Crittografia

Una Panoramica

Aspetti della Sicurezza

- Confidenzialità
  - I dati ed iservizi non devono fornire informazioni sensibili a persone **non** autorizzate
- Integrità
  - Deve essere evidente l'eventuale manomissione ed alterazione dei dati
- Autenticità
  - Deve essere possibile ricondurre i dati al reale proprietario e creatore
- Non Ripudio
  - L'autore o il proprietario dei dati **non** deve poter rinnegare le proprie azioni
- Identità
  - Deve essere possibile verificare che la reale identità del creatore dei dati

Crittografia

- Utilizzando algoritmi derivati da alcuni dei problemi matematici di più difficile risoluzione, si implementano in hardware o in software gli obiettivi di cui sopra
- La sicurezza della criptografia non si basa sulla segretezza degli algoritmi ma su quella delle chiavi in essi usate
- La forza dei vari algoritmi è soggetta al dinamismo introdotto dall'evoluzione dei processori e delle tecniche di criptoanalisi

Valutazione del Rischio

- La sicurezza al 100% non solo non sarebbe possibile ma risulterebbe proibitiva in termini di costi sostenuti
- Quindi è necessario scegliere che cosa porre in sicurezza ed in che misura farlo
- Questo processo decisionale di tipo strategico viene chiamato **Risk Assessment**

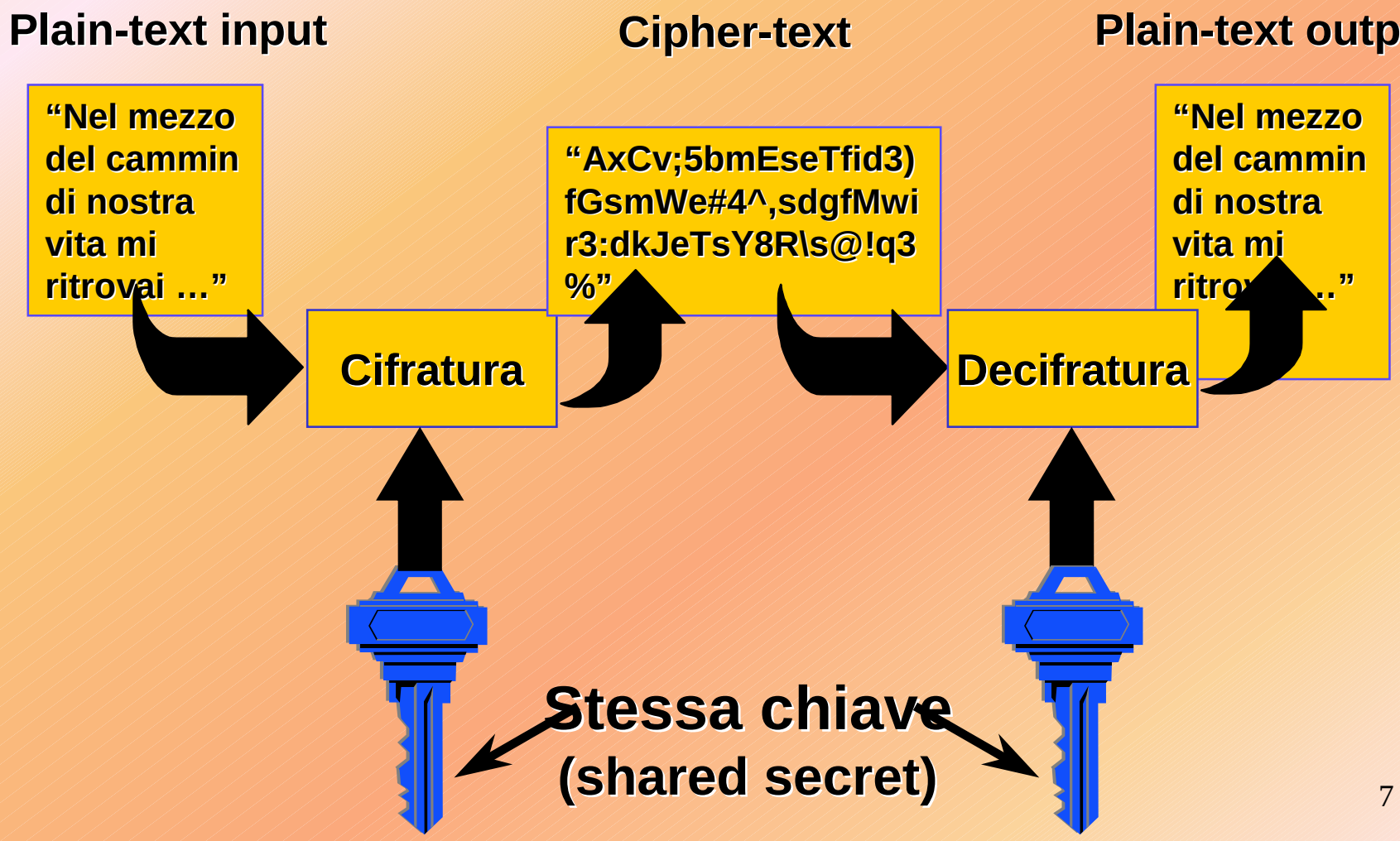
Scelta dei mezzi

- Per la scelta dei sistemi di sicurezza
  - Rivolgersi a produttori affidabili (diffidare quasi sempre di soluzioni a basso prezzo o improvvisate)
  - Preferire algoritmi ben conosciuti e comprovati da esperienze e solidi test di criptoanalisi
  - Scartare, se possibile, soluzioni che di cui siano note eccessive vulnerabilità
  - Assolutamente **non** sviluppare algoriti proprietari data l'enorme complessità dell'argomento e le sue vastissime implicazioni
  - Verificare sul campo la solidità della propria scelta attraverso tecniche di **Penetration Test**

Terminologia Criptografia

- Testo in chiaro (plaintext)
  - Dato in forma leggibile da un uomo o da un computer
- Testo cifrato (ciphertext)
  - Dato che deve essere prima decifrato per poter essere letto da un uomo o un computer
- Chiave (key)
  - Necessaria per cifrare il testo in chiaro e decifrare il testo cifrato
- Criptoanalisi
  - Tecnica e metodologia di tipo matematico per rilevare ed sfruttare le vulnerabilità degli algorimti di cifratura

Crittografia a Chiave Simmetrica



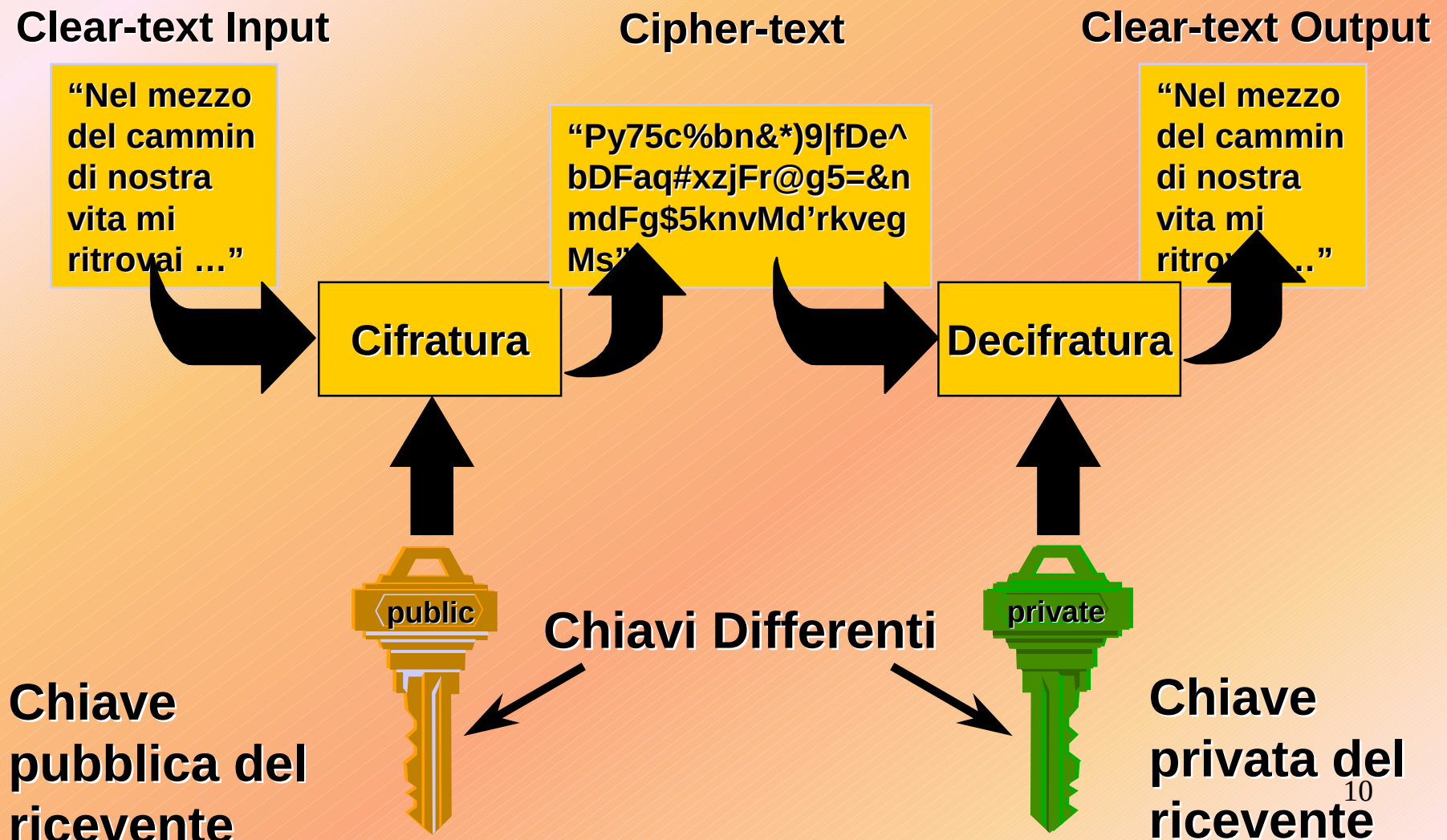
Cifratura Simmetrica: Pro e Contro

- Punti deboli:
  - Necessario un preventivo accordo sulla chiave condivisa
  - Sicurezza dello scambio della chiave
- Punti di forza:
  - Semplice e veloce (da 1.000 a 10.000 volte più veloce della cifratura asimmetrica)
    - Ancora più veloce se svolta in hardware
    - Cifratura in hardware più sicura della stessa cifratura software

Cifratura Asimmetrica (1)

- La conoscenza della chiave di cifratura non comporta la conoscenza della chiave di decifratura
- Il ricevente genera una coppia di chiavi
  - Pubblica la chiave pubblica in una directory
- Ognuno può usare questa chiave pubblica per cifrare messaggi che solo il proprietario della relativa chiave privata potrà decifrare

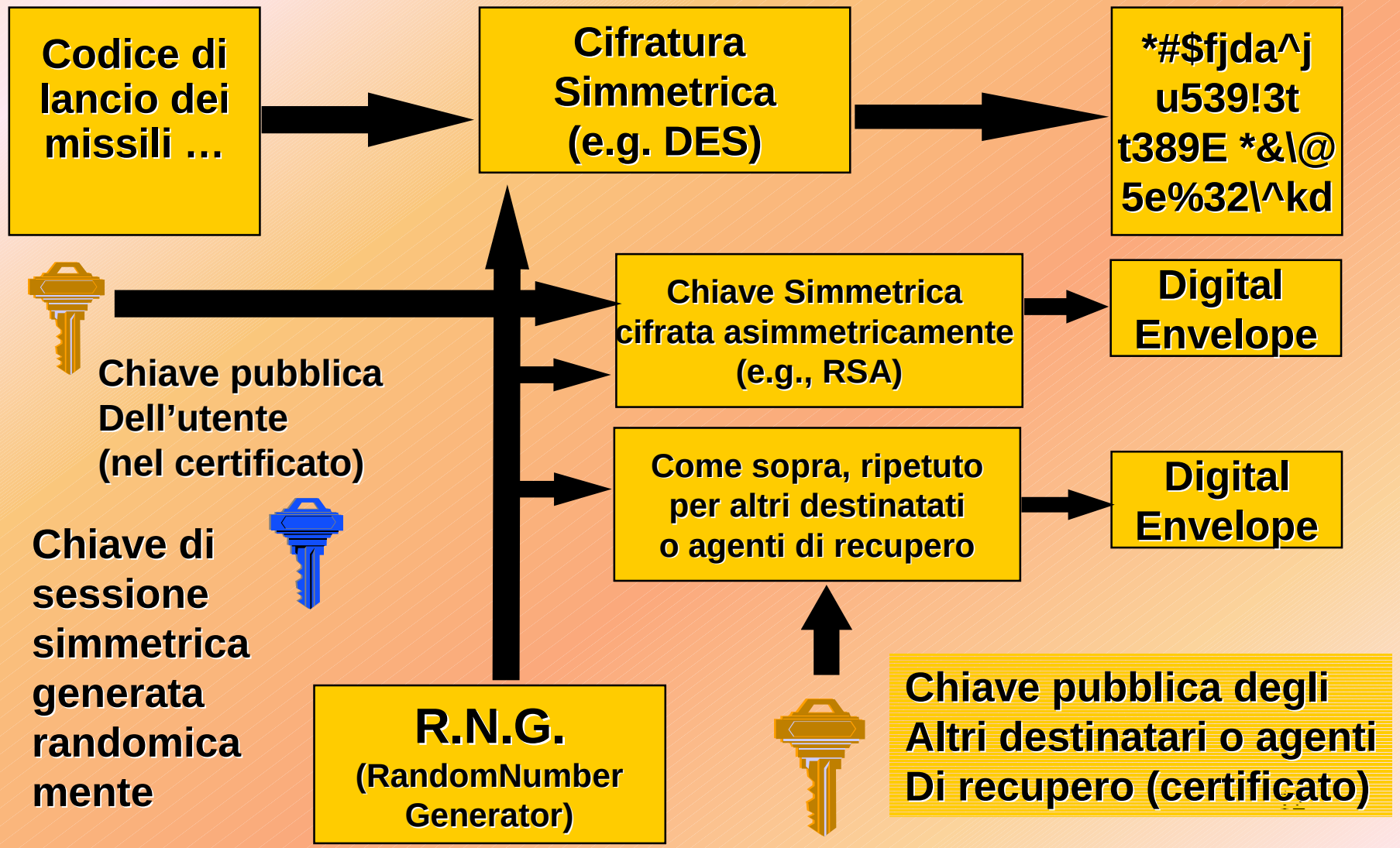
Cifratura Asimmetrica (2)



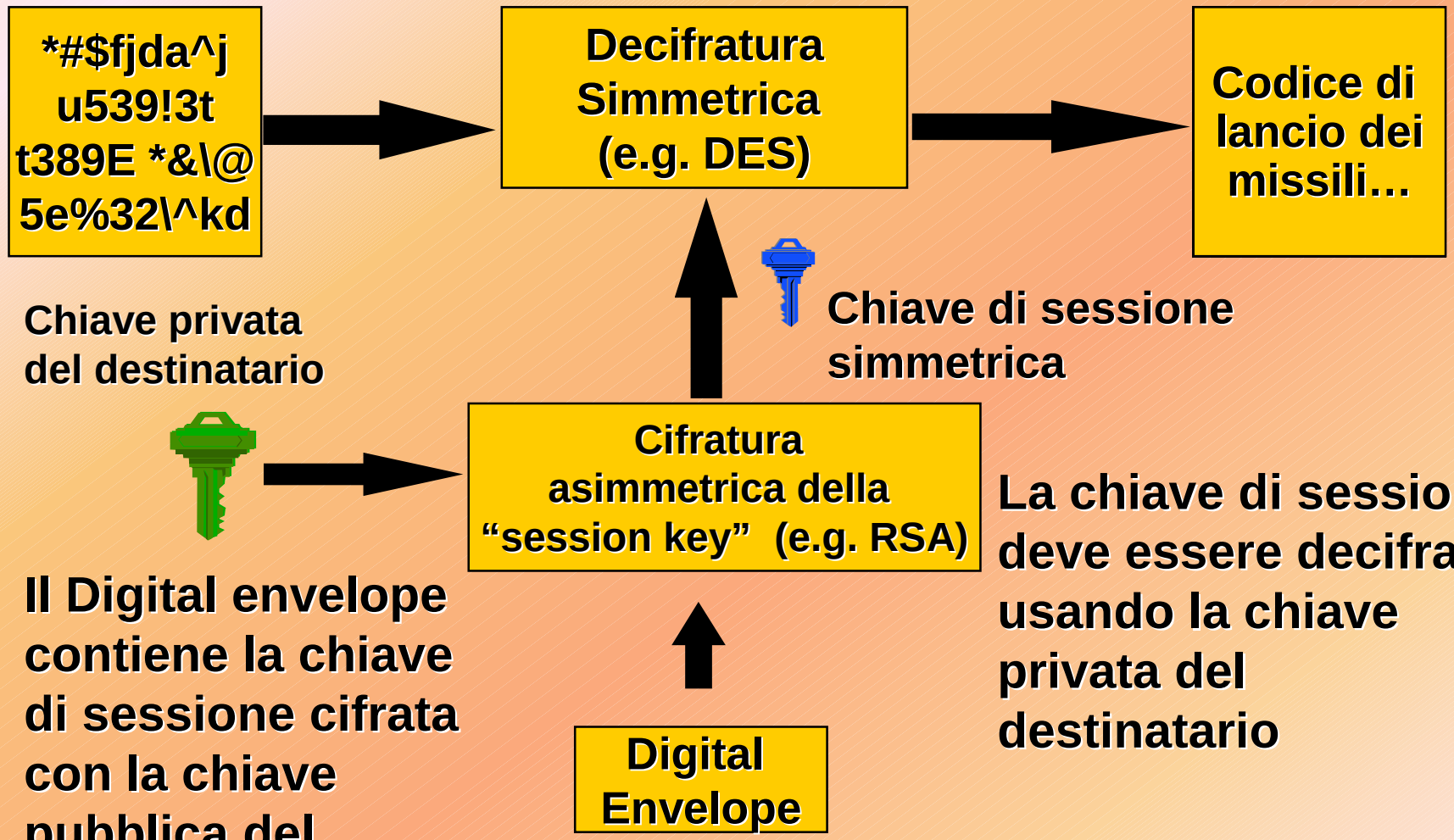
Cifratura Asimmetrica: Pro e Contro

- Punti Deboli
  - Estremamente lenta
  - Suscettibile ad attacchi del tipo “known ciphertext”
- Punti di Forza
  - Risolve il problema del passaggio della chiave

Modello Ibrido: Cifratura



Modello Ibrido: Decifratura



Firma Digitale

- Si vuole consegnare un testo in chiaro al destinatario permettendogli di verificarne l'autenticità
  - Integrità, Autenticità e non-ripudio
  - NO confidenzialità

Algoritmi: DES, IDEA, RC2, RC5

- Simmetrici
- DES (Data Encryption Standard) è il più popolare
  - Le chiavi sono molto piccole (56 bits)
  - Un attacco di tipo *forza-bruta* impiega pochi secondi con le potenze di calcolo oggi disponibili
  - Triple Des (3 DES) NON è molto più sicuro
  - Evitarlo, a meno che i dati protetti siano di scarsa rilevanza
- IDEA (International Data Encryption Standard)
  - Simile al DES
  - Chiave a 128 bits
- RC2 & RC5 (Rivest)
  - Simile a DES e IDEA

Algoritmi: Rijndael

- Standard del governo statunitense per sostituire DES
  - Vincitore della competizione AES (Advanced Encryption Standard) lanciata dal NIST (National Institute of Standards and Technology in US) nel 1997-2000
  - Sviluppato in Europa in Belgio da Joan Daemen e Vincent Rijmen
- Cifratura simmetrica a blocco (*block-cipher* a 128, 192 e 256 bits) con chiavi variabili di 128, 192 e 256 bits
- Veloce e ricco di proprietà positive come una buona immunità ad analisi temporali e di carico elettrico
- Costruzione vagamente simile a DES (S-Boxes, XORs, ecc) ma con profonde differenze

Algoritmi: CAST & GOST

- CAST
  - Canadians Carlisle Adams & Stafford Tavares
  - Chiave a 64 bits
  - 64 bits di dati
  - Possibilità di scegliere le S-Boxes
  - Si mostra resistente alla criptoanalisi differenziale e lineare
  - Unico mezzo per rompere la cifratura: brute-force (purtroppo la chiave è un po' corta)
- GOST
  - Versione sovietica del DES con un progetto migliorato ed un maggior numero di ripetizioni
  - Chiave a 256 bits , ma 610 bits di "segreto"

Attenzione ai Flussi

- Non usare un block-cipher in un loop
- Usare tecniche cripto-correttive per trattare *flussi* di dati, come il CBC (Cipher Block Chaining)
  - Il framework .NET implementa una funzione ICryptoTransform su un flusso di cifratura

Algoritmi: RC4

- Simmetrico
  - Veloce
  - Cifratura a flusso
- Sviluppato da Rivest nel 1994
  - Originariamente segreto, venne poi pubblicato su sci.crypt
- In relazione con “One Time Pad”, teoricamente più sicuro
- MA….
- Si basa su un *Random Number Generator* di non eccezionale qualità
  - E questo è il problema

Algoritmi: RSA, DSA, ElGamal, ECC

- Asimmetrici
  - Molto lenti e costosi in termini computazionali
  - Molto sicuri
- Rivest, Shamir and Adleman – 1978
  - Popolare e molto indagato
  - Ha la sua forza nell'inefficienza degli odierni metodi per la fattorizzazione dei grandi numeri primi
  - Qualche preoccupazione per la generazione della chiave in alcune implemenatzioni
- DSA (Digital Signature Algorithm) – NSA/NIST
  - Solamente per la firma digitale, non per la cifratura
- ElGamal
  - Si basa sulla complessità dei logaritmi discreti
- ECC (Elliptic Curve Cryptography)
  - Problemi di matematica superiore e topologia
  - Migliore e più efficiente del RSA

Crittografia Quantica

- Metodo per la generazione ed il passaggio di una chiave segreta o di un flusso random
  - Non per la cifratura dei dati
- La polarizzazione della luce (fotoni) può essere rilevata solo in un modo che ne distrugge la direzione
  - Se qualcuno osserva la trasmissione, il ricevente se ne accorge tempestivamente perché il flusso ricevuto viene irrimediabilmente alterato e corrotto
- Perfettamente adattabile ai lunghi link in fibra ottica

Algoritmi: MD5 & SHA

- Funzioni di Hashing
- NO algoritmi di cifratura
- Obiettivi:
  - Non reversibilità: non si può ottenere il messaggio partendo dal hash
  - L'hash è molto più breve del messaggio
  - Due messaggi NON possono avere lo stesso hash
- MD5 (Rivest)
  - 512 bits → 128 bits di hash
- SHA (Secure Hash Algorithm)
  - Standard US basato su MD5

Sistemi Robusti

- E’ sempre meglio un sistema ibrido
- Simmetrico:
  - Min.128 bits per RC2 & RC5, 3DES, IDEA
  - Min 256 bits per RC4
- Asimmetrico
  - Da 1024 a 4096 bits per RSA, ElGmal, Diffie-Hellman
- Hash
  - 128 o meglio 256 bits sia per MD5 che per SHA

Sistemi Deboli

- Qualunque cosa con 40 bits (incluse le versioni con 128 e 56 bits ma con un resto fisso)
- CLIPPER
- A5 (telefonia GSM fuori dagli US)
- Vigenère (telefonia mobile negli US)
- Algoritmi non verificati e certificati