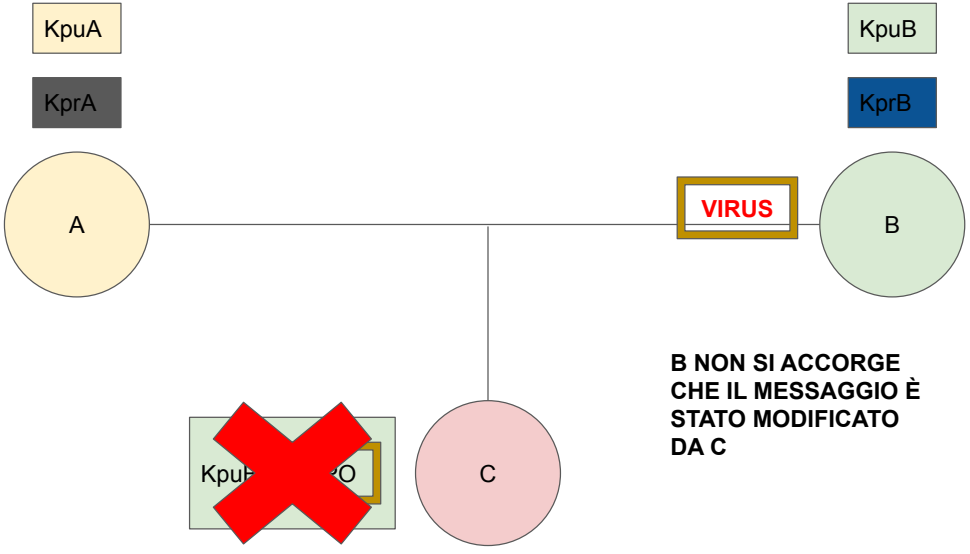

KpuA
KprA
KpuB
KprB
A
B
VIRUS
C


KpuA
KprA
KpuB
KprB
A
B
KpuB
VIRUS
C


KpuA
KprA
KpuB
KprB
A
KpuB
VIRUS
B
C

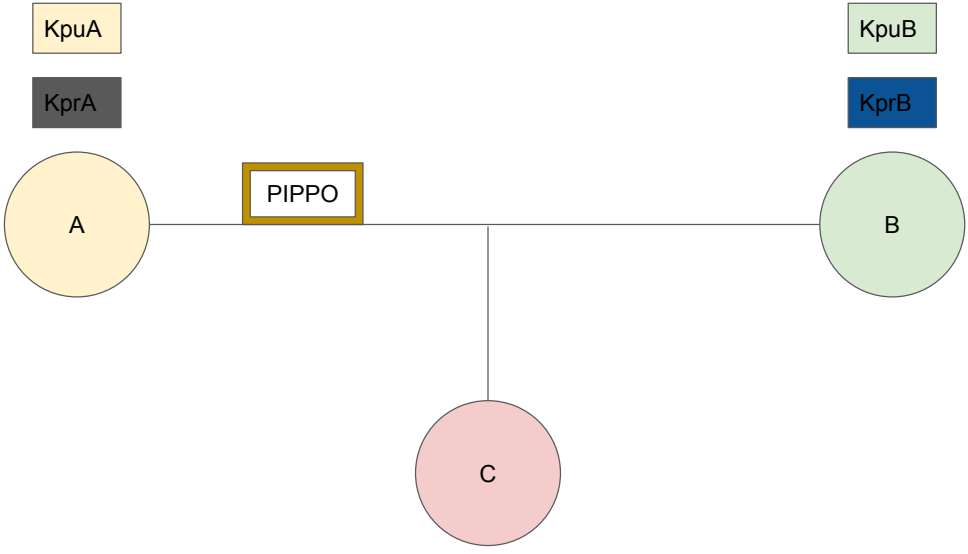

KpuA
KprA
KpuB
KprB
A
KpuB
VIRUS
B
C

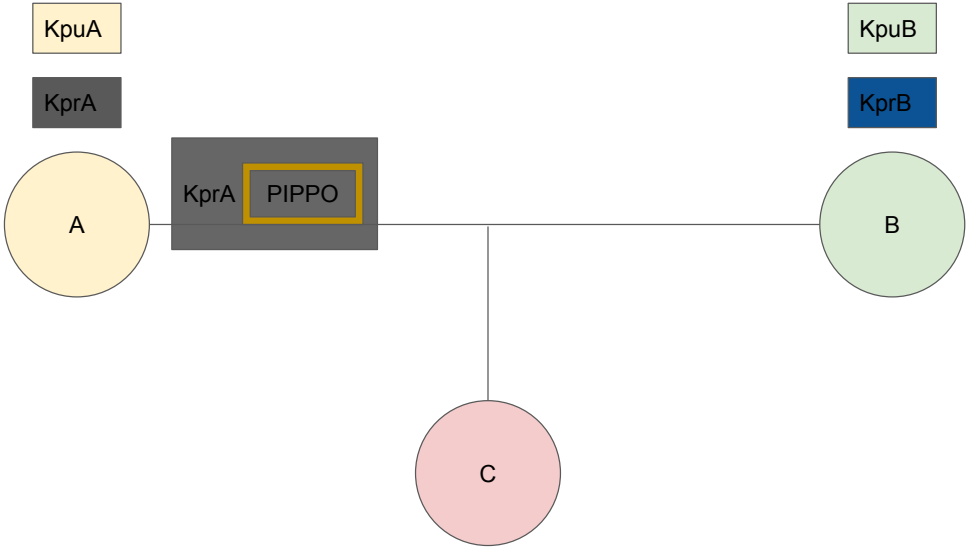

KpuA
KprA
KpuB
KprB
A
KprB
KpuB
VIRUS
B
C

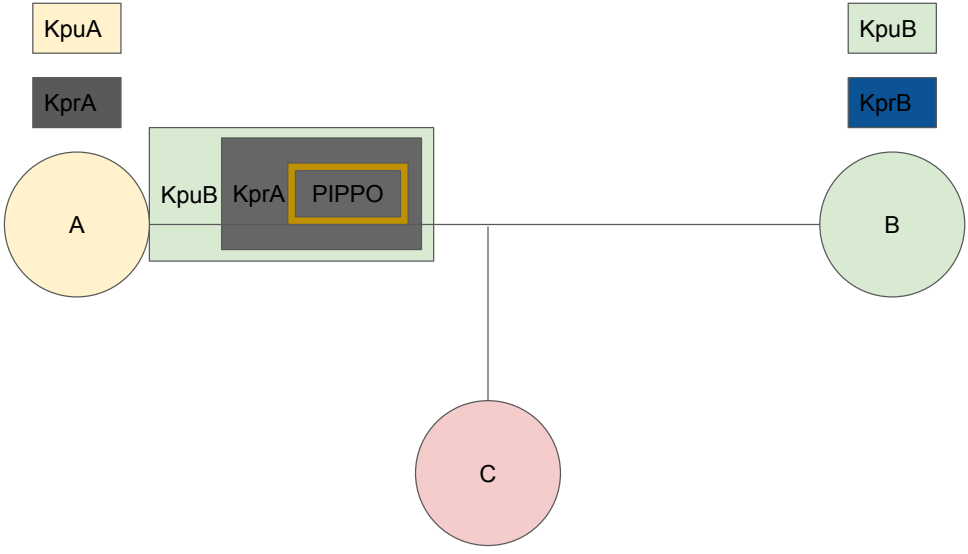

KpuA
KprA
KpuB
KprB
A
VIRUS
B
C
B NON SI ACCORGE
CHE IL MESSAGGIO È
STATO MODIFICATO
DA C

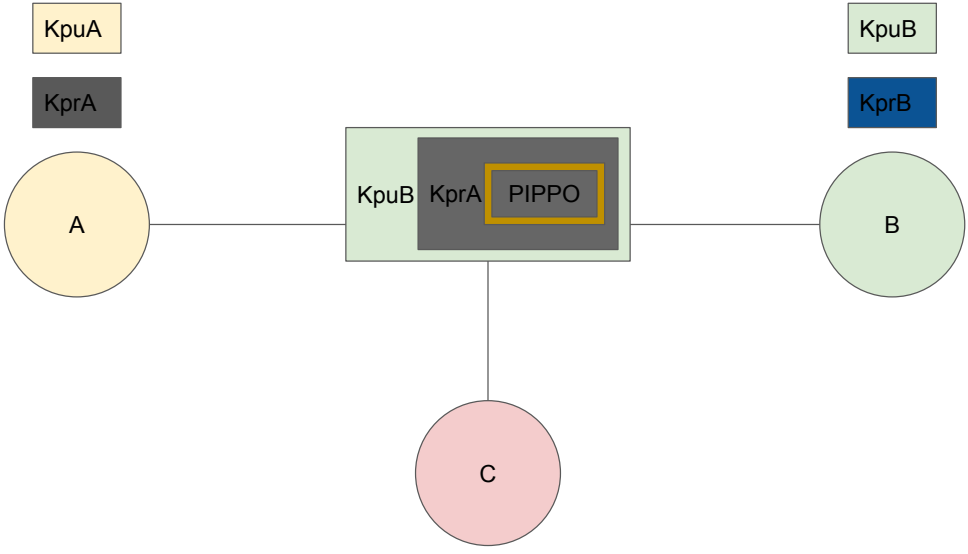
SOLUZIONE

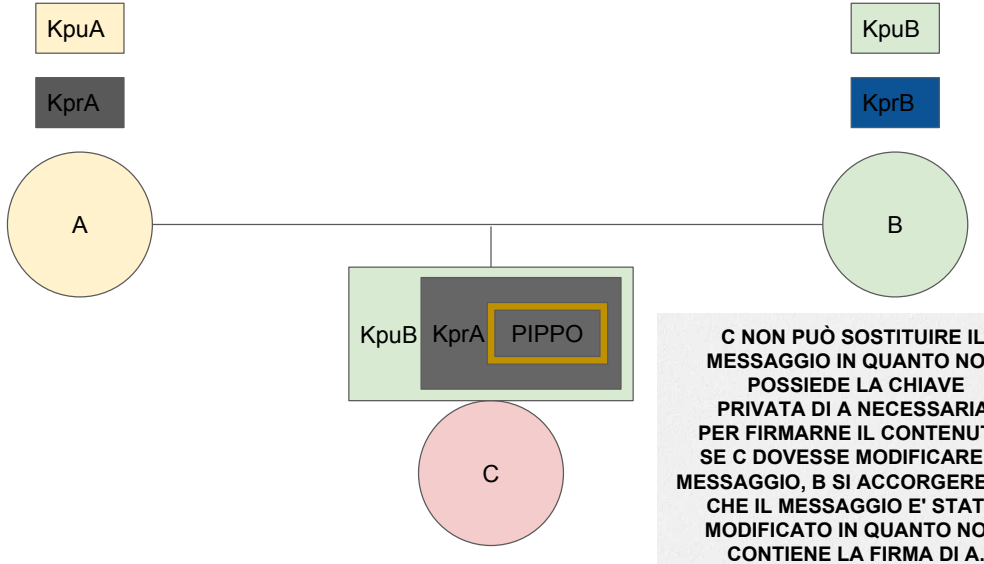
possibile attacco all’integrità di un messaggio


KpuA
KprA
KpuB
KprB
A
PIPPO
B
C

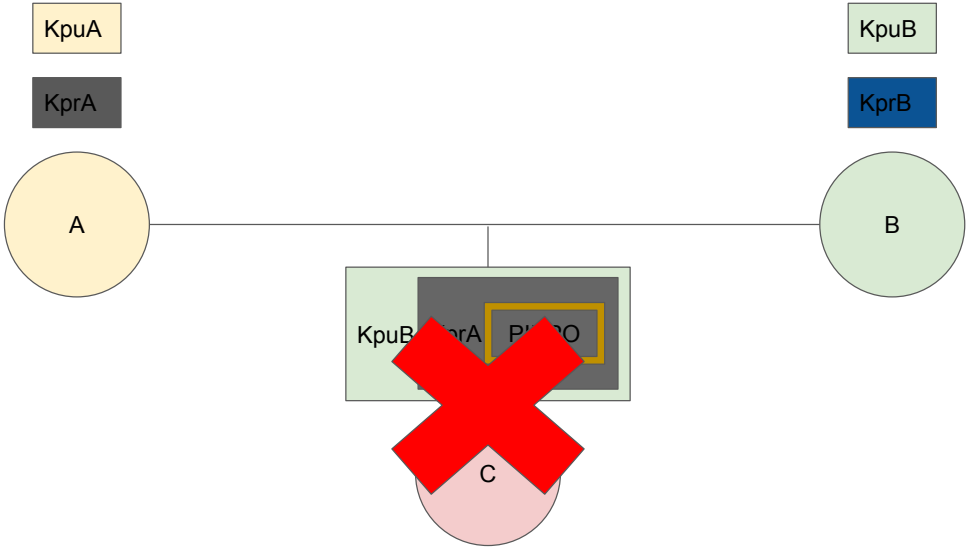

KpuA
KprA
KprA
PIPPO
A
B
C
KpuB
KprB

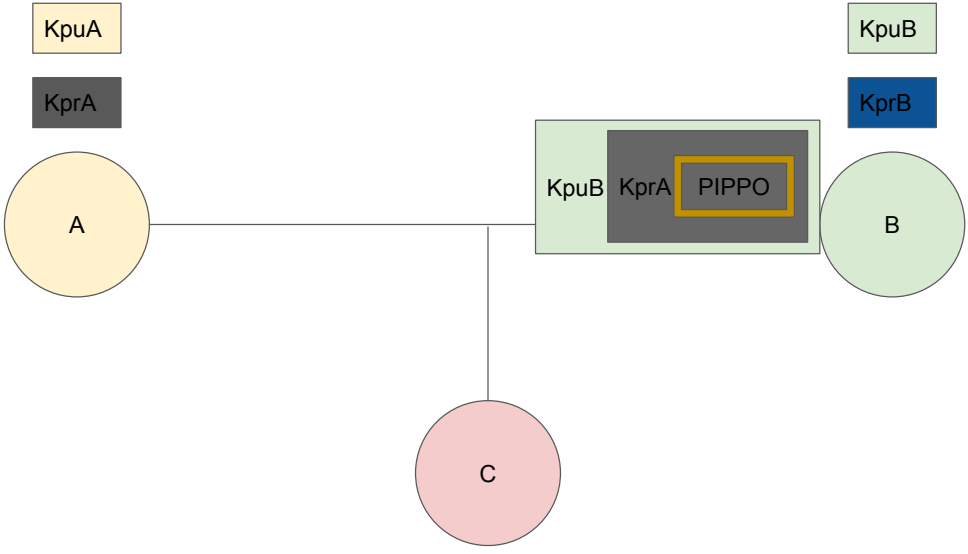

KpuA
KprA
KpuB
KprB
KpuB
KprA
PIPPO
A
B
C

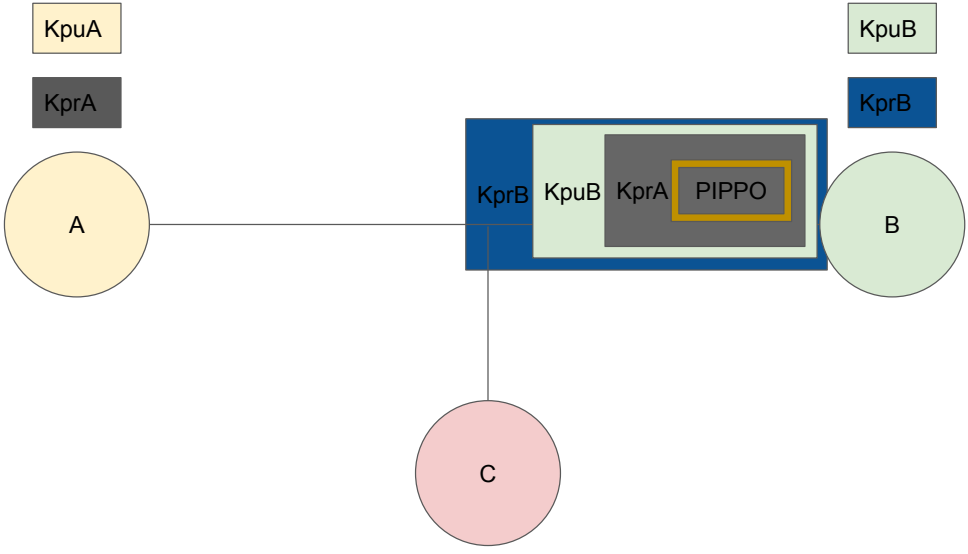

KpuA
KprA
KpuB
KprB
A
KpuB
KprA
PIPPO
B
C

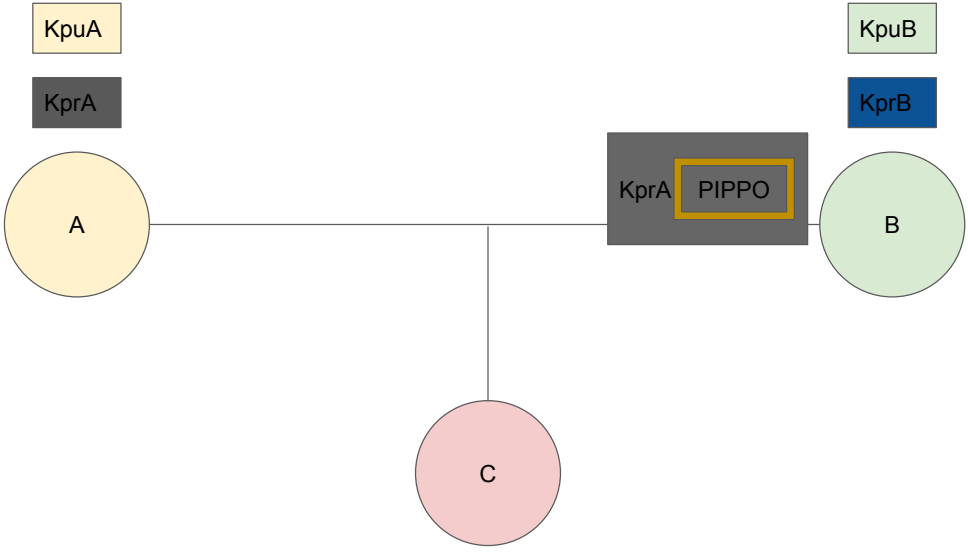


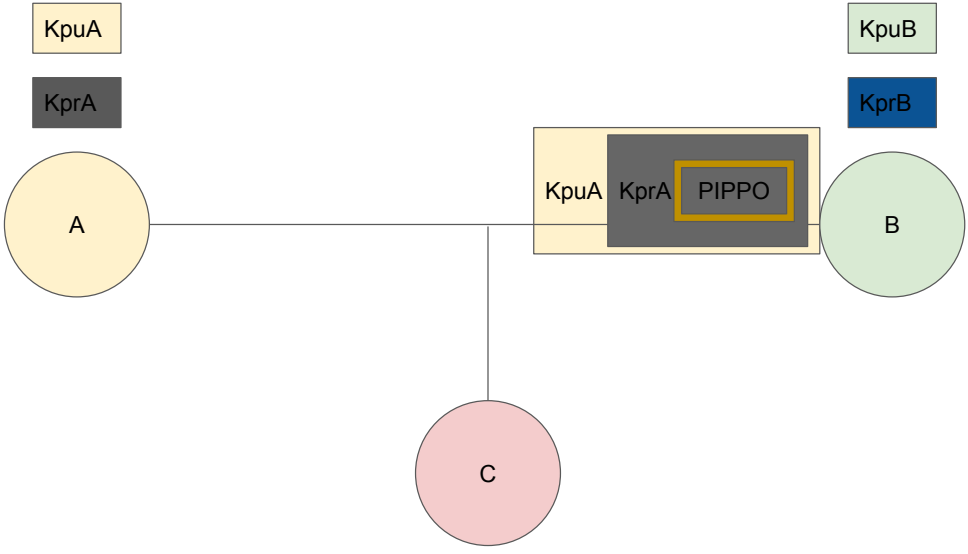
C NON PUÒ SOSTITUIRE IL MESSAGGIO IN QUANTO NON POSSIEDE LA CHIAVE PRIVATA DI A NECESSARIA PER FIRMARNE IL CONTENUTO. SE C DOVESSE MODIFICARE IL MESSAGGIO, B SI ACCORGEREBBE CHE IL MESSAGGIO E' STATO MODIFICATO IN QUANTO NON CONTIENE LA FIRMA DI A.

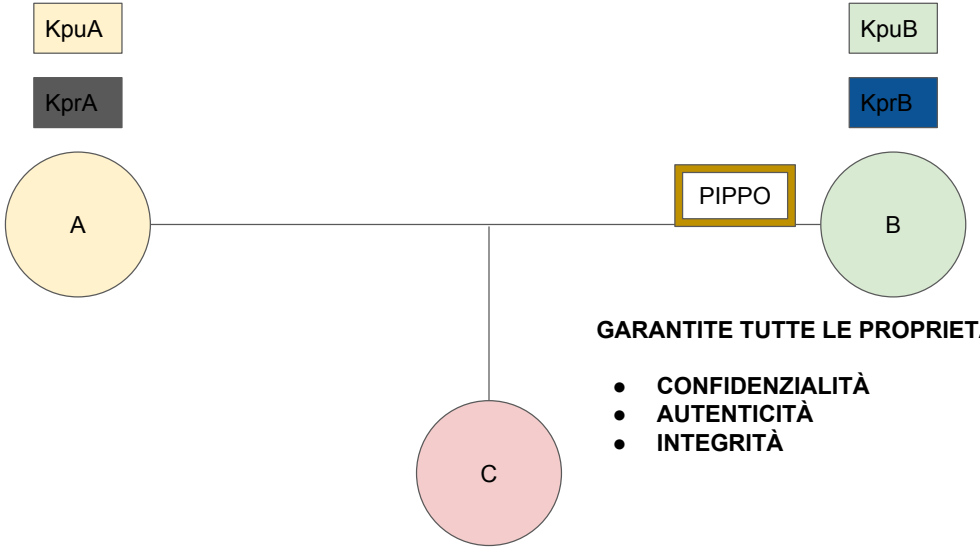

KpuA
KprA
KpuB
KprB
A
B
C


KpuA
KprA
KpuB
KprB
A
KpuB
KprA
PIPPO
B
C


KpuA
KprA
KpuB
KprB
A
KprB
KpuB
KprA
PIPPO
B
C


KpuA
KprA
KpuB
KprB
KprA
PIPPO
A
B
C


KpuA
KprA
KpuB
KprB
A
KpuA
KprA
PIPPO
B
C

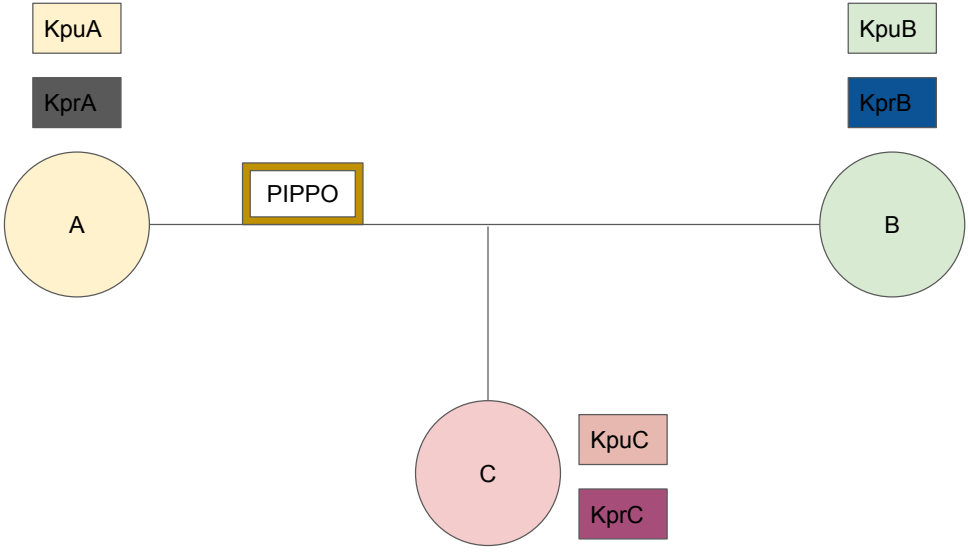


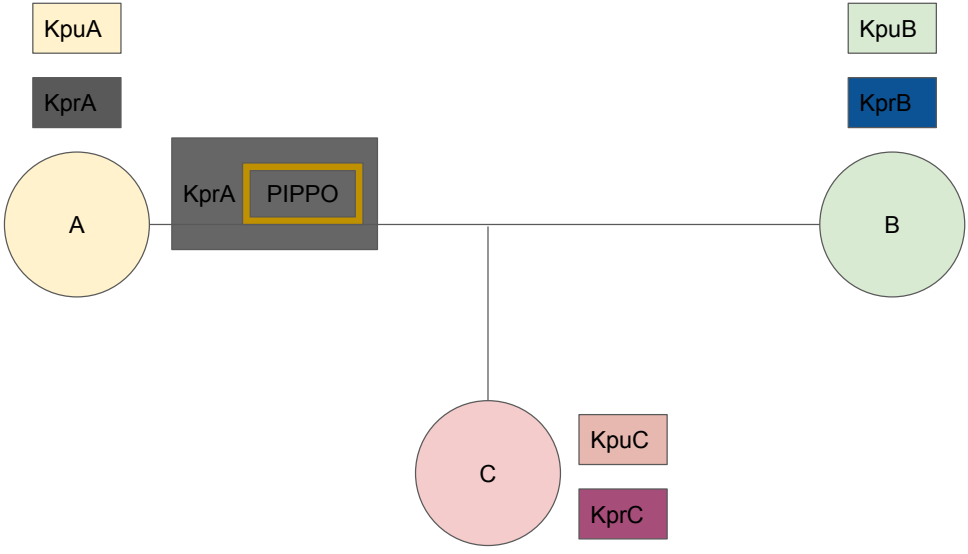
GARANTITE TUTTE LE PROPRIETÀ

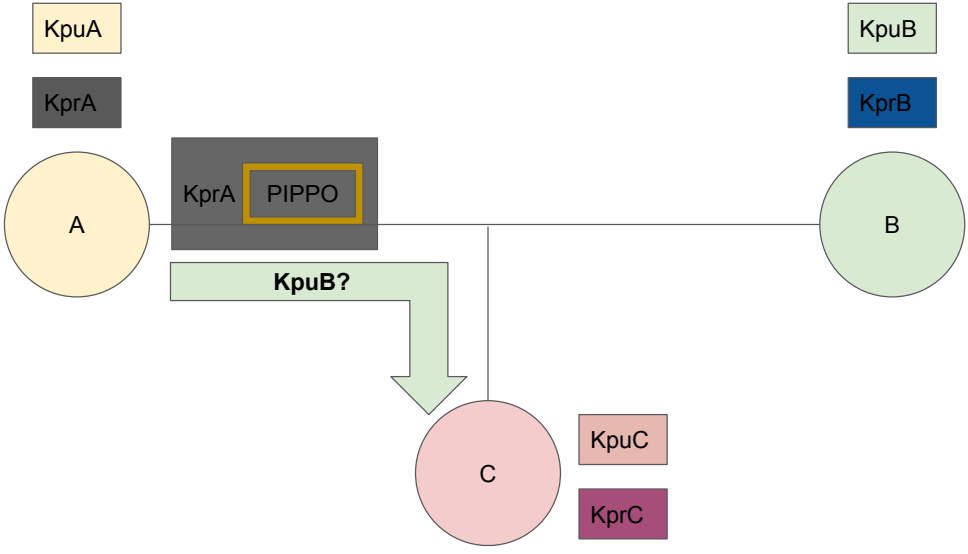
- **CONFIDENZIALITÀ**
- **AUTENTICITÀ**
- **INTEGRITÀ**

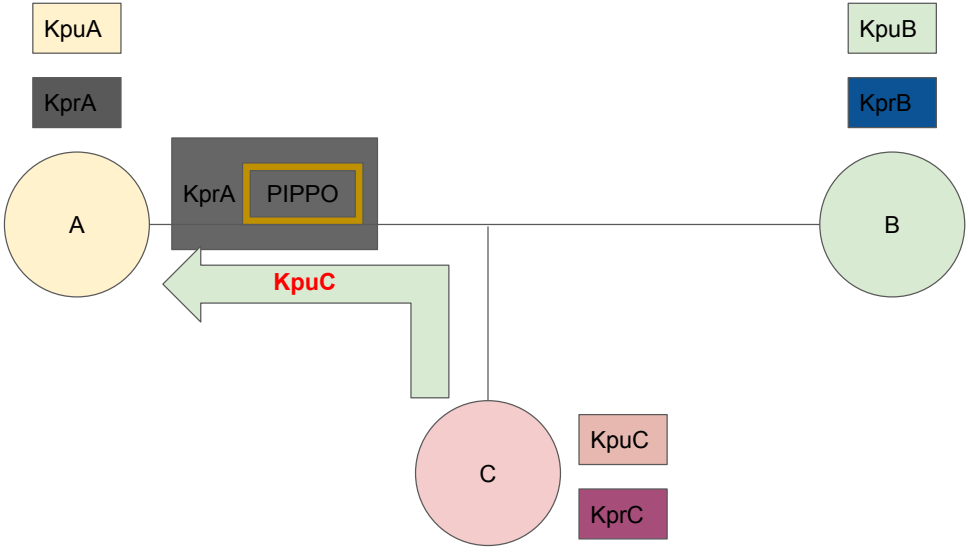
MAN IN THE MIDDLE

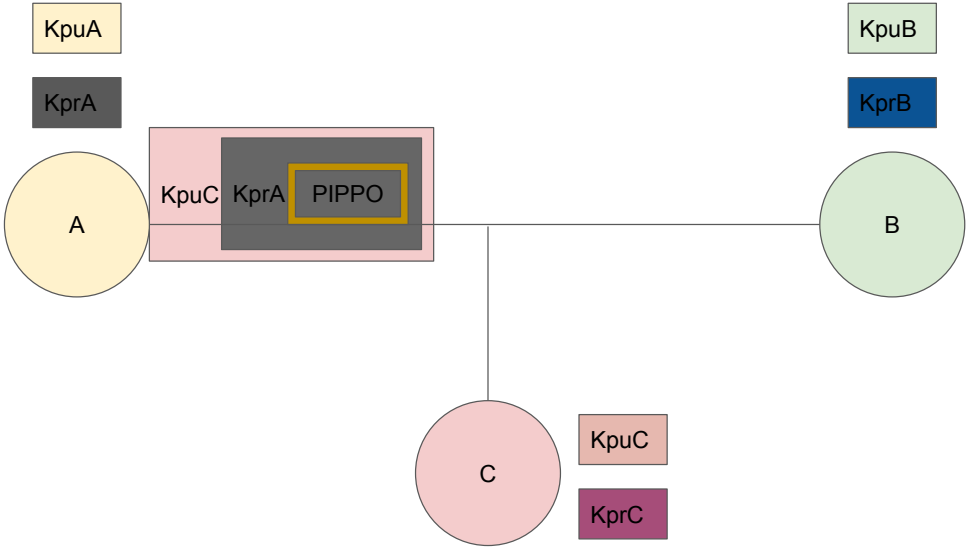
attacco al modello RSA

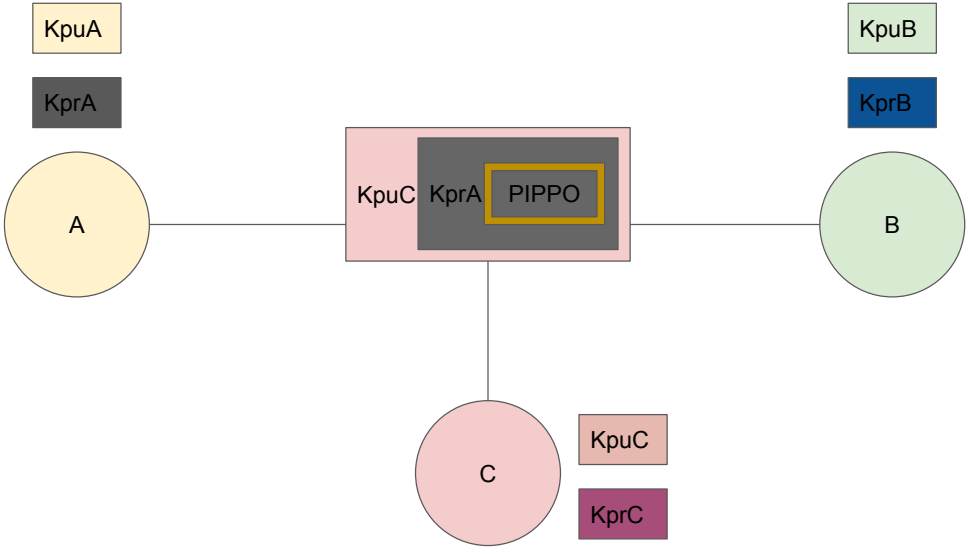

KpuA
KprA
KpuB
KprB
A
PIPPO
B
C
KpuC
KprC

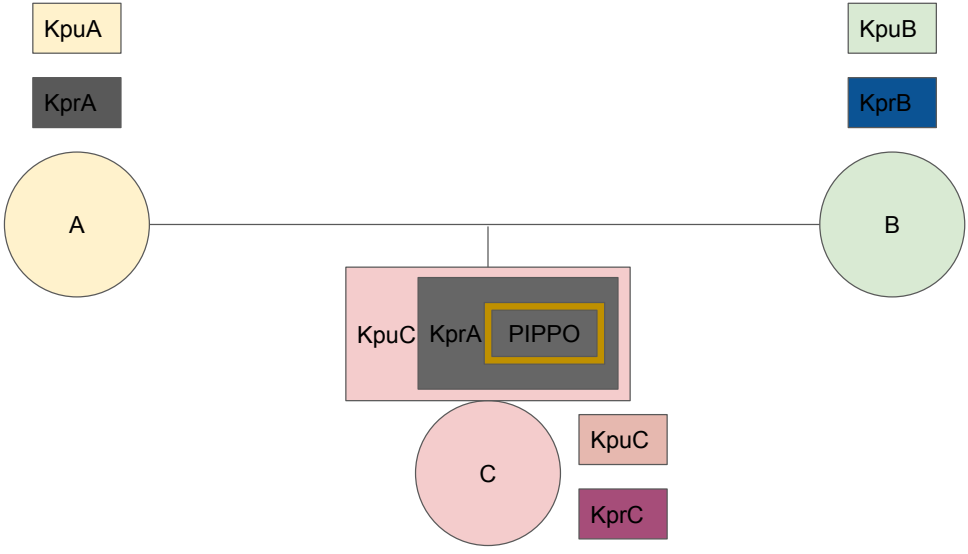

KpuA
KprA
A
KprA
PIPPO
KpuB
KprB
B
C
KpuC
KprC

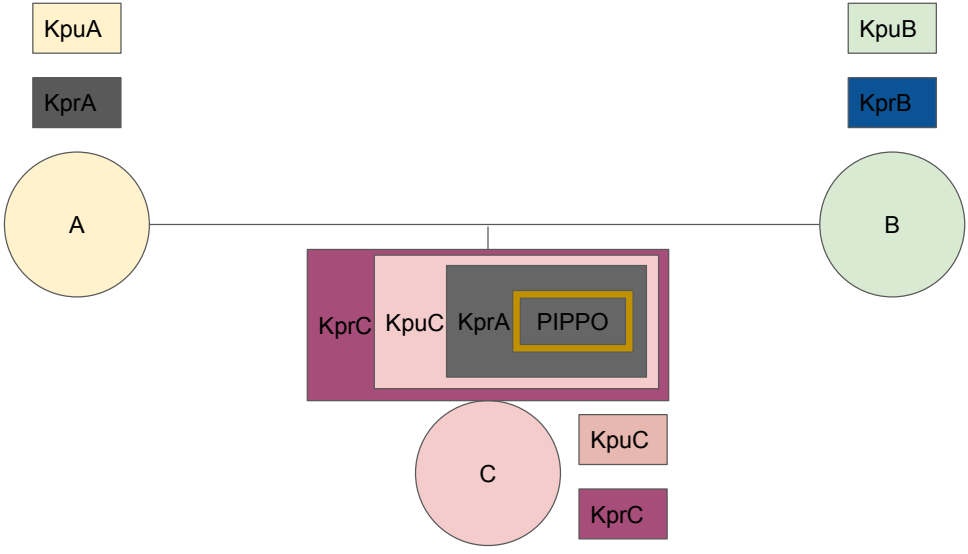

KpuA
KprA
KprA
PIPPO
A
KpuB
KprB
B
KpuB?
C
KpuC
KprC

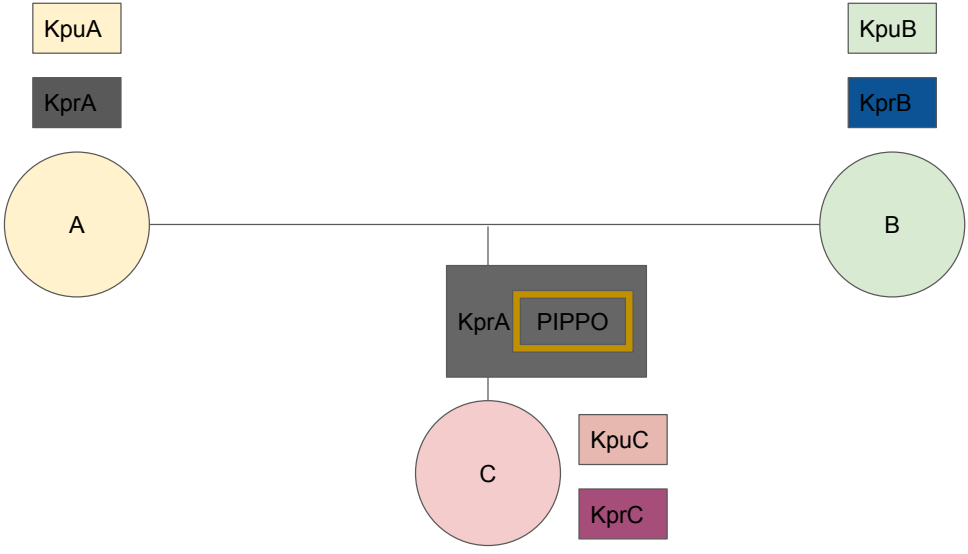

KpuA
KprA
KprA
PIPPO
A
KpuC
KpuB
KprB
B
C
KpuC
KprC

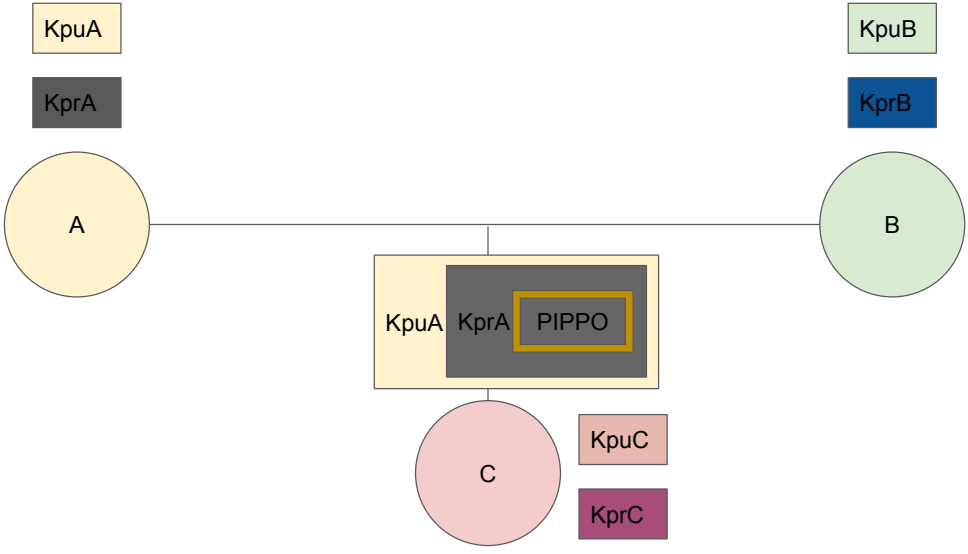

KpuA
KprA
KpuB
KprB
KpuC
KprA
PIPPO
A
B
C
KpuC
KprC

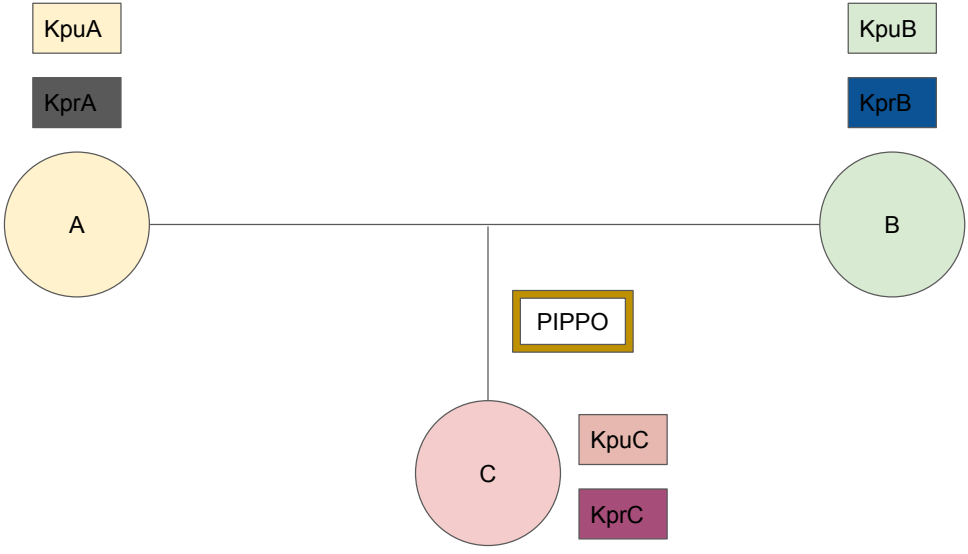

KpuA
KprA
A
KpuC
KprA
PIPPO
KpuB
KprB
B
C
KpuC
KprC

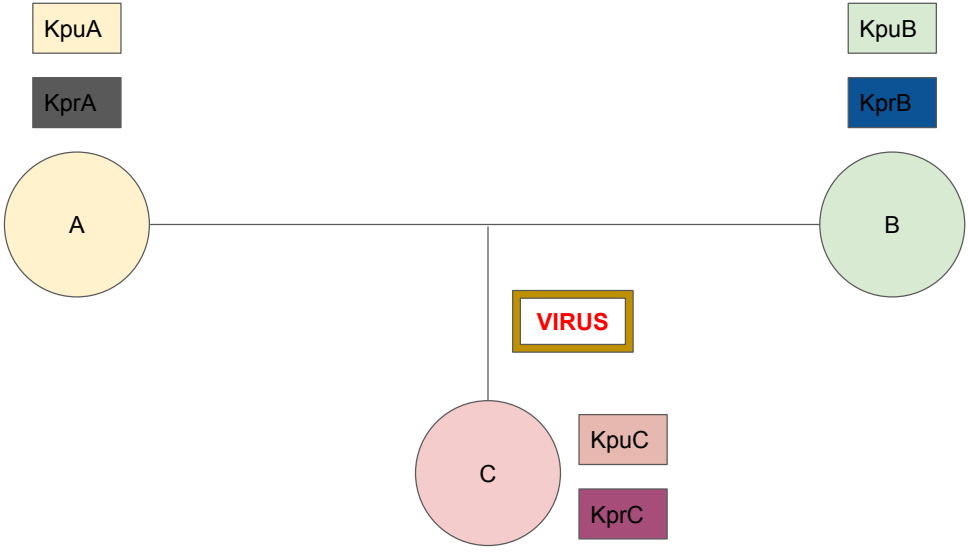

KpuA
KprA
KpuB
KprB
A
B
KpuC
KprA
PIPPO
C
KpuC
KprC

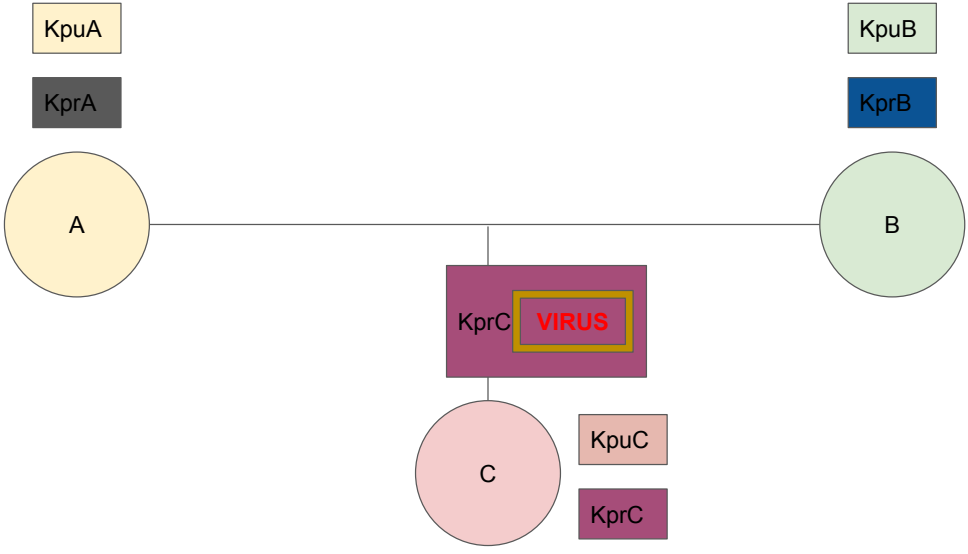

KpuA
KprA
KpuB
KprB
A
B
KprC
KpuC
KprA
PIPPO
C
KpuC
KprC

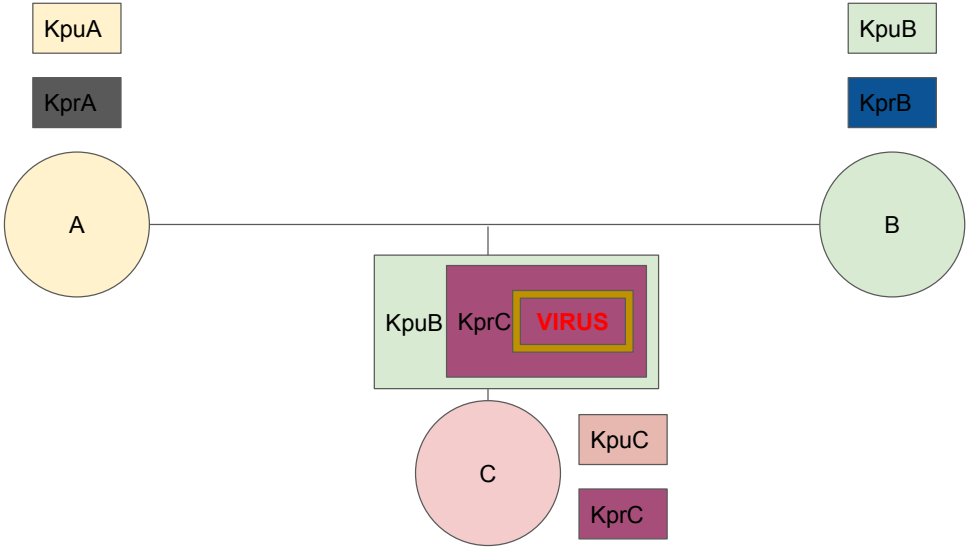

KpuA
KprA
A
KpuB
KprB
B
KprA
PIPPO
C
KpuC
KprC

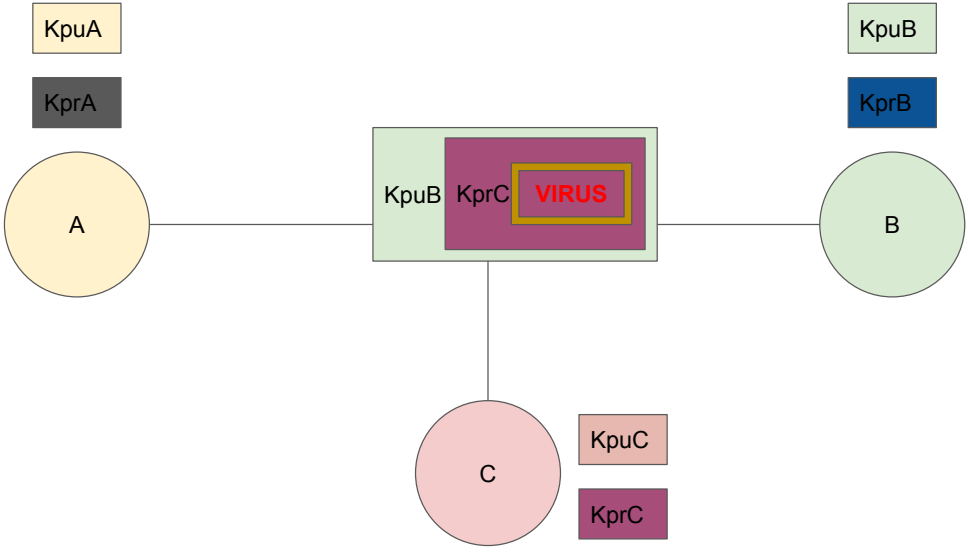

KpuA
KprA
KpuB
KprB
A
B
KpuA
KprA
PIPPO
C
KpuC
KprC

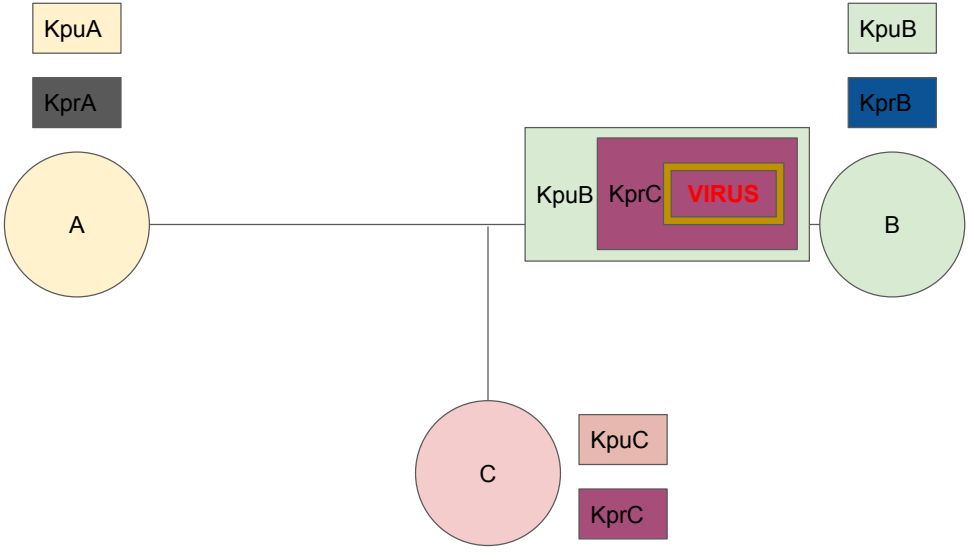

KpuA
KprA
KpuB
KprB
A
B
PIPPO
C
KpuC
KprC

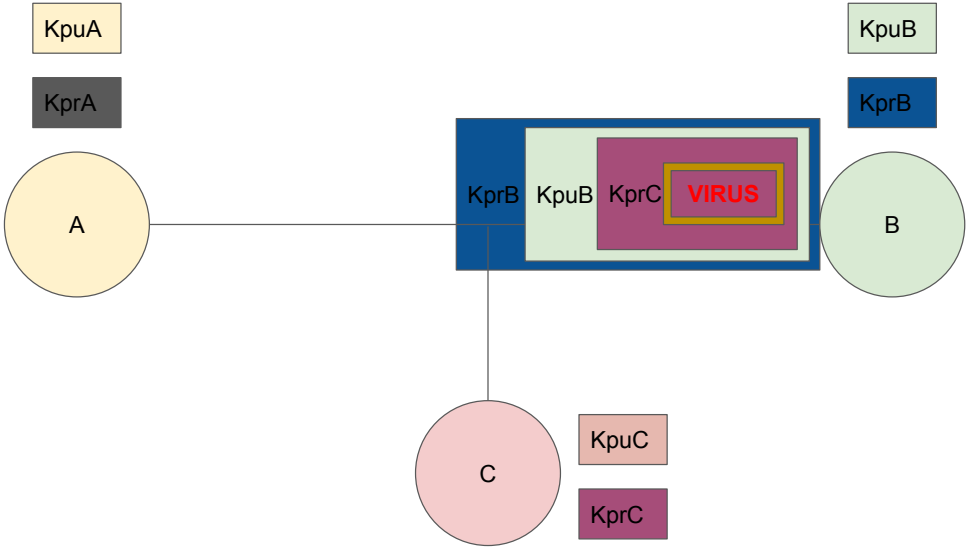

KpuA
KprA
KpuB
KprB
A
B
VIRUS
C
KpuC
KprC

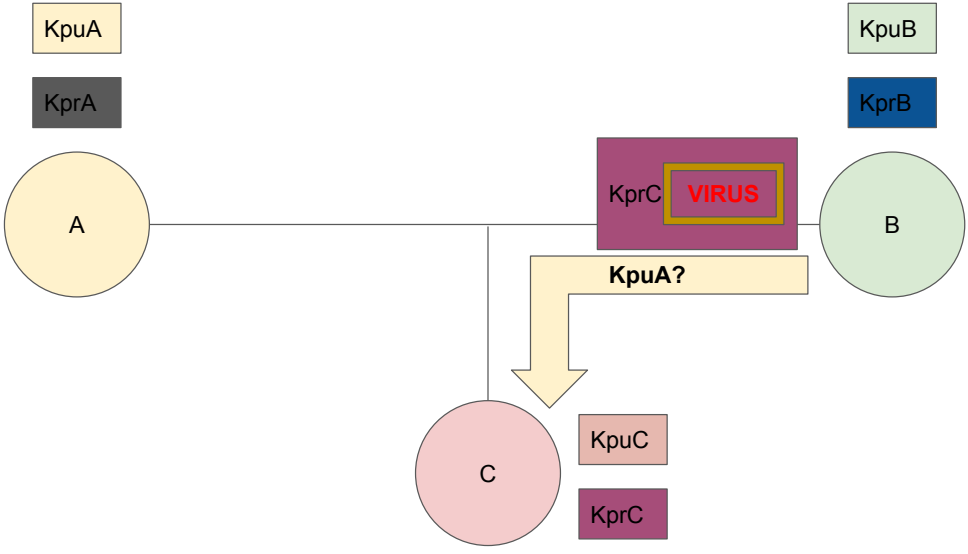

KpuA
KprA
KpuB
KprB
A
B
KprC
VIRUS
C
KpuC
KprC

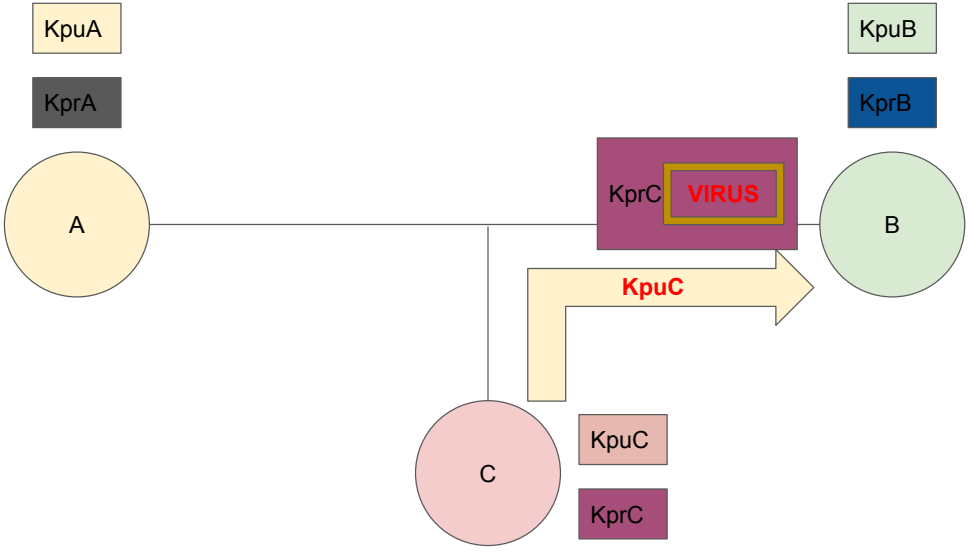

KpuA
KprA
KpuB
KprB
A
B
KpuB
KprC
VIRUS
C
KpuC
KprC

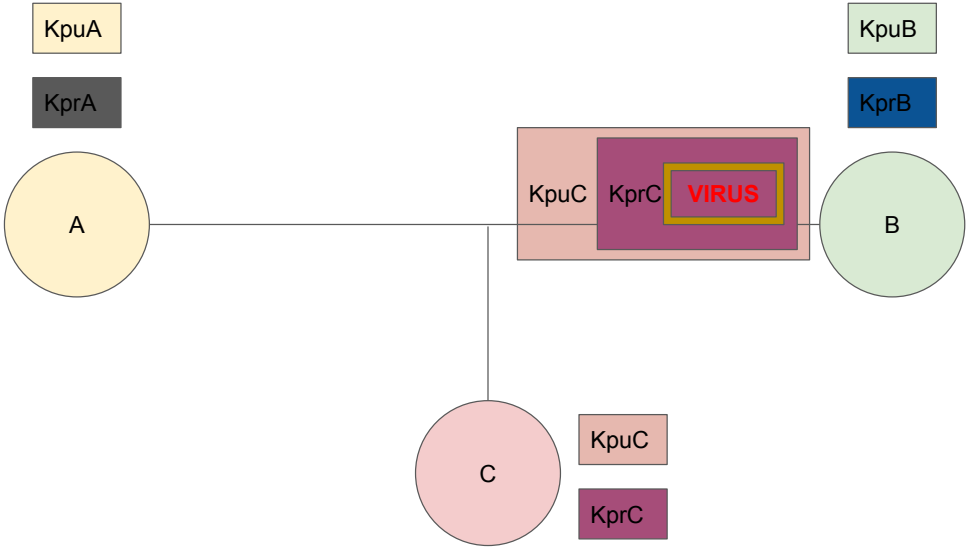

KpuA
KprA
A
KpuB
KprC
VIRUS
KpuB
KprB
B
C
KpuC
KprC

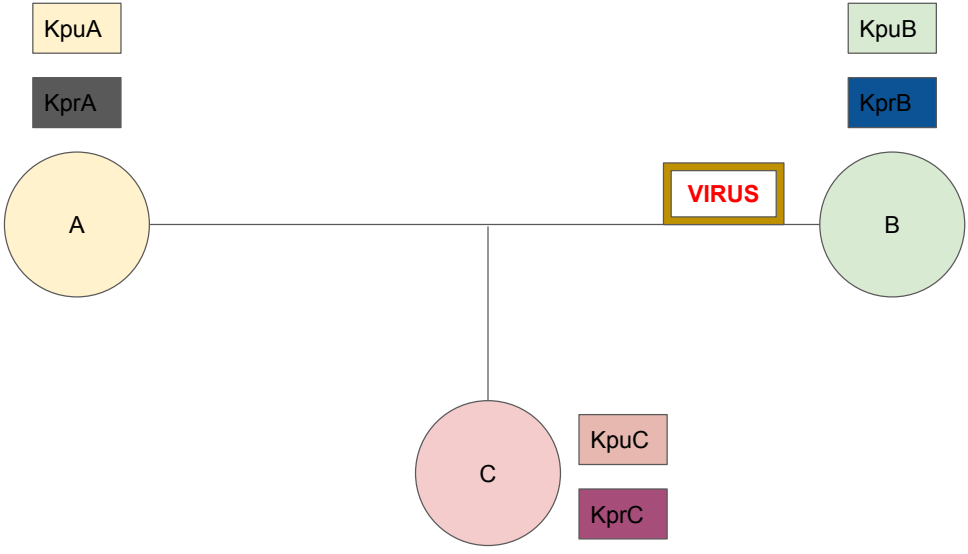

KpuA
KprA
KpuB
KprB
A
KpuB
KprC
VIRUS
B
C
KpuC
KprC


KpuA
KprA
KpuB
KprB
KprB
KpuB
KprC
VIRUS
A
B
C
KpuC
KprC


KpuA
KprA
KpuB
KprB
A
KprC
VIRUS
B
KpuA?
C
KpuC
KprC

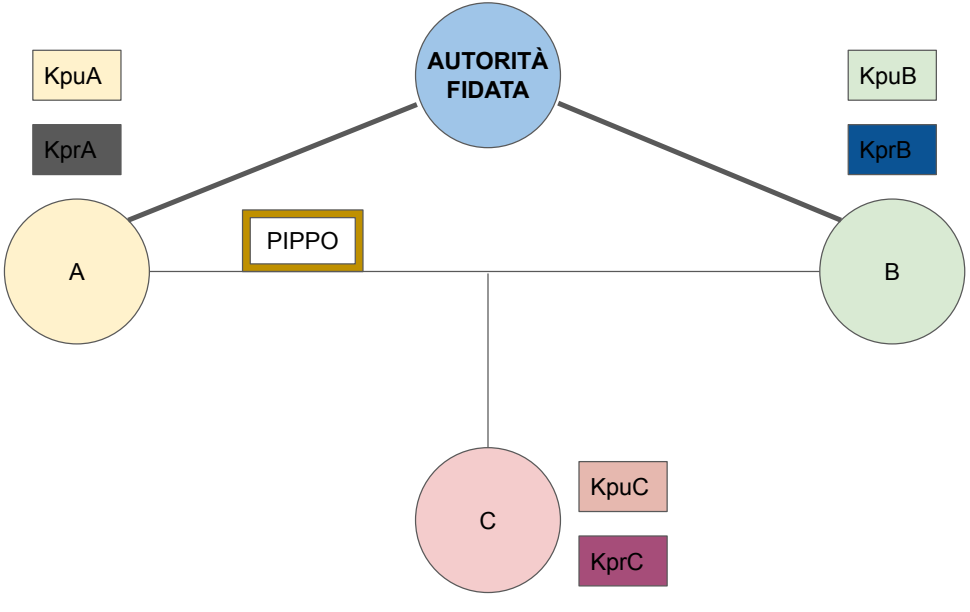

KpuA
KprA
KpuB
KprB
A
KprC
VIRUS
B
KpuC
C
KpuC
KprC

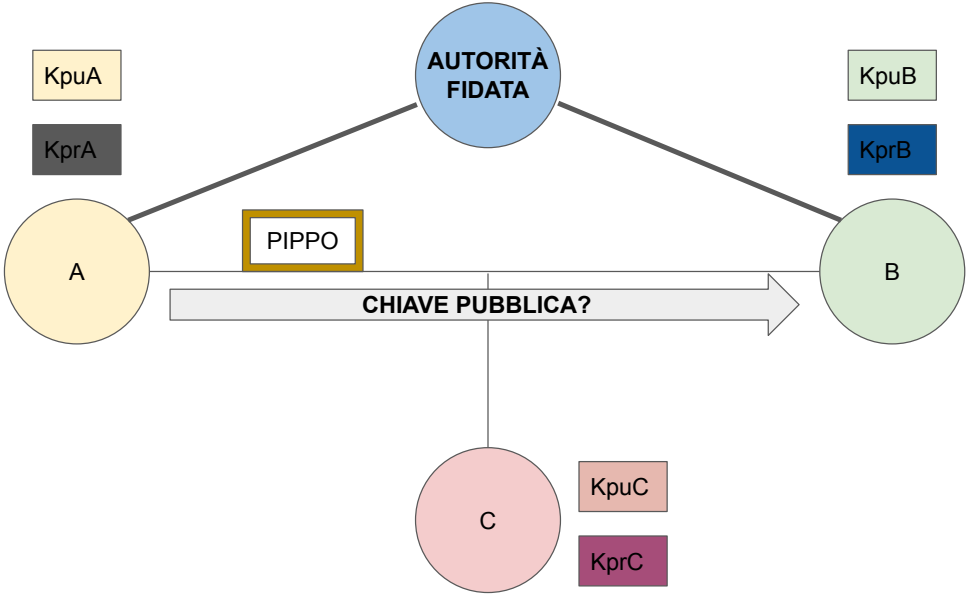

KpuA
KprA
KpuB
KprB
KpuC
KprC
VIRUS
A
B
C
KpuC
KprC

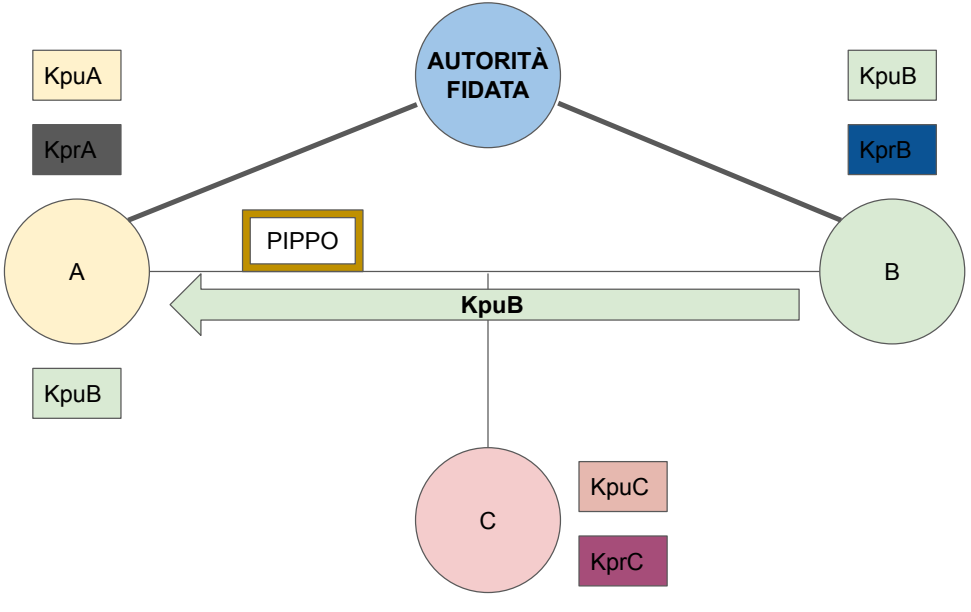

KpuA
KprA
KpuB
KprB
A
VIRUS
B
C
KpuC
KprC

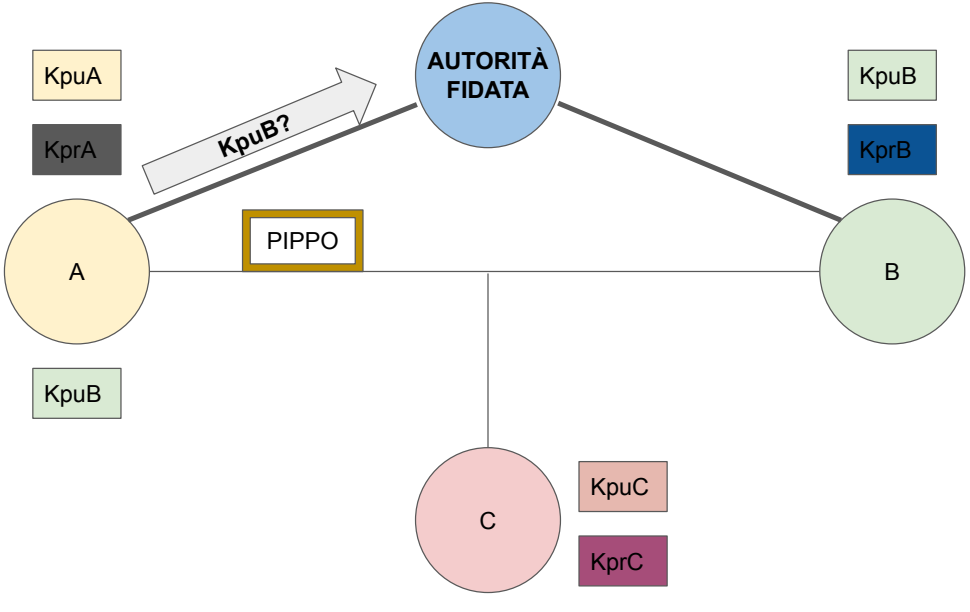
SOLUZIONE

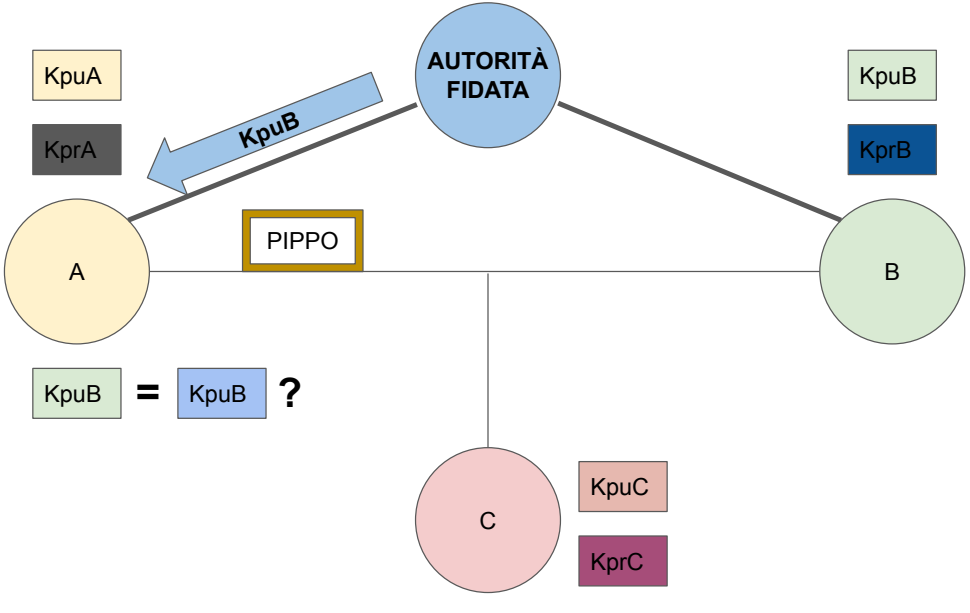
certificato digitale

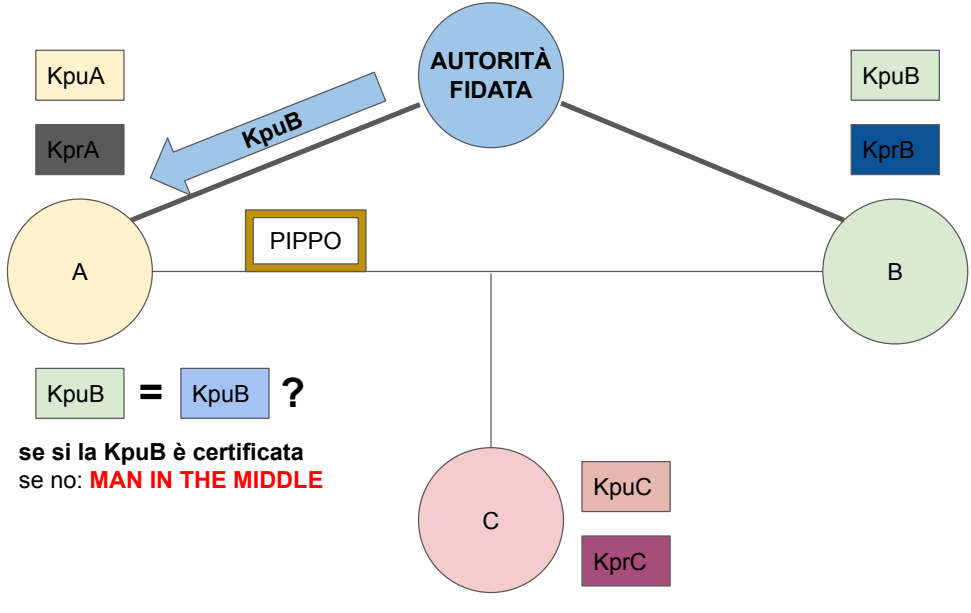

AUTORITÀ FIDATA
KpuA
KprA
KpuB
KprB
A
PIPPO
B
C
KpuC
KprC


AUTORITÀ FIDATA
KpuA
KprA
KpuB
KprB
A
PIPPO
B
CHIAVE PUBBLICA?
C
KpuC
KprC

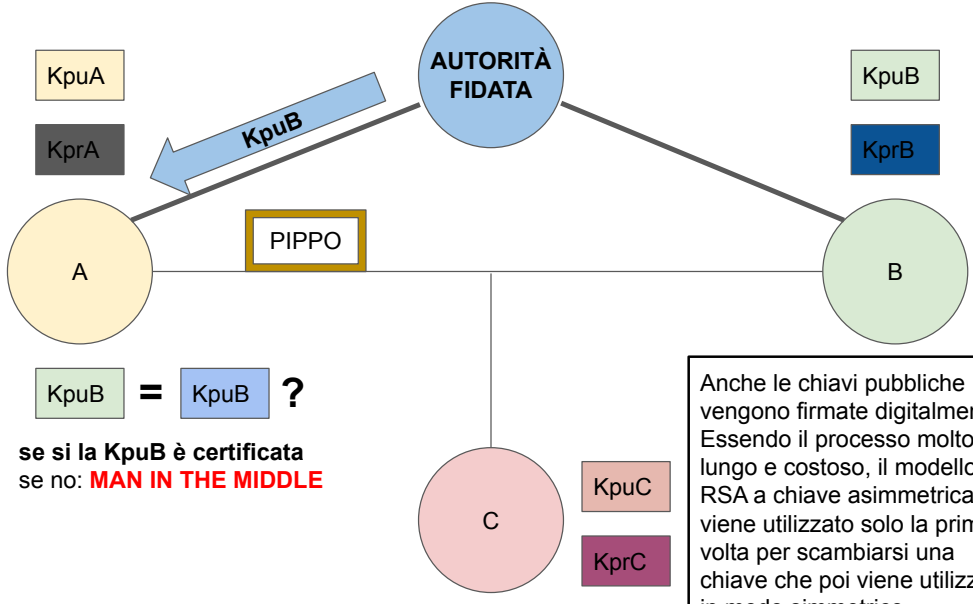

AUTORITÀ FIDATA
KpuA
KprA
KpuB
KprB
A
B
PIPPO
KpuB
KpuB
C
KpuC
KprC


AUTORITÀ FIDATA
KpuA
KprA
KpuB?
KpuB
KprB
PIPPO
A
B
KpuB
C
KpuC
KprC


AUTORITÀ FIDATA
KpuA
KprA
KpuB
KpuB
KprB
PIPPO
A
B
KpuB = KpuB ?
C
KpuC
KprC



- **se si la KpuB è certificata**
- se no: **MAN IN THE MIDDLE**



- **se si la KpuB è certificata**
- se no: **MAN IN THE MIDDLE**

Anche le chiavi pubbliche vengono firmate digitalmente. Essendo il processo molto lungo e costoso, il modello RSA a chiave asimmetrica viene utilizzato solo la prima volta per scambiarsi una chiave che poi viene utilizzata in modo simmetrico.