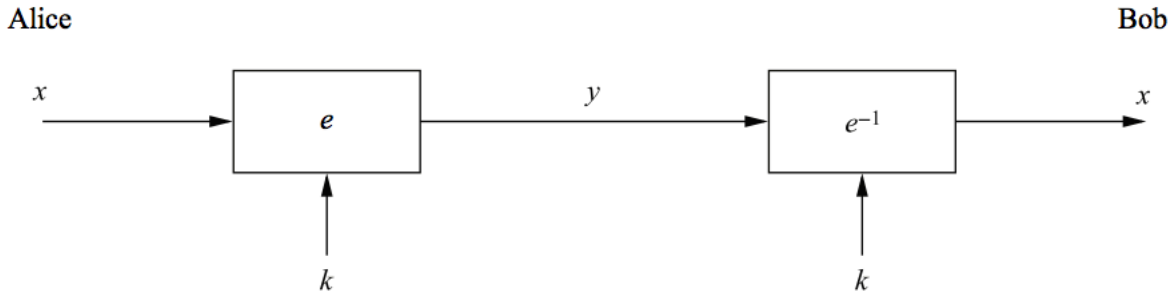
Sicurezza Informatica

Crittografia a Chiave Pubblica

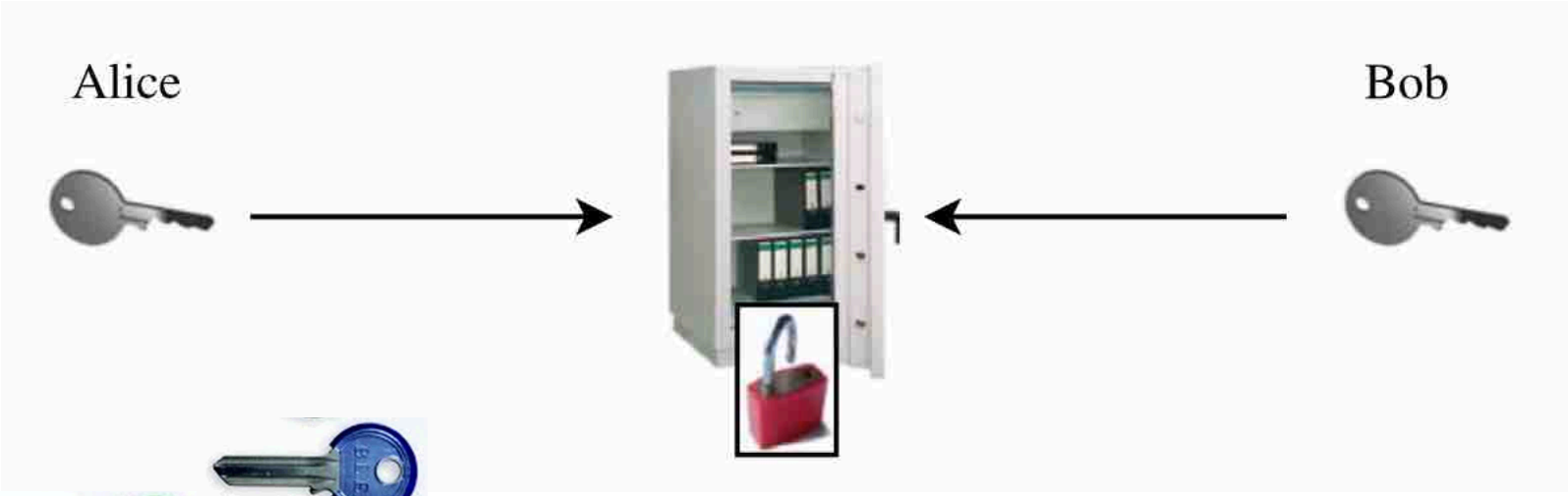
Concetti di base

Cifrari a chiave simmetrica



- La stessa chiave è usata per cifrare e decifrare
- Cifratura e decifratura sono funzioni molto simili (a volte identiche)
- Gli schemi di cifratura sono molto sicuri e *veloci*

Analogia con il *mondo fisico*



Per tutti gli utenti con cui Alice vuole comunicare deve essere stabilita una chiave

Carol

Diana

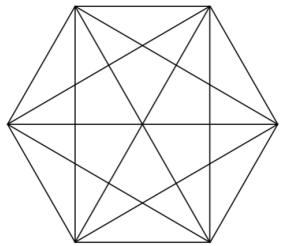
Grace

Edwin

Problemi con cifrari a chiave simmetrica

- Distribuzione della chiave
  - La chiave deve essere trasferita in modalità sicura

- Gestione delle chiavi
  - Per n utenti devono essere generate n(n-1)/2 chiavi
  - Ogni utente deve conservare n-1 chiavi
  - L'aggiunta di un nuovo utente implica la distribuzione della sua chiave a tutti gli altri utenti



Idea alla base della crittografia asimmetrica

Buca delle lettere

Chiunque può imbucare una lettera

Solo il postino che ha la chiave può aprire la cassetta

Crittografia Asimmetrica (a Chiave Pubblica)

- Idea: invece di una chiave utilizzarne due
- Una per cifrare, l'altra per decifrare
  - Chiave pubblica K_{pub} per cifrare
  - Chiave segreta (privata) K_{priv} per decifrare
- L'algoritmo di generazione della chiave deve prevedere la generazione delle due chiavi
- Gli algoritmi di cifratura e decifratura, in genere, sono differenti

Crittografia Asimmetrica

- Introdotta nel 1976 da Whitfield Diffie e Martin Hellman vincitori nel 2015 del Turing Award

W. Diffie and M. E. Hellman
New directions in cryptography
IEEE Transactions on Information Theory, IT-22:644–654, 1976.

- Concetto scoperto indipendentemente da Ralph Merkle, vincitore nel 1999 con Diffie e Hellman del IEEE Kobayashi Award

Ralph C. Merkle.
Secure communications over insecure channels
Commun. ACM, 21(4):294–299, 1978.

Lavoro sottomesso nel 1974, ma rifiutato
"...*not in the main stream of present cryptography thinking*...."

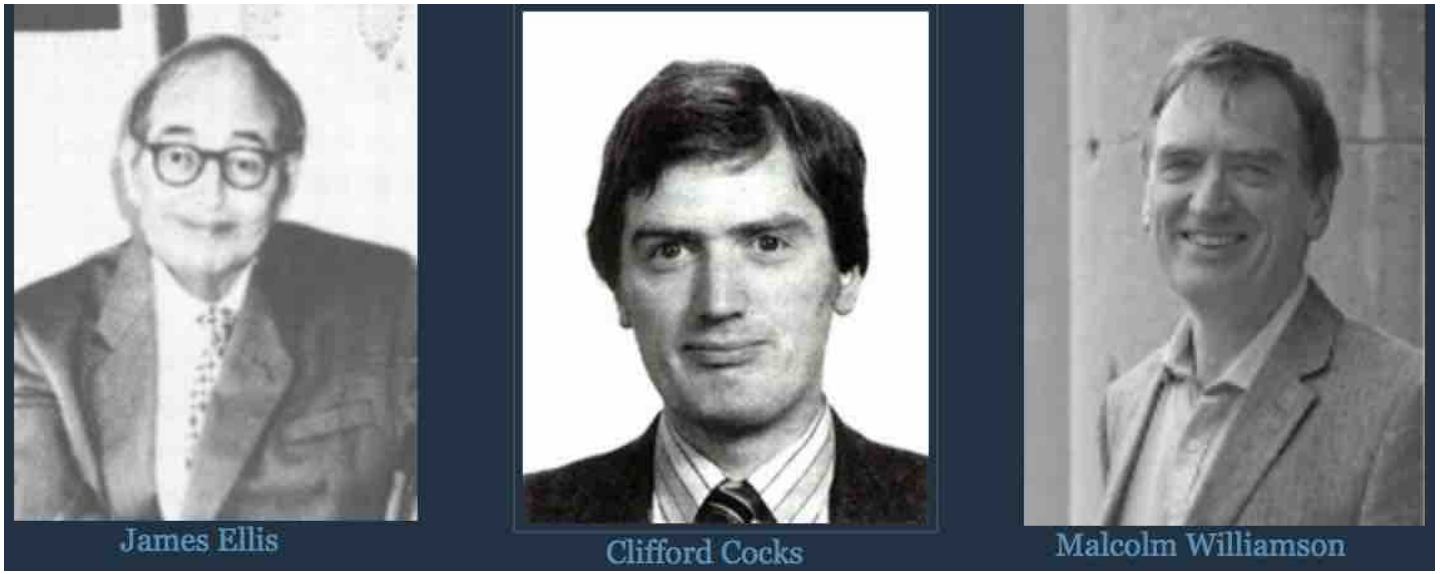
E i servizi segreti?

- Nel 1997 furono resi noti dei documenti segreti britannici da cui si dedusse che nel Regno Unito, qualcosa era noto
- Tra il 1972 ed il 1974, tre ricercatori del GCHQ, James Ellis, Clifford Cocks e Graham Williamson avevano già scoperto il concetto e le costruzioni di crittografia a chiave pubblica
  - Non-secret encryption
  - Schema simile ad RSA
  - Schema molto simile all'accordo di chiavi Diffie-Hellman
- È probabile che GCHQ non fu in grado di identificare le conseguenze della scoperta dei tre ricercatori

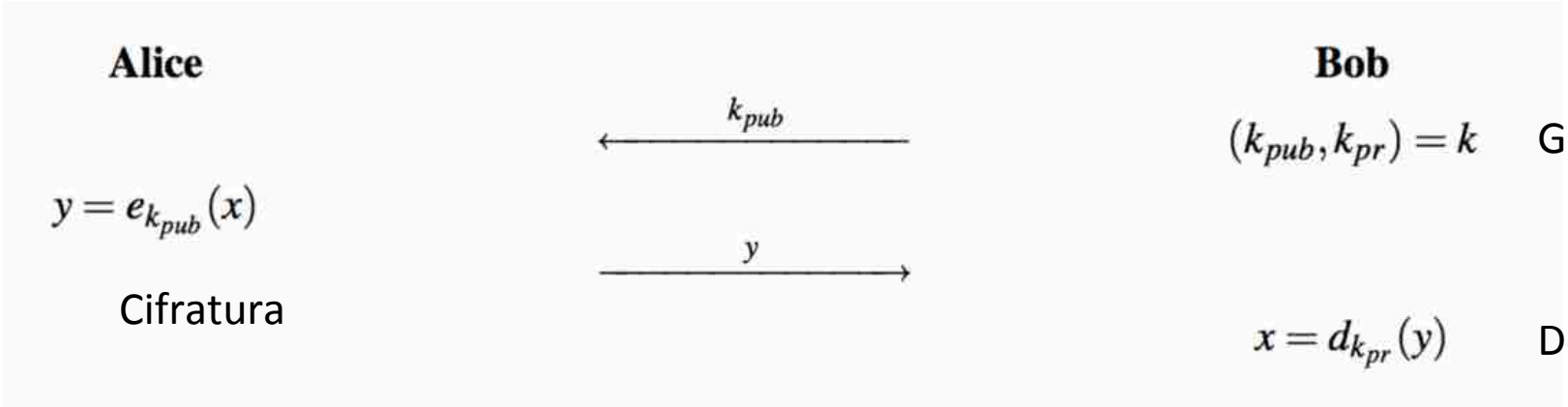
GCHQ

(GCHQ) Government Communications Headquarters

Agenzia governativa britannica che si occupa della sicurezza, nonché dello spionaggio e controspionaggio, nell'ambito delle comunicazioni



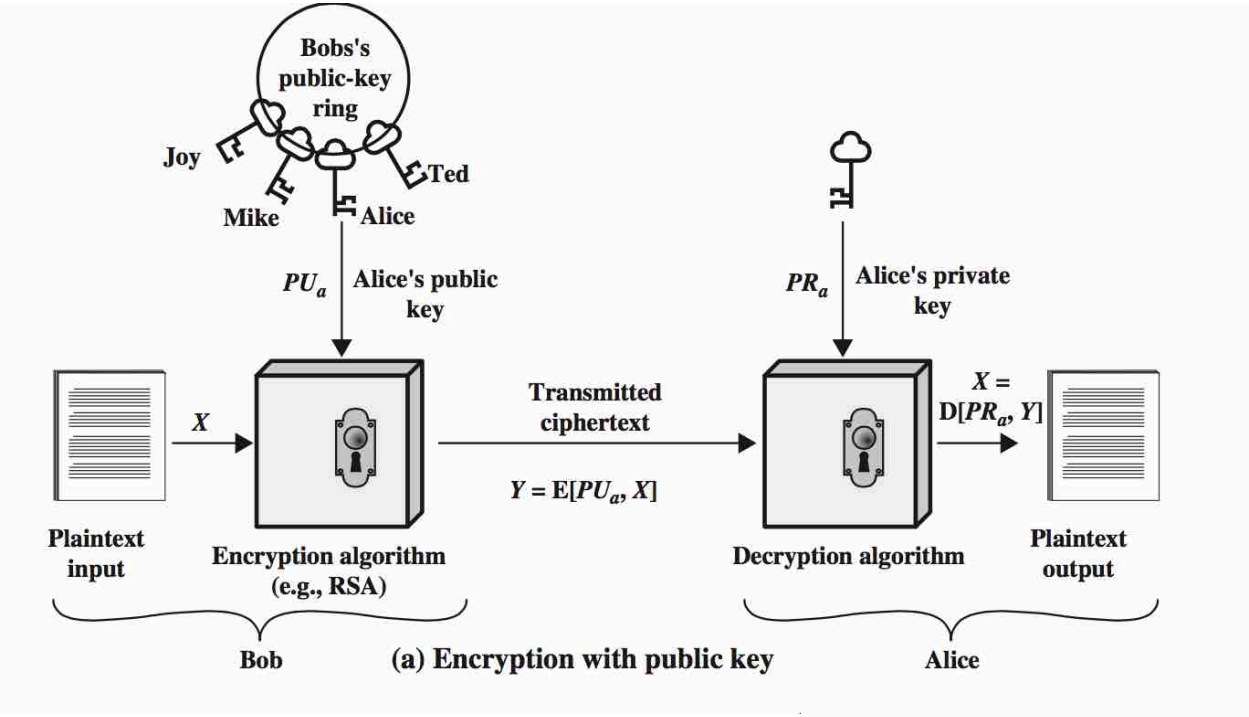
Protocollo di base per PKC



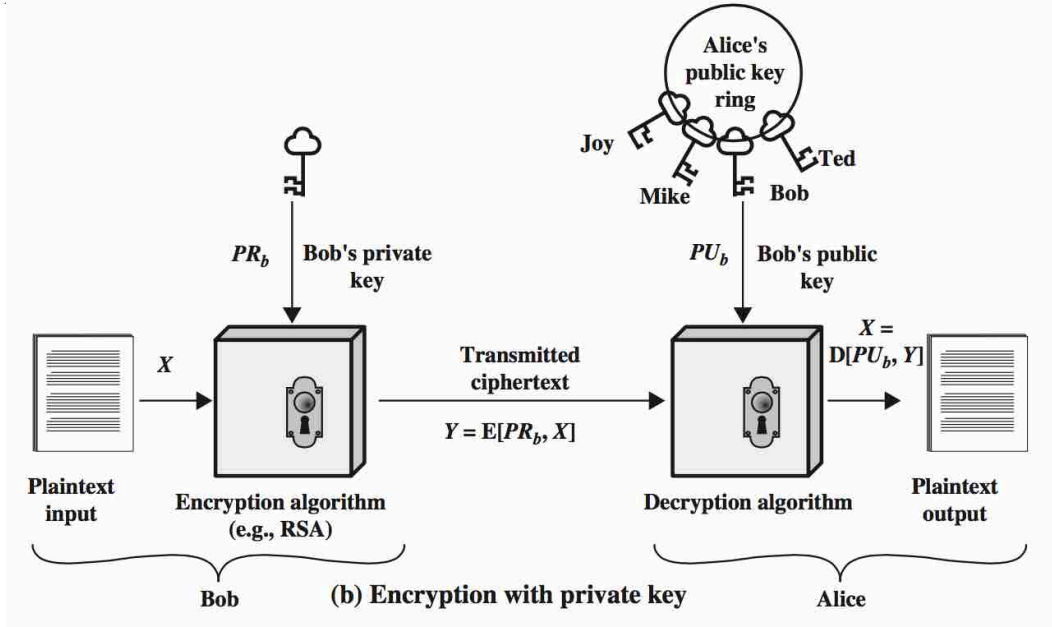
Il problema della distribuzione delle chiavi è risolto
o quasi
Le chiavi pubbliche devono essere autenticate

Dettagli in seguito

Chiave Pubblica



Chiave Privata



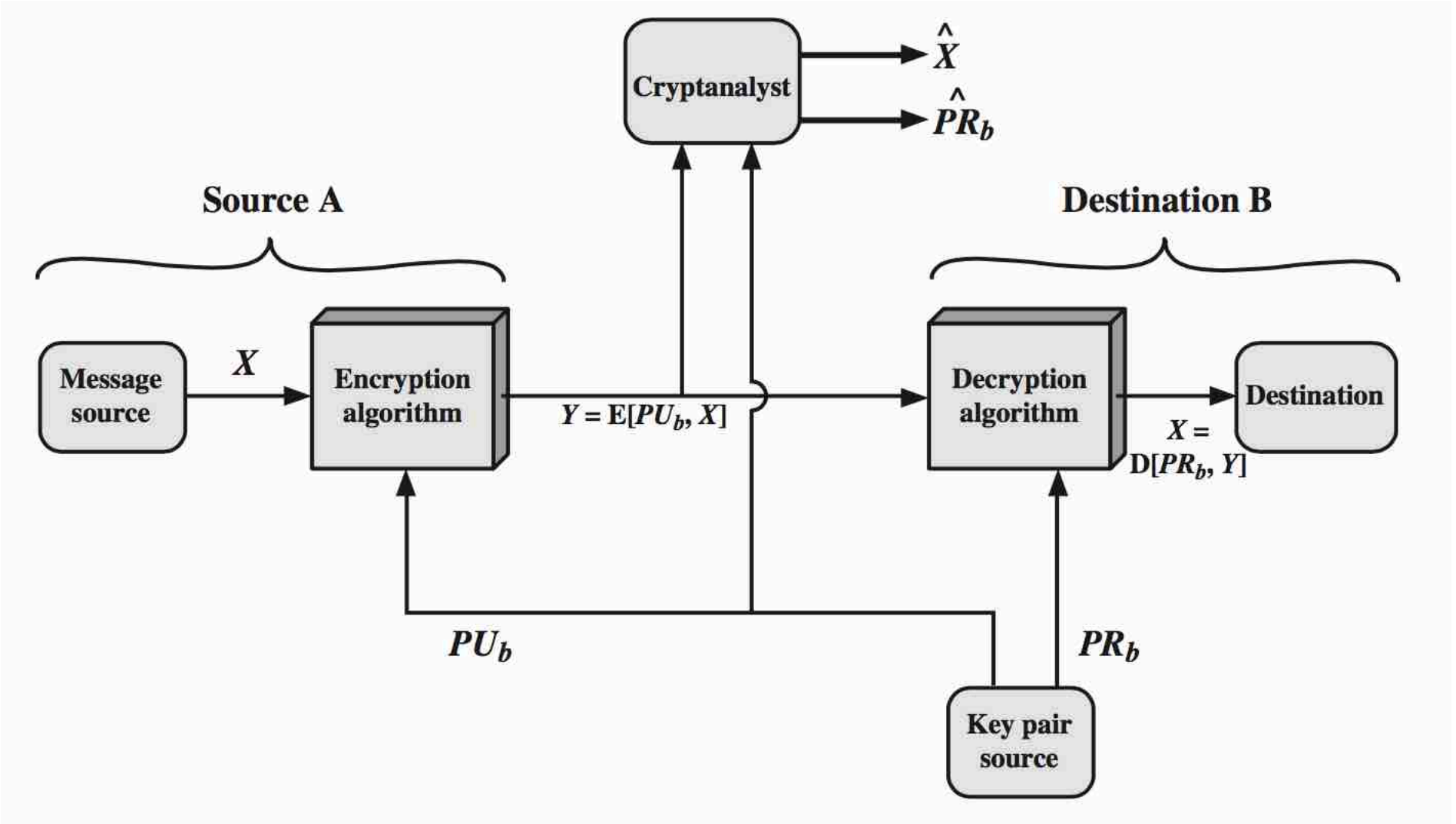
Requisiti (informali) di sicurezza

- Una delle due chiavi deve restare segreta
- Deve essere impossibile (o quanto meno *difficile*) decifrare un messaggio se una delle due chiavi è segreta
- La conoscenza dell'algoritmo, di una delle chiavi, e di alcuni esemplari di testo cifrato (oppure coppie plaintext-ciphertext) non è sufficiente per calcolare l'altra chiave (oppure, testo in chiaro)
  - Saremo formali in seguito con IND-CPA e IND-CCA

    IND-CPA: INDistinguishability under Chosen Plaintext Attack

    IND-CCA: INDistinguishability under Chosen Ciphertext Attack

Schematicamente



Meccanismi realizzati con PKC

- Key Establishment (Distribuzione di chiavi)
  - Senza una chiave condivisa è possibile per due utenti accordarsi, su un canale insicuro, su una chiave
    - Diffie–Hellman key exchange (DHKE)
    - RSA key transport protocols (usato in SSH – RFC2630)
- Nonrepudiation (non ripudio)
  - Realizzata tramite Firma Digitale
  - RSA, DSA, ECDSA

Meccanismi realizzati con PKC

- Identificazione
  - Si possono identificare entità attraverso protocolli di challenge-response
    - Si usano le primitive di Cifratura o Firma Digitale

- Cifratura
  - Ovvio
  - RSA, ElGamal, Goldwasser-Micali, Pailler,…

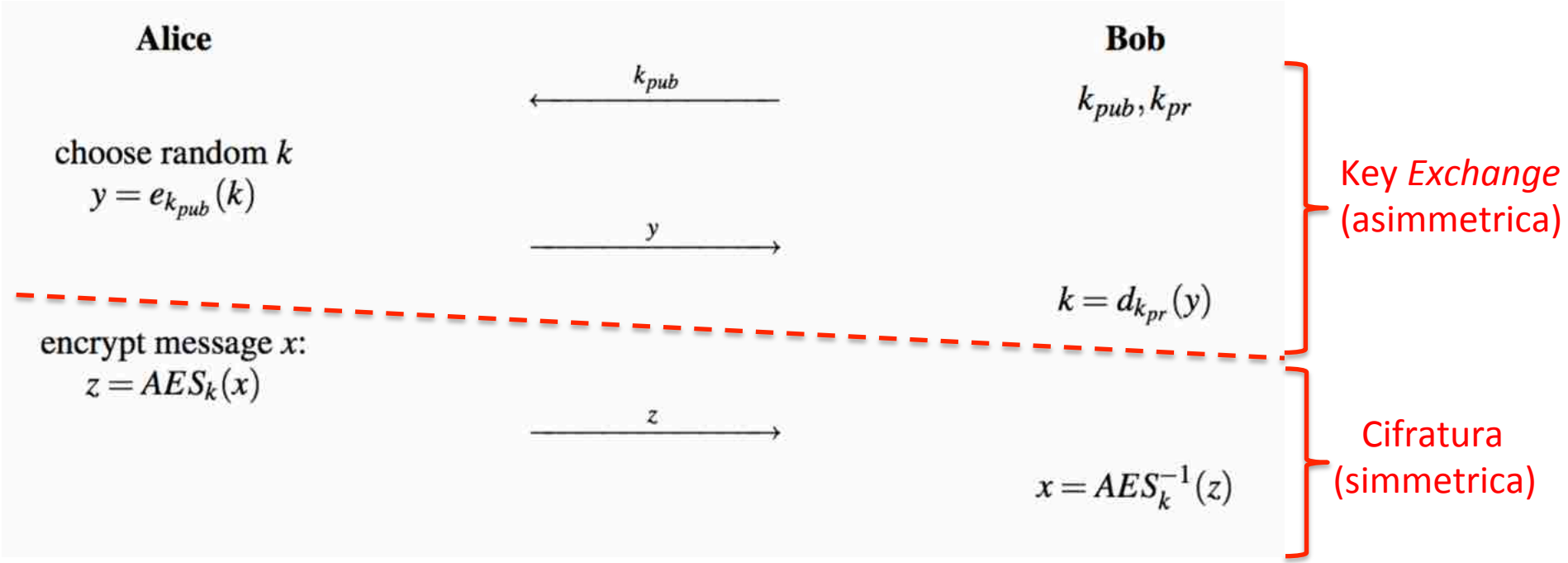
Osservazioni

- Identificazione e cifratura possono essere realizzati anche con schemi di cifratura simmetrici
  - La gestione delle chiavi è più onerosa
- Molti cifrari a blocchi o stream cipher sono centinaia di volte più veloci degli algoritmi a chiave pubblica
- Algoritmi simmetrici non sono insufficienti nel fornire le funzionalità di non ripudio e distribuzione chiavi

Prendiamo il meglio dei due approcci

Cifrari Ibridi

- Incorporano sia algoritmi simmetrici sia a chiave pubblica
  - Key Exchange, Digital Signature: crittografia asimmetrica
  - Cifratura: crittografia simmetrica
  - Esempi: SSL/TLS, IPSec, …



Per essere precisi….

- Nei documenti NIST si fa riferimento a
  - asymmetric-key-based key transport scheme

Key transport

A key establishment procedure whereby one party (the sender) selects a value for the secret keying material and then securely distributes that value to another party (the receiver). Contrast with key agreement.

Come costruire schemi a chiave pubblica

- Tutti sono costruiti a partire da un principio comune, la **funzione one-way**
- Possiamo definirla informalmente come

Definition 6.1.1 One-way function
A function $f()$ is a one-way function if:

1. $y = f(x)$ *is computationally easy, and*
2. $x = f^{-1}(y)$ *is computationally infeasible.*

f^{-1} è facile da calcolare se si conosce una **trap-door**

Easy: calcolabile in tempo polinomiale
Infeasible: non è fattibile calcolarla in tempo ragionevole usando il miglior algoritmo

Esempi di problemi difficili

- Fattorizzazione di interi (e.g., RSA)
  - Dati due primi p e q, calcolarne il prodotto $n=p \cdot q$ è facile
  - Dato n è difficile calcolare p e q quando p e q sono *sufficientemente* grandi
- Calcolo del logaritmo discreto (DH, ElGamal, DSA)
  - Dato a, x ed m calcolare $y = a^x \bmod m$ è facile — Elevamento a potenza
  - Dato a, y ed m trovare x tale che $y = a^x \bmod m$ è difficile — Logaritmo discreto

Definizione Formale
Schema di Cifratura a Chiave Pubblica

DEFINITION 10.1 *A* public-key encryption scheme *is a tuple of probabilistic, polynomial-time algorithms* (Gen, Enc, Dec) *that satisfies the following:*

1. *Algorithm* Gen *takes as input a security parameter* 1^n *and outputs a pair of keys* (pk, sk). *We refer to the first of these as the* public key *and the second as the* private key. *We assume for convenience that* pk *and* sk *each have length at least* n, *and that* n *can be determined from* pk, sk.

2. *Algorithm* Enc *takes as input a public key* pk *and a message* m *from some underlying plaintext space (that may depend on* pk*). It outputs a ciphertext* c, *and we write this as* $c \leftarrow \mathsf{Enc}_{pk}(m)$.

3. *Algorithm* Dec *takes as input a private key* sk *and a ciphertext* c, *and outputs a message* m *or a special symbol* $\perp$ *denoting failure. We assume without loss of generality that* Dec *is deterministic, and write this as* $m := \mathsf{Dec}_{sk}(c)$.

We require that for every n, *every* (pk, sk) *output by* $\mathsf{Gen}(1^n)$, *and every message* m *in the appropriate underlying plaintext space, it holds that*

$$\mathsf{Dec}_{sk}(\mathsf{Enc}_{pk}(m)) = m.$$

Riferimenti

Christof Paar and Jan Pelzl

Understanding Cryptography

Capitolo 6 (tranne paragrafo 6.3)

Introduction to Public-Key Cryptography

6.3 Essential Number Theory for Public-Key Algorithms