Seminario sulla Crittografia

Corso: T.A.R.I
Prof.: Giulio Concas
Autore: Ivana Turnu

Crittografia

- Cos'è la crittografia
- Le tecniche più usate
- La firma digitale

Cos'è la crittografia

- Per garantire la riservatezza di un messaggio si usa normalmente trasformarlo in modo tale che solo le persone abilitate siano in grado di recuperare il messaggio originale.

- Esiste a tale scopo, una serie di algoritmi e di tecniche di protezione dei dati che garantiscono buoni livelli di sicurezza per tutti i diversi aspetti riguardanti la "secure comunication".

Le tecniche più usate

- Chiave segreta (simmetrica)
- Chiave pubblica (asimmetrica)

Crittografia a chiave segreta

- E' la forma più tradizionale di crittografia, nella quale una sola chiave viene usata per cifrare e decifrare i messaggi.
- **Vantaggi**:
  - E' generalmente più veloce di un sistema a chiave pubblica.
  - A parità di lunghezza della chiave, i sistemi a chiave simmetrica sono più sicuri.

Crittografia a chiave segreta

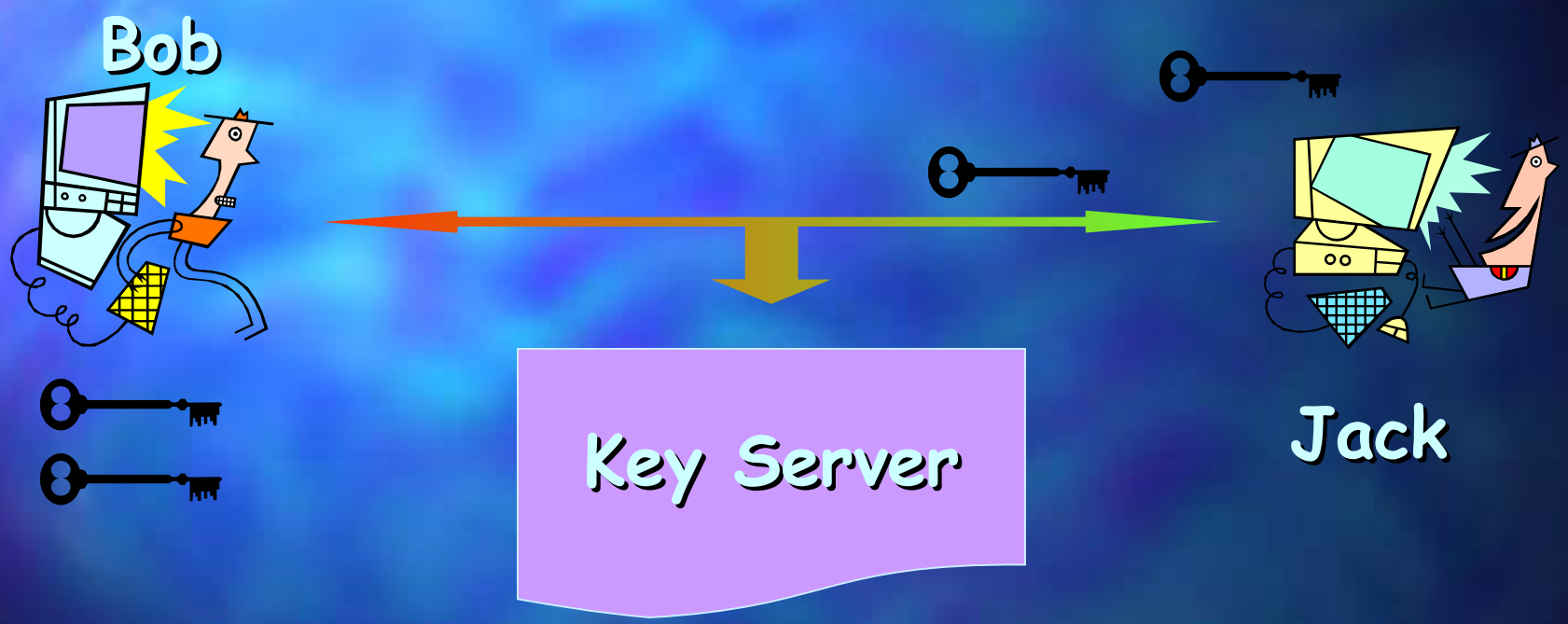
- **Svantaggi**:
  - Problemi nel key management. Il mittente e il ricevente devono trovare un mezzo sicuro per scambiarsi la chiave in modo che nessuno la scopra
  - In un sistema a chiave segreta per ogni possibile coppia di utenti deve esistere una chiave, per cui per n utenti occorrono $n(n-1)/2$

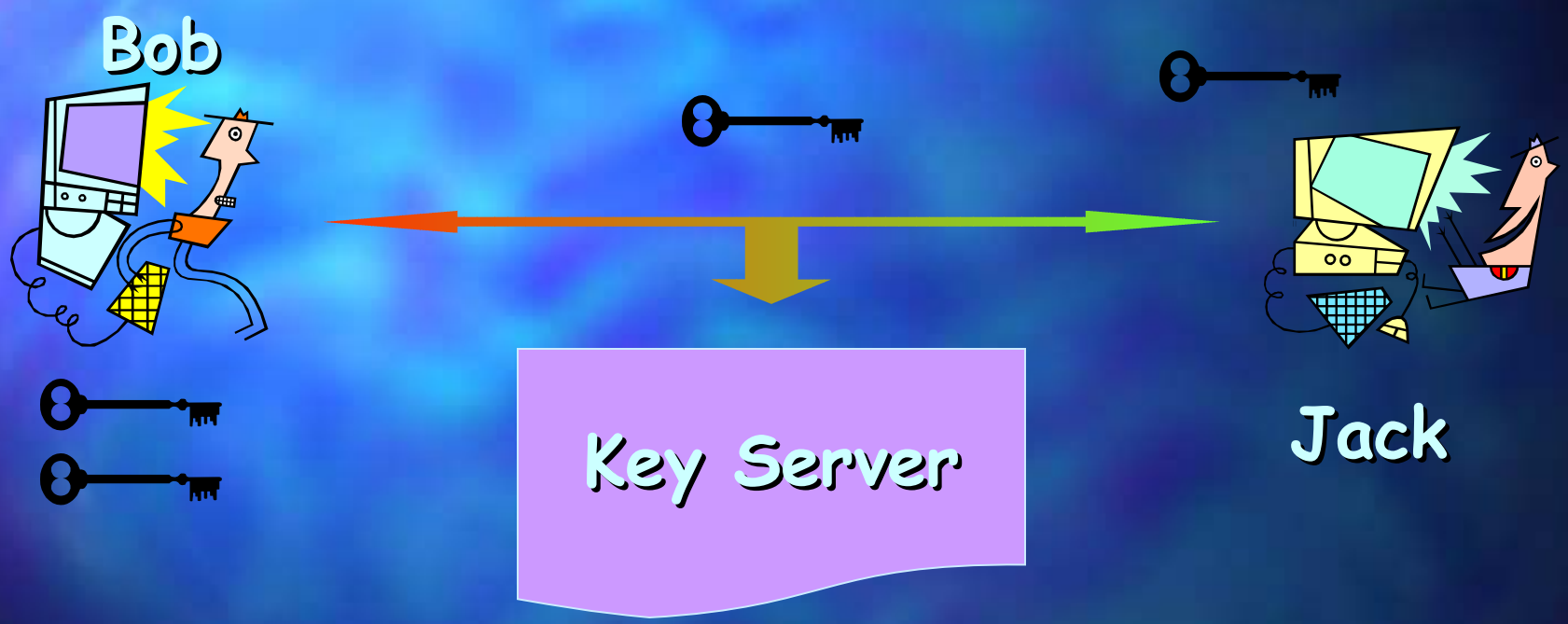
Crittografia a chiave pubblica

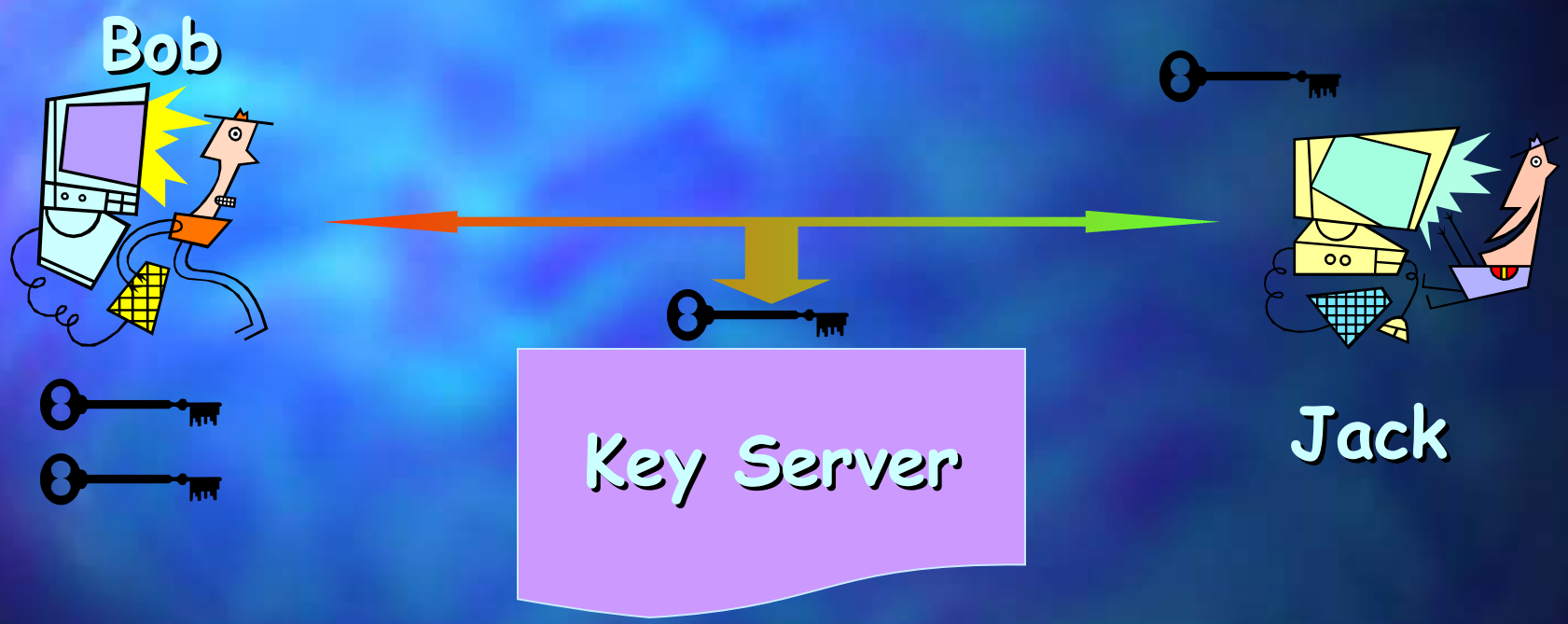
- In questo sistema, ogni persona possiede due chiavi, una pubblica e una privata. Tutti possono accedere alla prima mentre la seconda deve rimanere segreta.

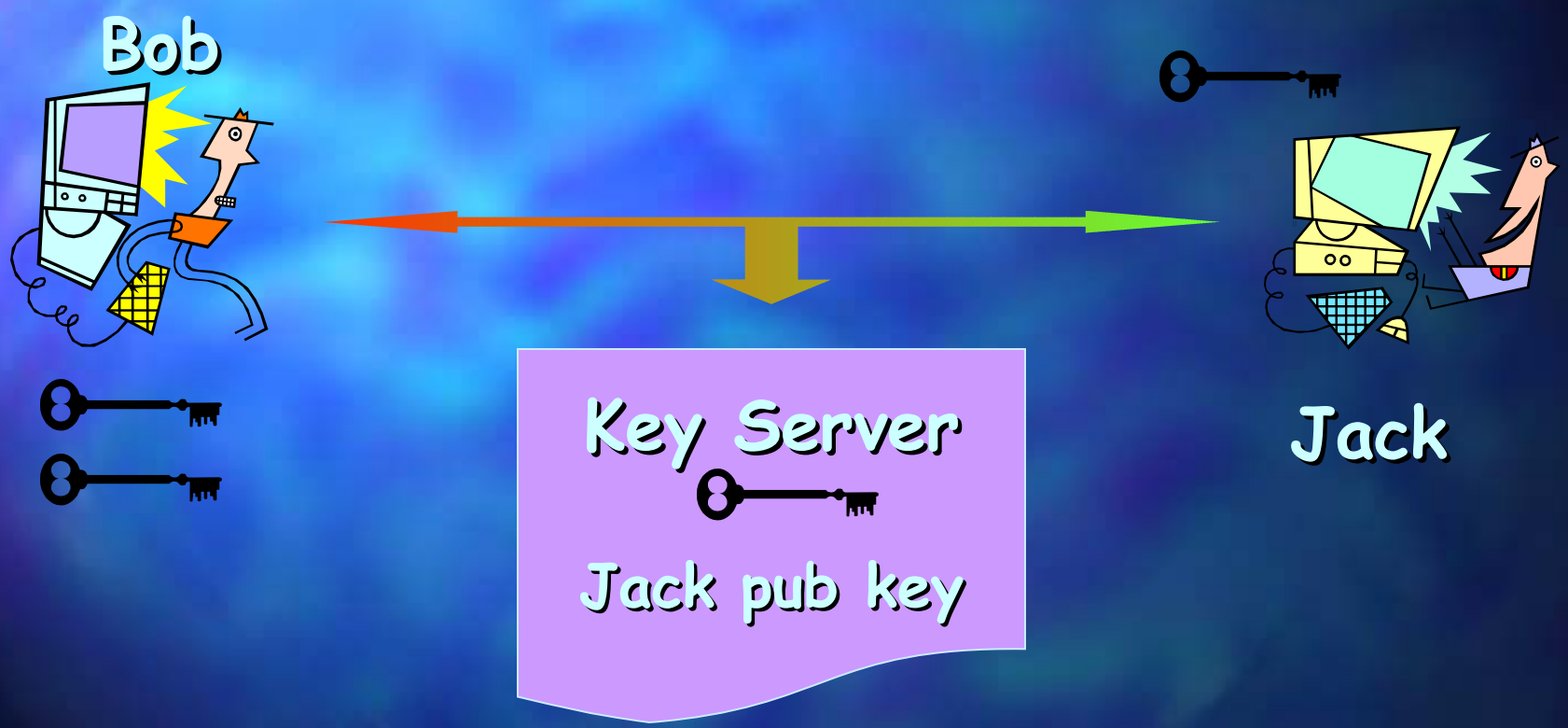
- La chiave pubblica viene usata per cifrare il messaggio mentre quella privata per decifrarlo.

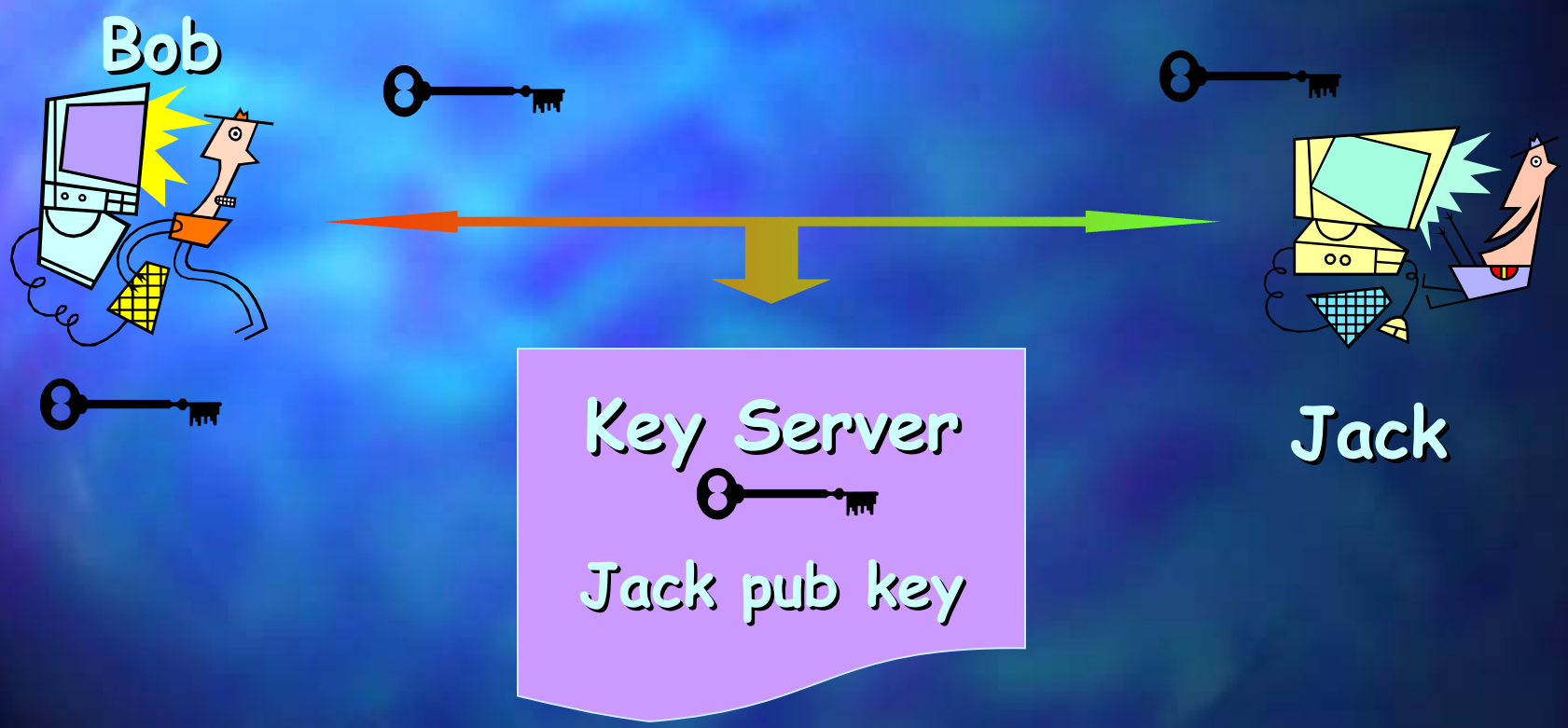

Bob
Key Server
Jack

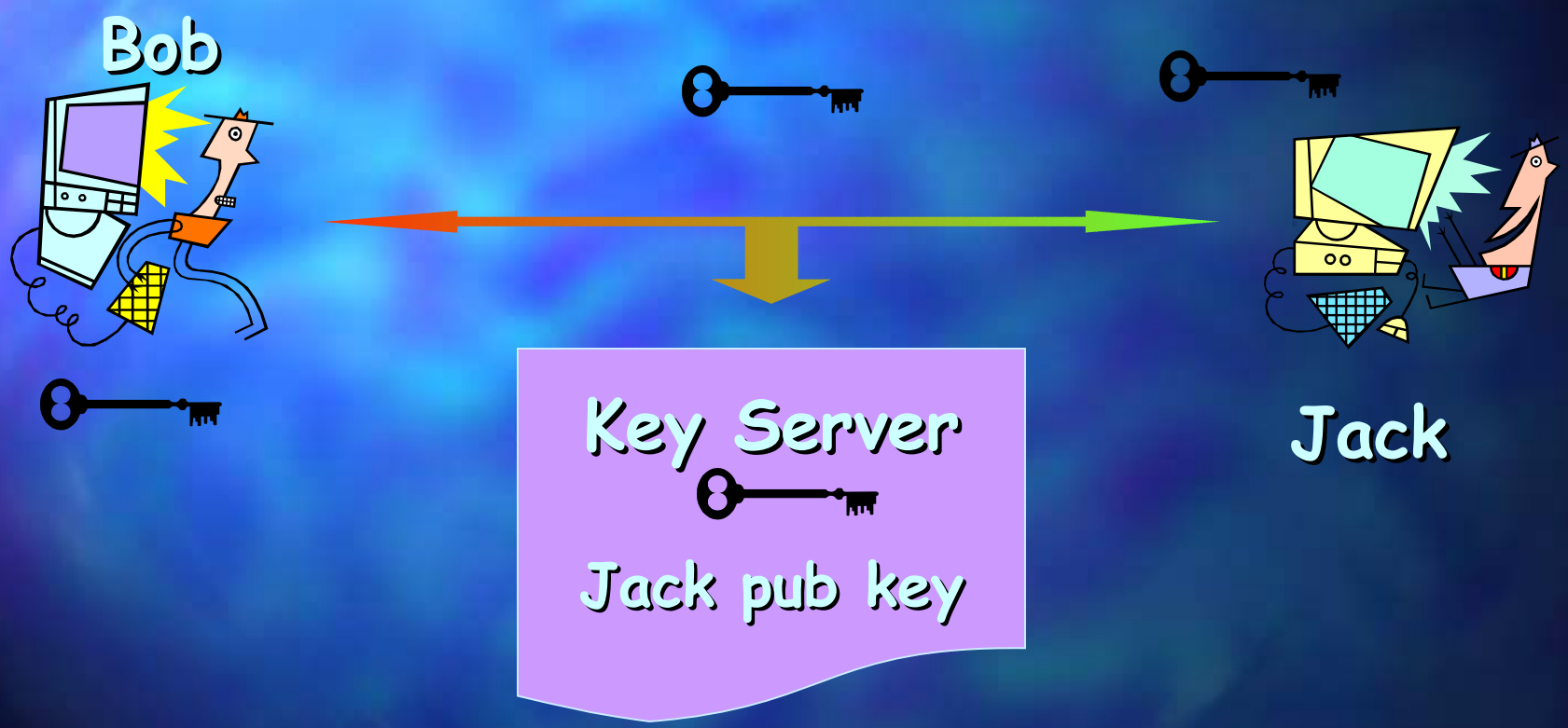

Bob
Key Server
Jack

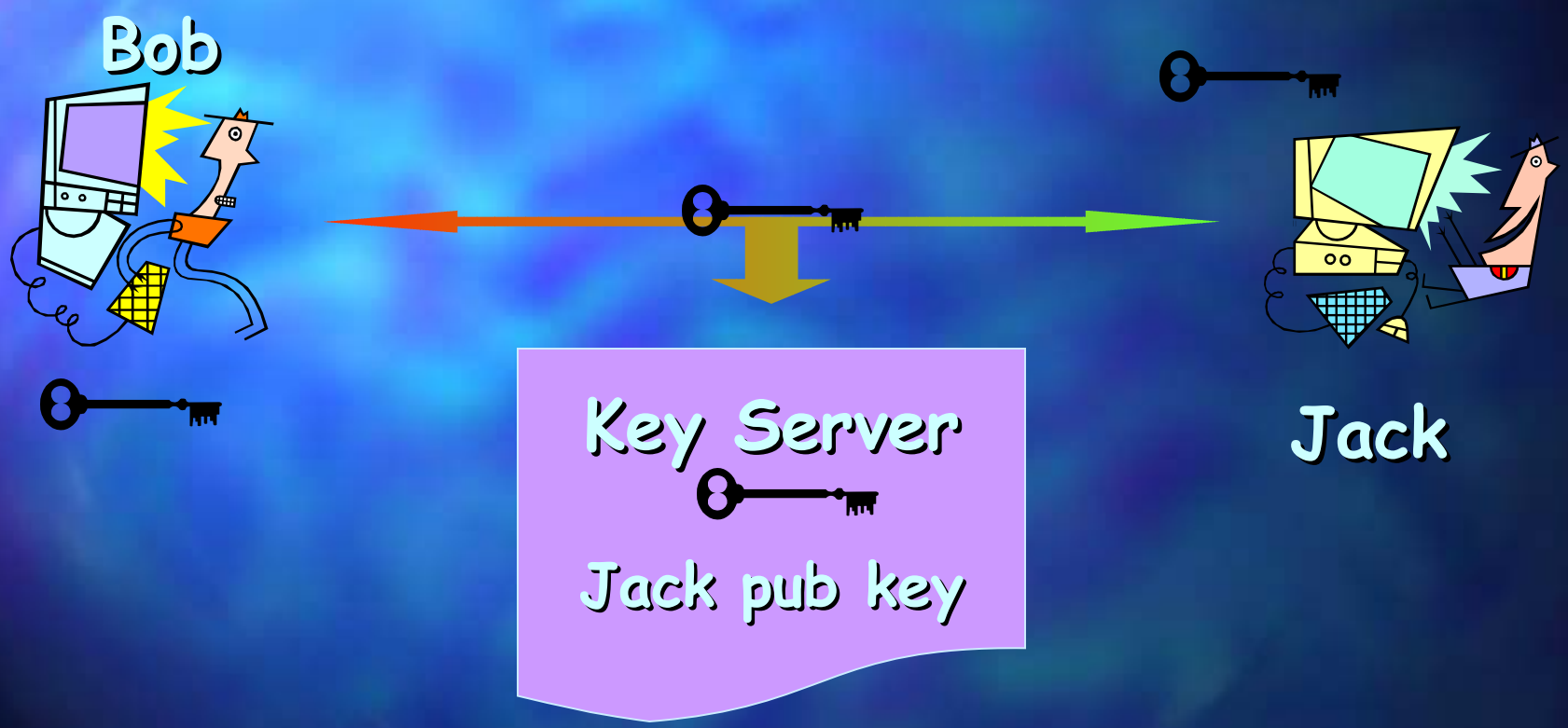

Bob
Key Server
Jack

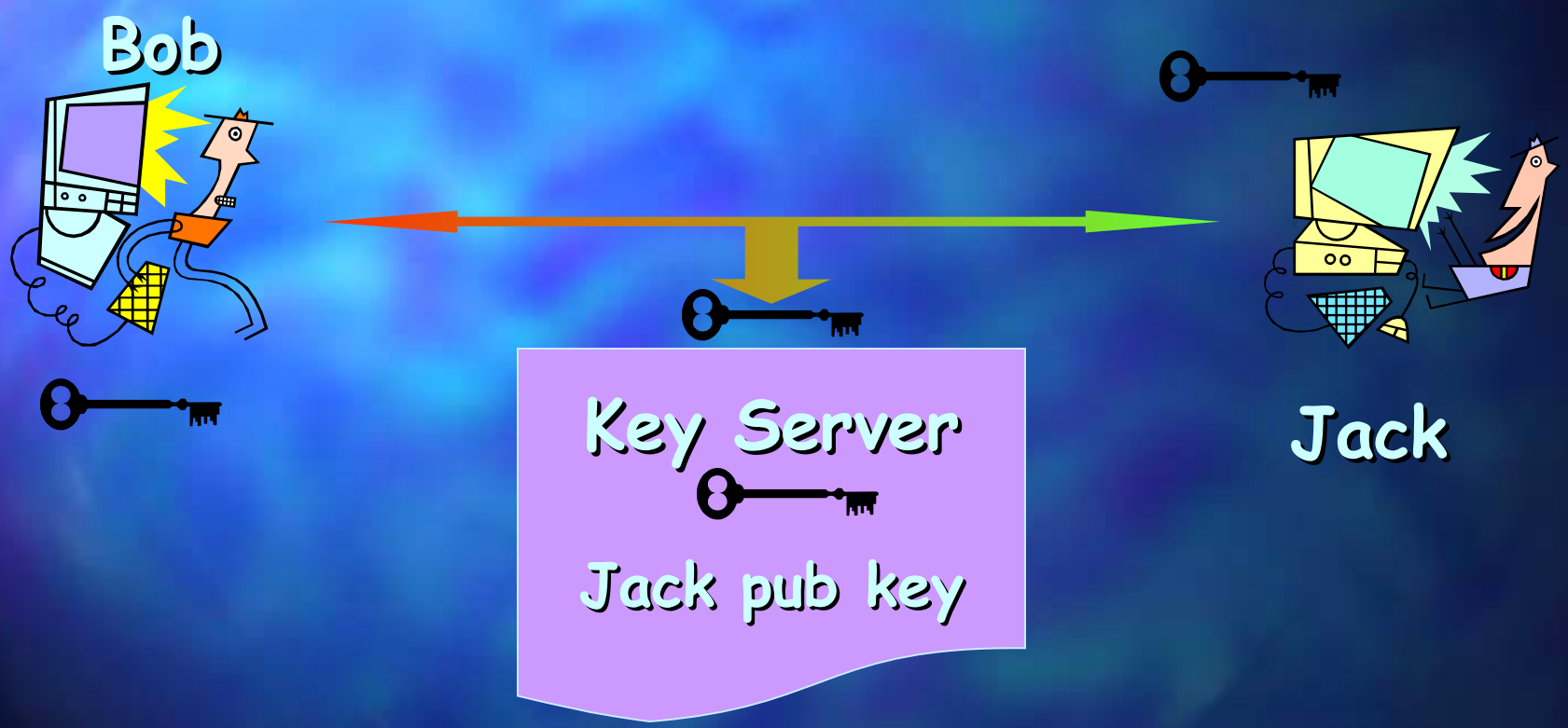

Bob
Key Server
Jack

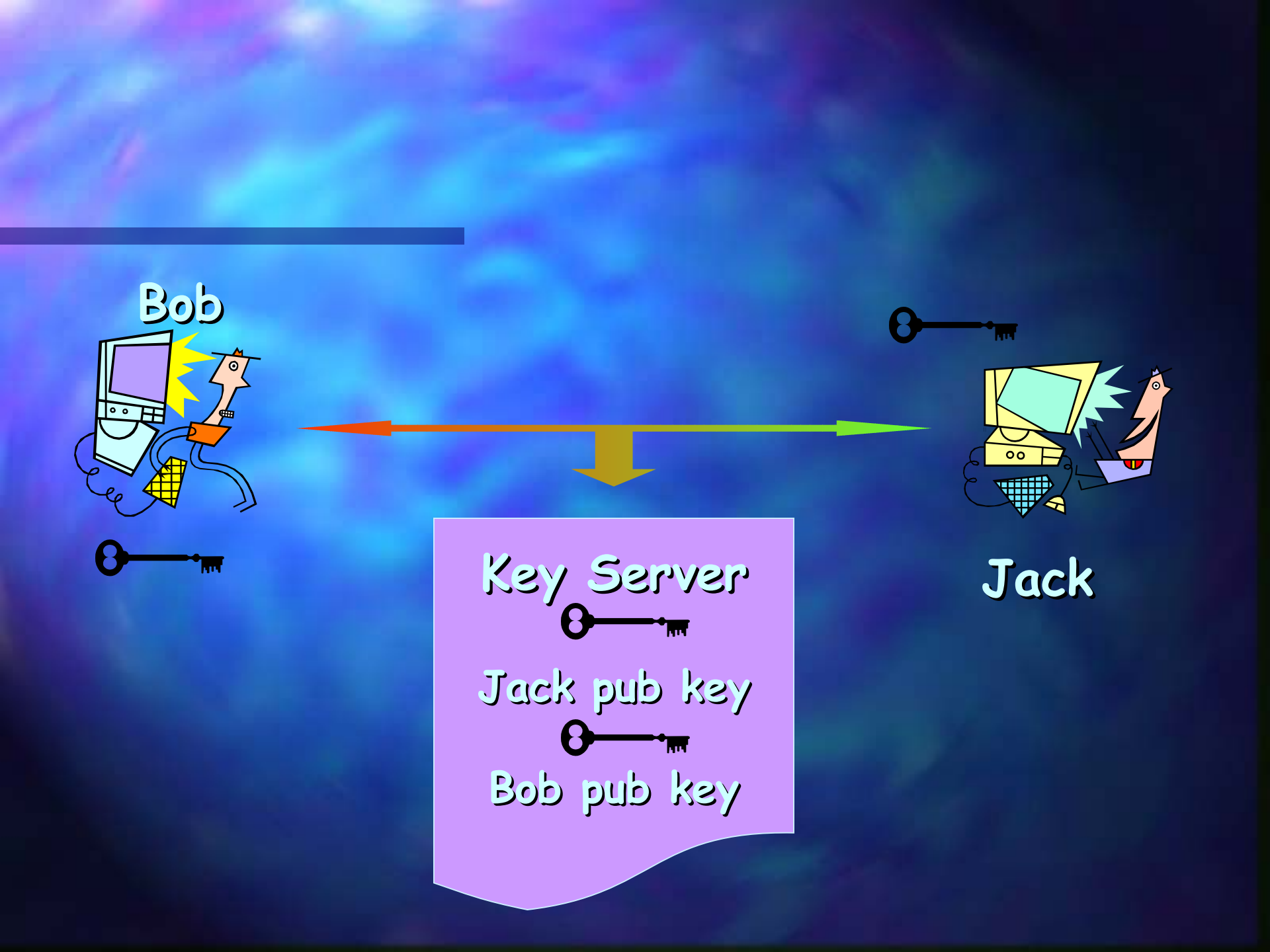

Bob
Key Server
Jack pub key
Jack

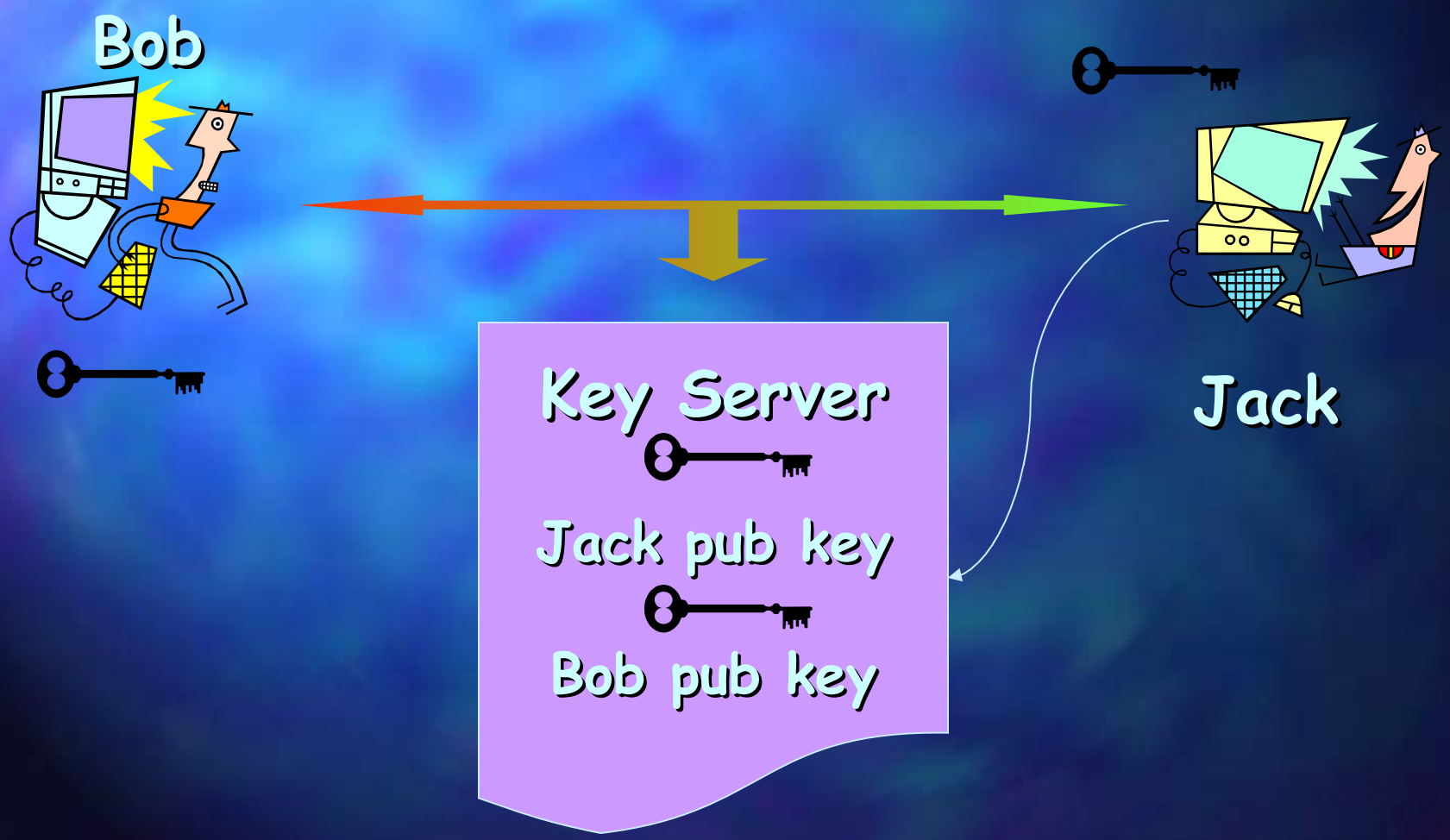

Bob
Key Server
Jack pub key
Jack

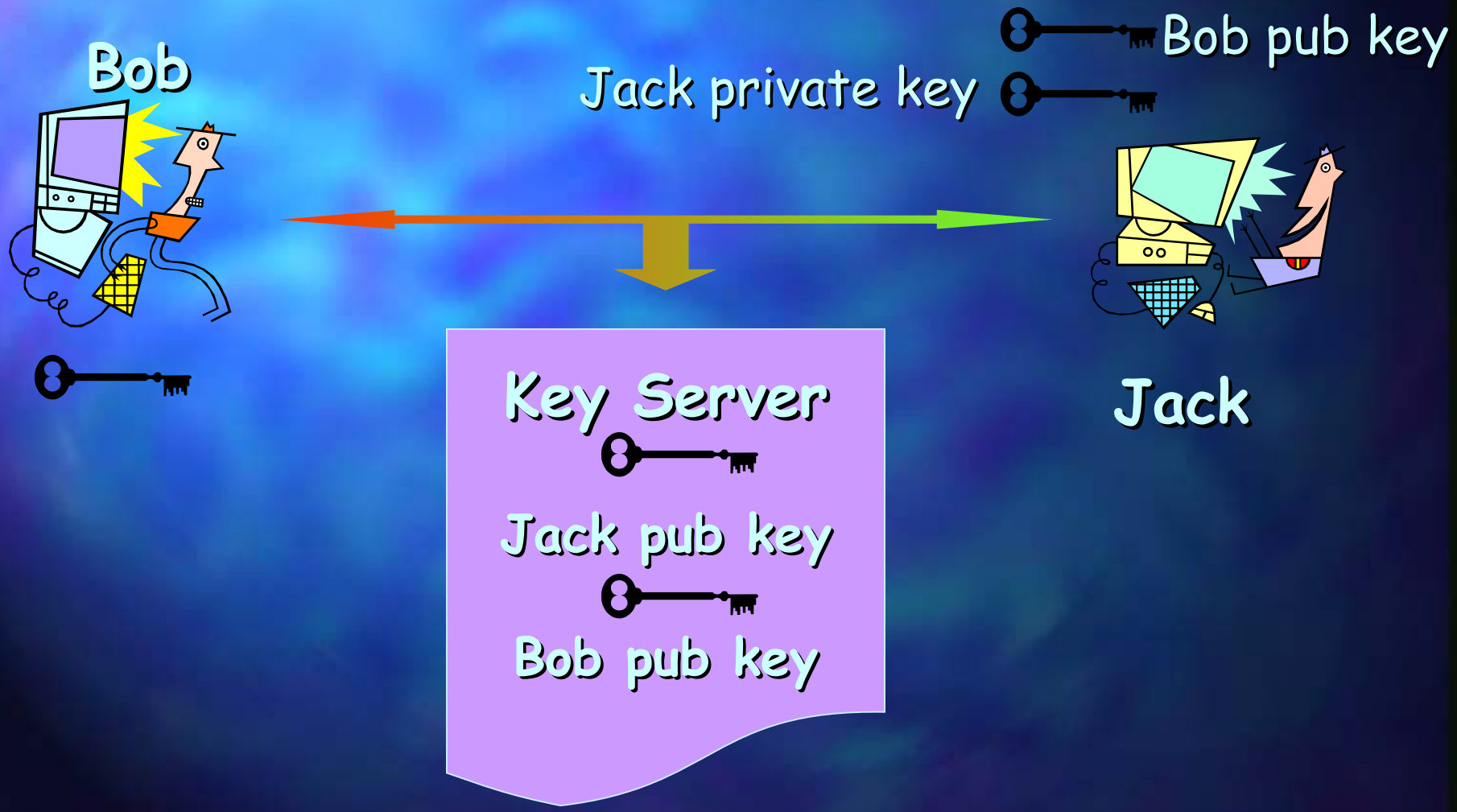

Bob
Key Server
Jack pub key
Jack

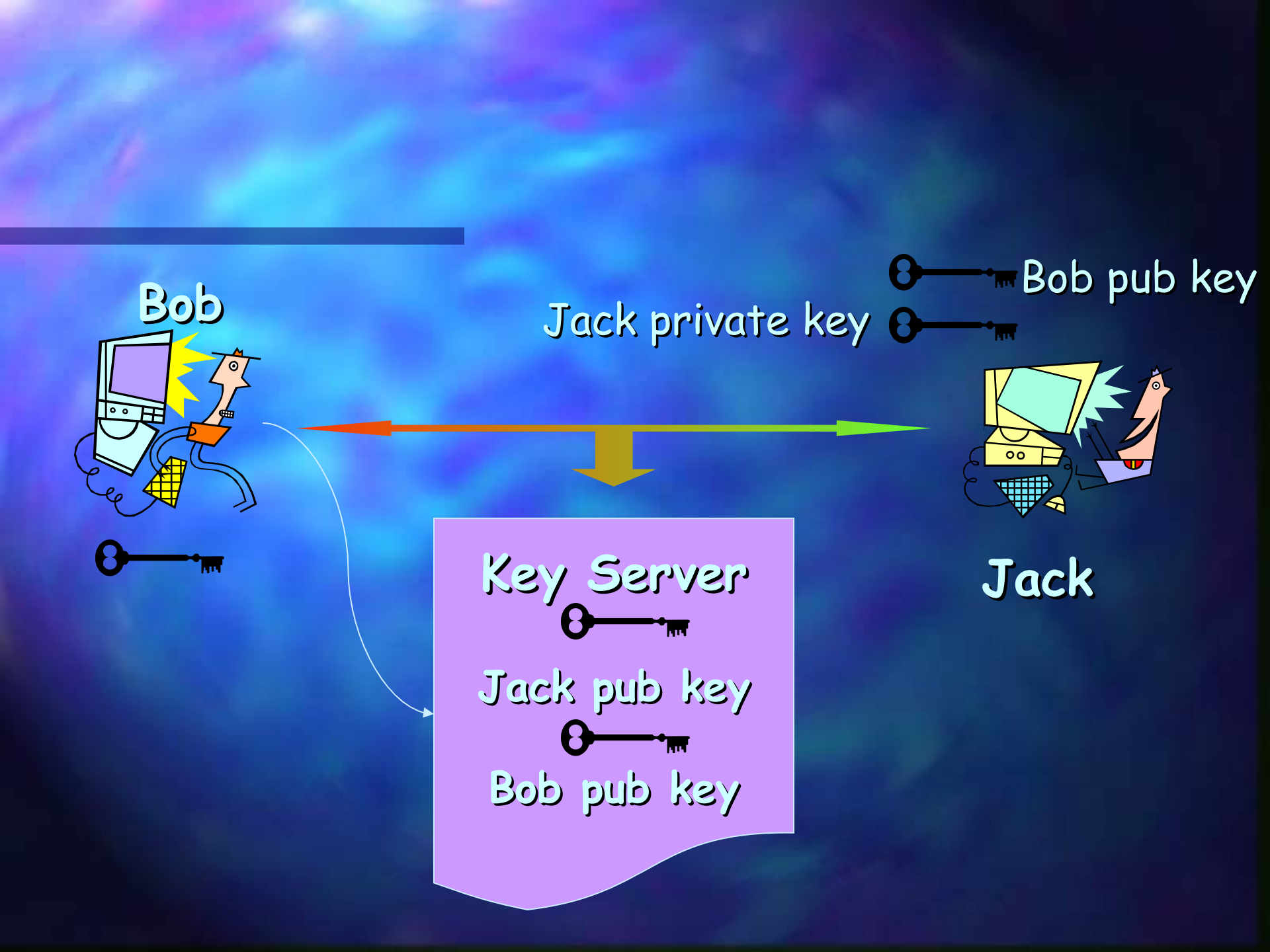

Bob
Key Server
Jack pub key
Jack

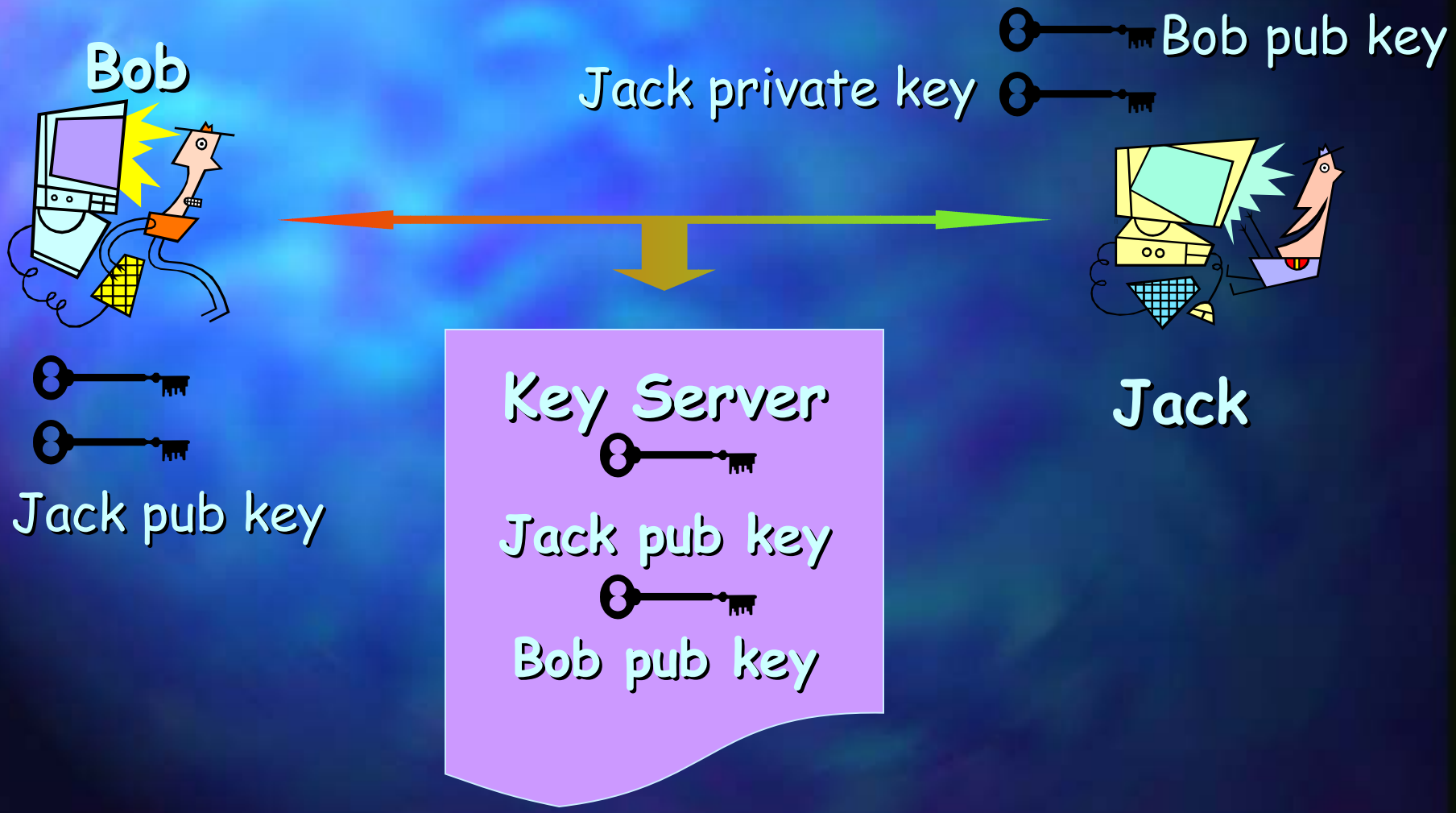

Bob
Key Server
Jack pub key
Jack


Bob
Key Server
Jack pub key
Bob pub key
Jack


Bob
Jack
Key Server
Jack pub key
Bob pub key


Bob
Bob pub key
Jack private key
Jack
Key Server
Jack pub key
Bob pub key


Bob
Jack private key
Bob pub key
Jack
Key Server
Jack pub key
Bob pub key


Bob
Jack pub key
Jack private key
Bob pub key
Jack
Key Server
Jack pub key
Bob pub key


Bob
Jack private key
Bob pub key
Jack
Jack pub key
?

Cos' è l' RSA

- L' RSA è il crittosistema a chiave pubblica che permette sia la cifratura che la firma digitale (autenticazione). L' RSA fu sviluppato nel 1977 da Ron Rivest, Adi Shamir e Leonard Adleman. La sigla RSA deriva dalle iniziali dei loro autori.

Come funziona l' RSA ?

- Si prendono due numeri primi grandi, p e q.
- Si calcola il prodotto n=pq detto modulo.
- Si sceglie un numero e minore di n e primo rispetto a (p-1)(q-1) .
- Si sceglie un altro numero d=[k(p-1)(q-1)+1]/e con k tale per cui d sia un numero intero.
- I valori e e d prendono il nome di esponente pubblico e privato.
- La chiave pubblica è la coppia (n,e) .
- La chiave privata è la coppia (n,d) .

Cifrare con RSA

- Supponiamo che Bob voglia mandare un messaggio m a Jack. Egli crea un messaggio cifrato $c = m^e \bmod n$ dove (n,e) è la chiave pubblica di Jack.
- Jack per decifrare il messaggio si calcola $m = c^d \bmod n$
- La relazione tra e e d assicura che Jack possa recuperare correttamente il messaggio m.
- Poiché solo Jack conosce d, è l'unico in grado di decifrare il messaggio.

Esempio numerico

- Si prendono due numeri primi, 11 e 7.
- Si calcola il prodotto $n=(p \times q)=77$ detto modulo.
- Si sceglie un numero e minore di n e primo rispetto a $(p-1)(q-1)=60$, prendiamo ad esempio $e=13$.
- La coppia (n,e) costituisce la chiave pubblica, ovvero $(77, 13)$.
- Si sceglie un altro numero $d=[k(p-1)(q-1)+1]/e$ con k tale per cui d sia un numero intero, per $k=8$ abbiamo $d=37$.
- La coppia (n,d) costituisce la chiave privata, ovvero $(77, 37)$.

Criptazione del messaggio

Ciao → $67^{13} \bmod 77$ → 67

Criptazione del messaggio

Ciao → $105^{13} \bmod 77$ →

67

7

Criptazione del messaggio

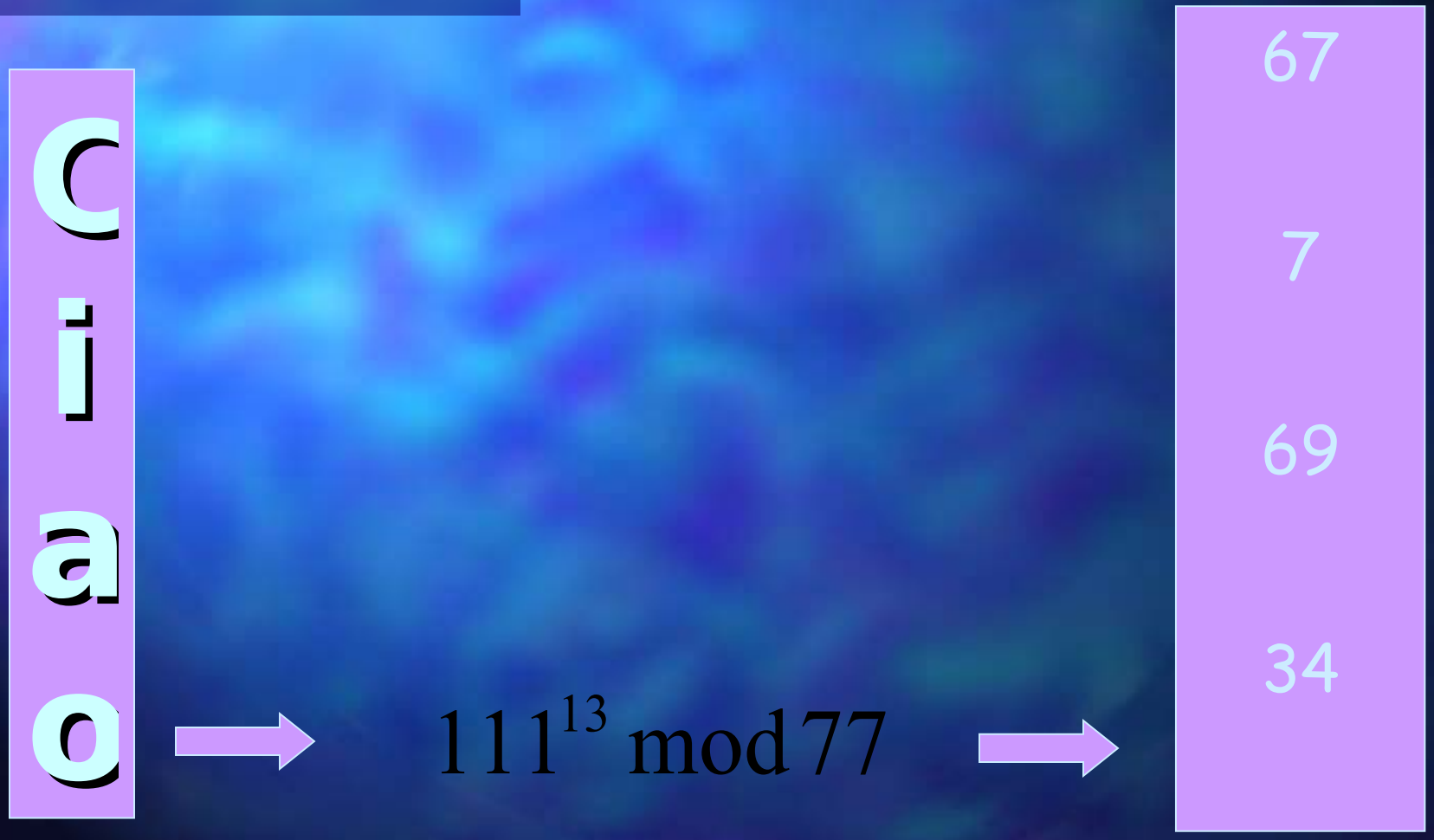
Ciao → $97^{13} \bmod 77$ →

67

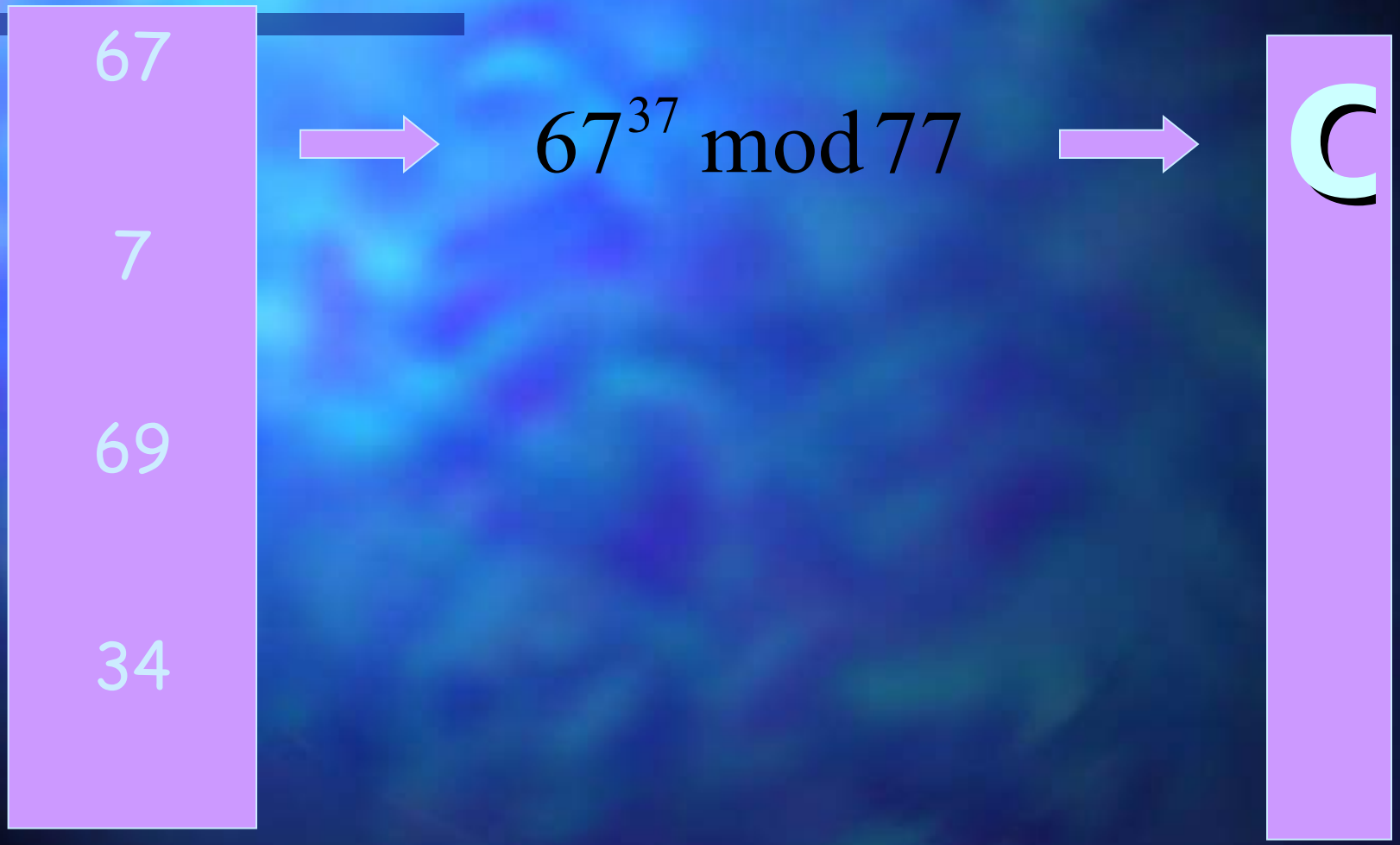
7

69

Criptazione del messaggio

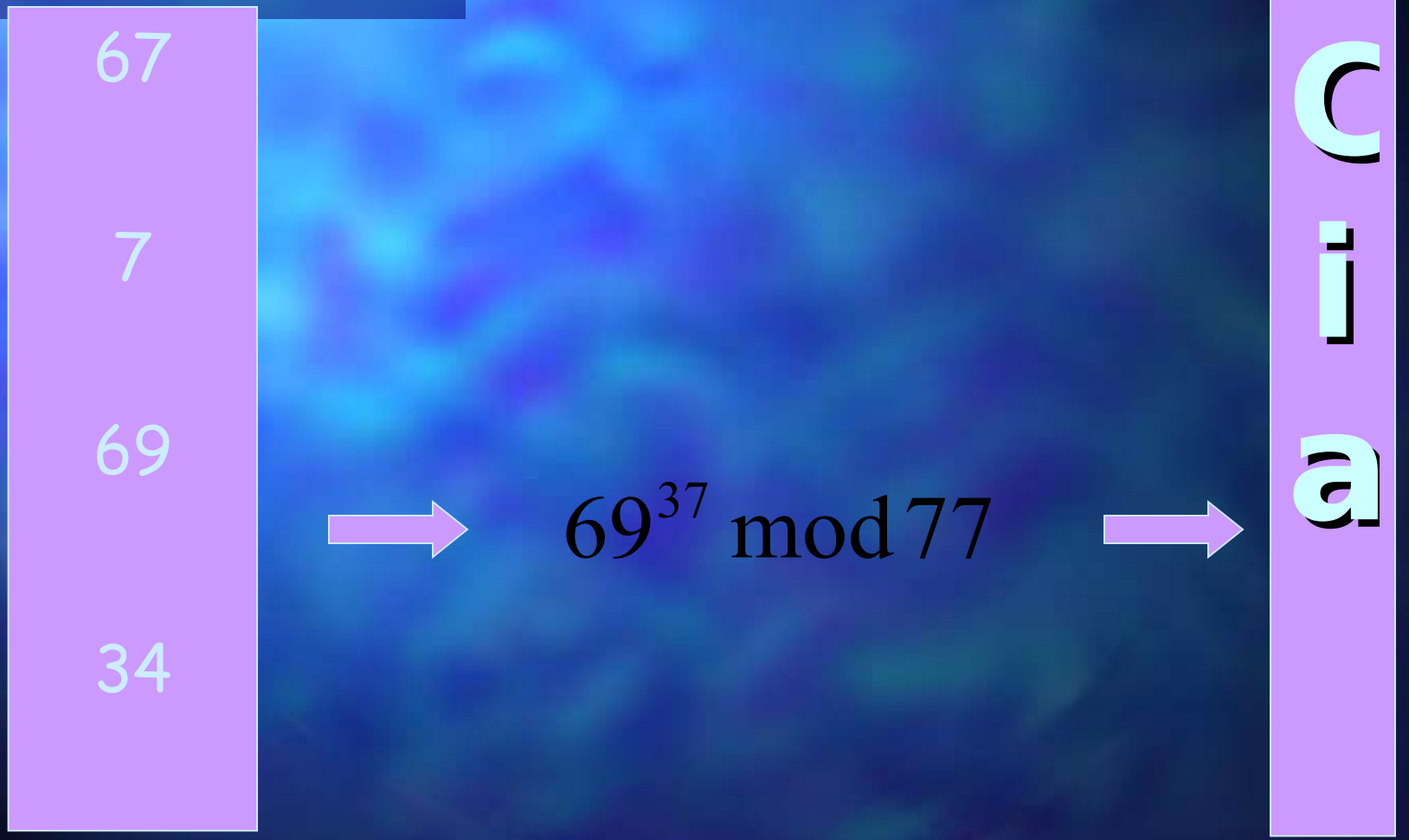


Decriptazione del messaggio



Decriptazione del messaggio

criptazione del messagg



Decriptazione del messaggio

67

7

69

34

$34^{37} \bmod 77$

C

i

a

o

Funzioni “One-Way”

- La sicurezza dell’RSA si basa sul fatto che la funzione di cifratura $c = m^e \bmod n$ è un funzione “one-way” che è computazionalmente difficile da invertire.
- Solo conoscendo la fattorizzazione di n è possibile trovare il valore delle chiavi.
- La sicurezza dell’ RSA dipende dal problema di fattorizzare grandi numeri.

Funzioni "One-Way"

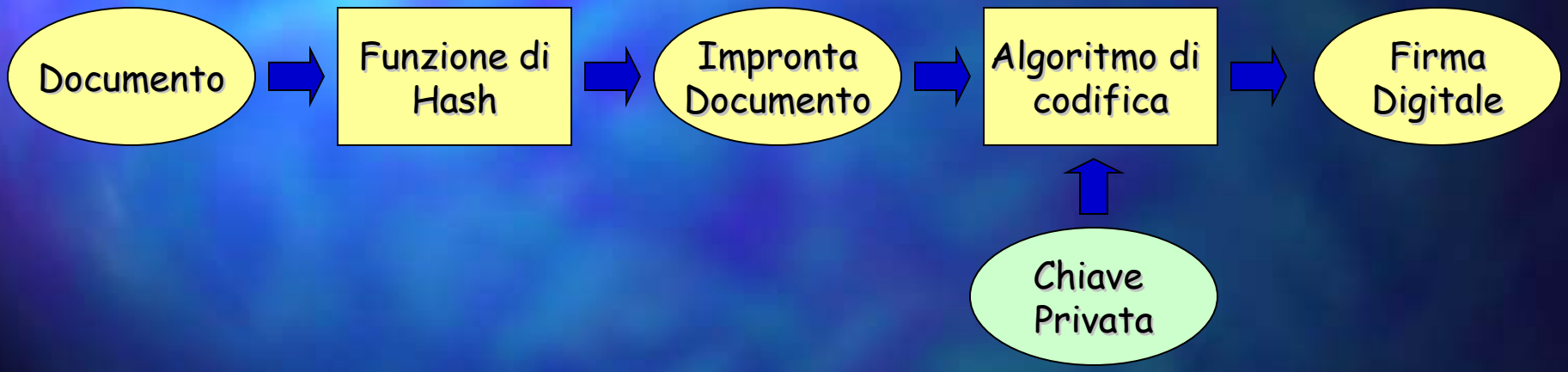
- Fattorizzare un numero di 664 bit richiede 10^{23} passi usando gli algoritmi più efficienti; per cui disponendo di una rete costituita da un milione di computer, ciascuno di loro capace di eseguire un milione di passi al secondo sarebbero necessari 4000 anni. Se n fosse un numero a 1024 bit la stessa rete impiegherebbe 10^{10} anni.
- Non è impossibile decifrare un testo cifrato con il crittosistema RSA, ma piuttosto è computazionalmente difficile.

La firma digitale

- La firma digitale é un' informazione che viene aggiunta ad un documento informatico al fine di garantirne integrità e provenienza.
- Il processo di firma digitale richiede che l'utente effettui una serie di azioni preliminari:
  - La registrazione dell'utente presso un'Autorità di Certificazione (AC)
  - La generazione di una coppia di chiavi Ks e Kp
  - La certificazione della chiave pubblica Kp
  - La registrazione della chiave pubblica Kp

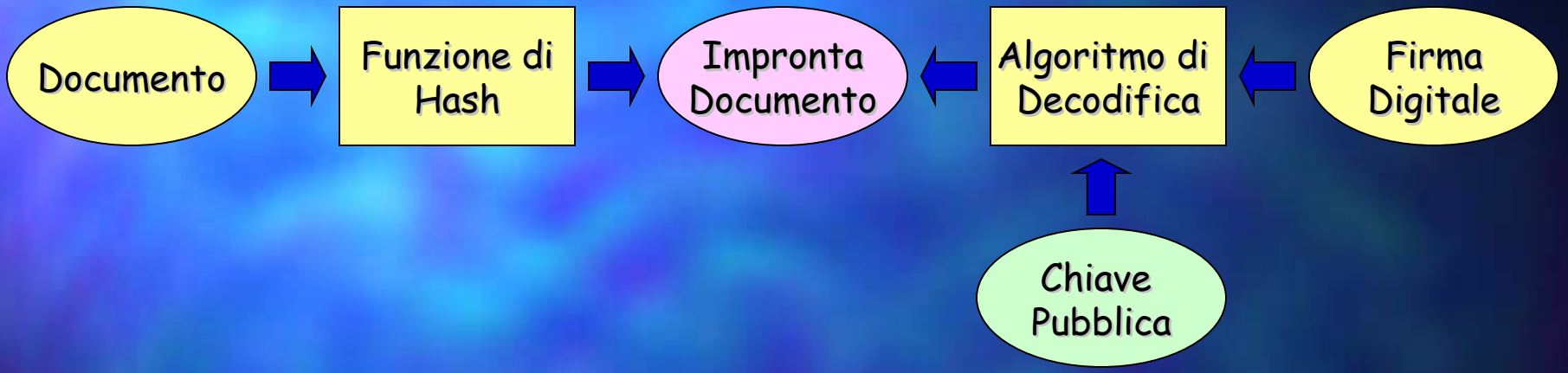
Generazione della firma digitale

La firma viene apposta, con il processo schematicamente mostrato in Figura , mediante una sequenza di tre operazioni:



- Generazione dell'impronta del documento da firmare
- Generazione della firma mediante cifratura dell'impronta
- Apposizione della firma al documento.

Verifica della firma digitale



L'operazione di verifica della firma digitale viene effettuata calcolando, con la medesima funzione di hash usata nella fase di sottoscrizione, il valore dell'impronta e controllando che il valore così ottenuto coincida con quello generato per decodifica della firma digitale stessa. La disponibilità del valore dell'impronta all'interno del messaggio semplifica l'operazione.

Vantaggi dei sistemi a chiave pubblica

- Il principale vantaggio è l'incremento di sicurezza, infatti la chiave privata non deve essere trasmessa o rivelata.
- Un altro vantaggio è che la firma digitale non può essere ripudiata (non - repudiation).
- Servono meno chiavi rispetto al sistema a chiave simmetrica, 2n invece di n(n-1)/2.

Se n=100 servono 200 chiavi invece di 4950.

Svantaggi dei sistemi a chiave pubblica

- Il principale svantaggio è la maggiore lentezza di cifratura rispetto ai sistemi a chiave simmetrica.
- Gli algoritmi asimmetrici necessitano di chiavi più lunghe, rispetto a quelli simmetrici, per raggiungere il medesimo grado di sicurezza teorico.

Protocollo SSL

- SSL sta per Secure Socket Layer (Netscape)
- Un client invia una richiesta ed il server risponde con il proprio certificato e le sue preferenze riguardo i metodi di cifratura.
- Il client genera una chiave master e la cifra usando la chiave pubblica del server, poi trasmette la chiave segreta al server.

Protocollo SSL

- Il server recupera la chiave master ed autentica se stesso inviando un messaggio cifrato (usando la chiave master) al client.
- I dati successivi sono cifrati con chiavi derivate dalla chiave master, usando un sistema a chiave simmetrica, come DES, Triplo-DES, IDEA, RC2 ed RC4.