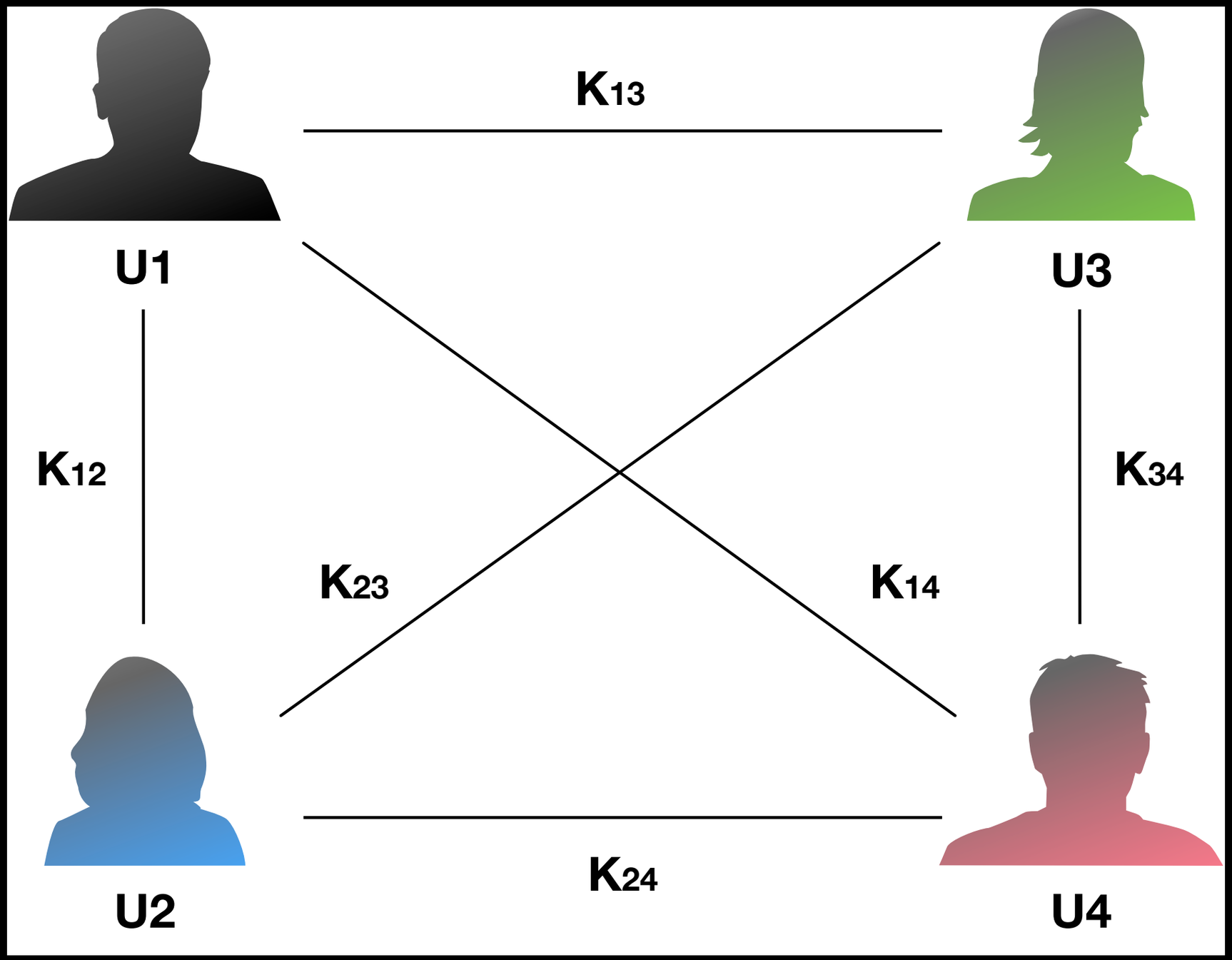
Public Key Cryptography

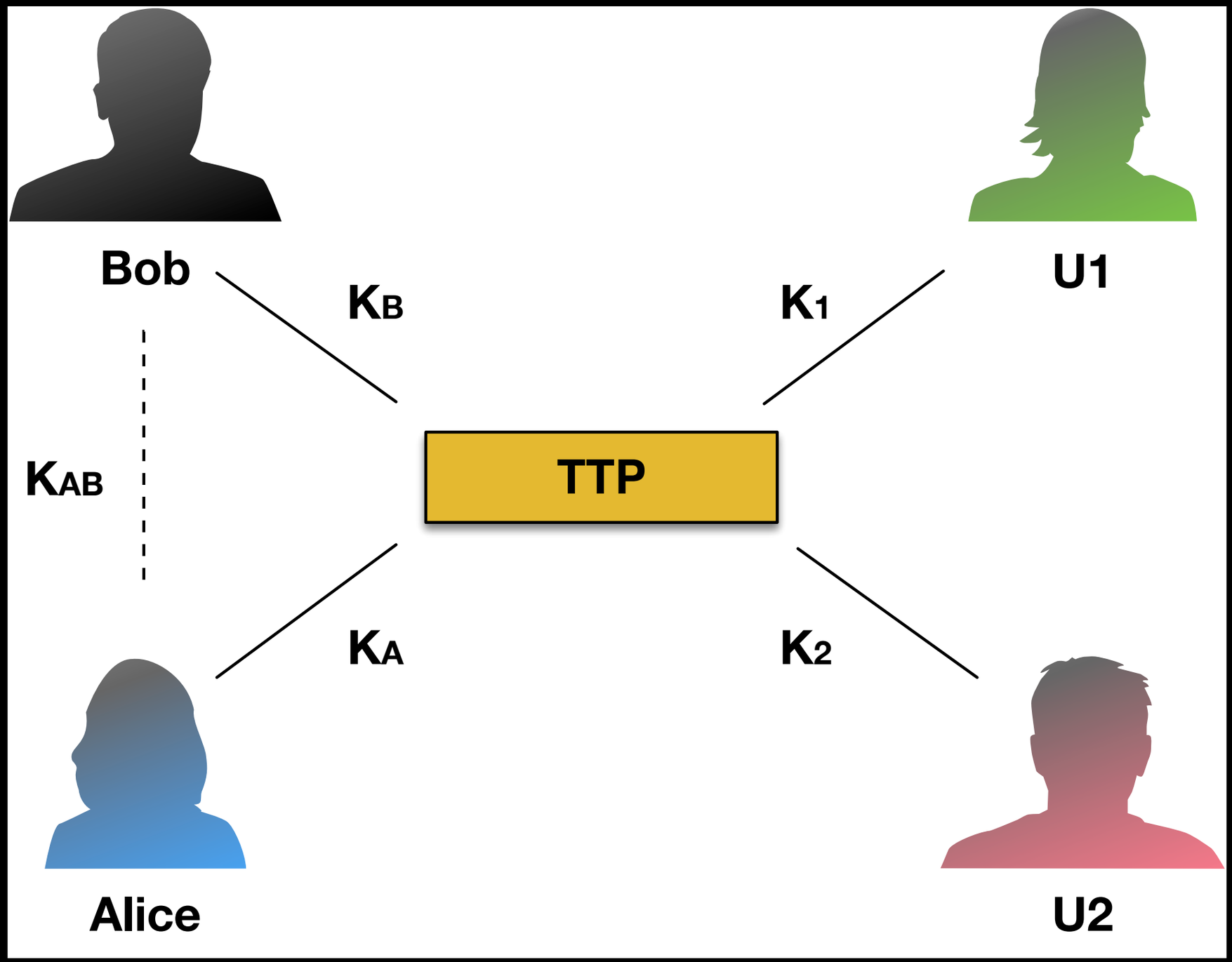
Dimitris Mitropoulos
dimitro@di.uoa.gr

Symmetric Cryptography

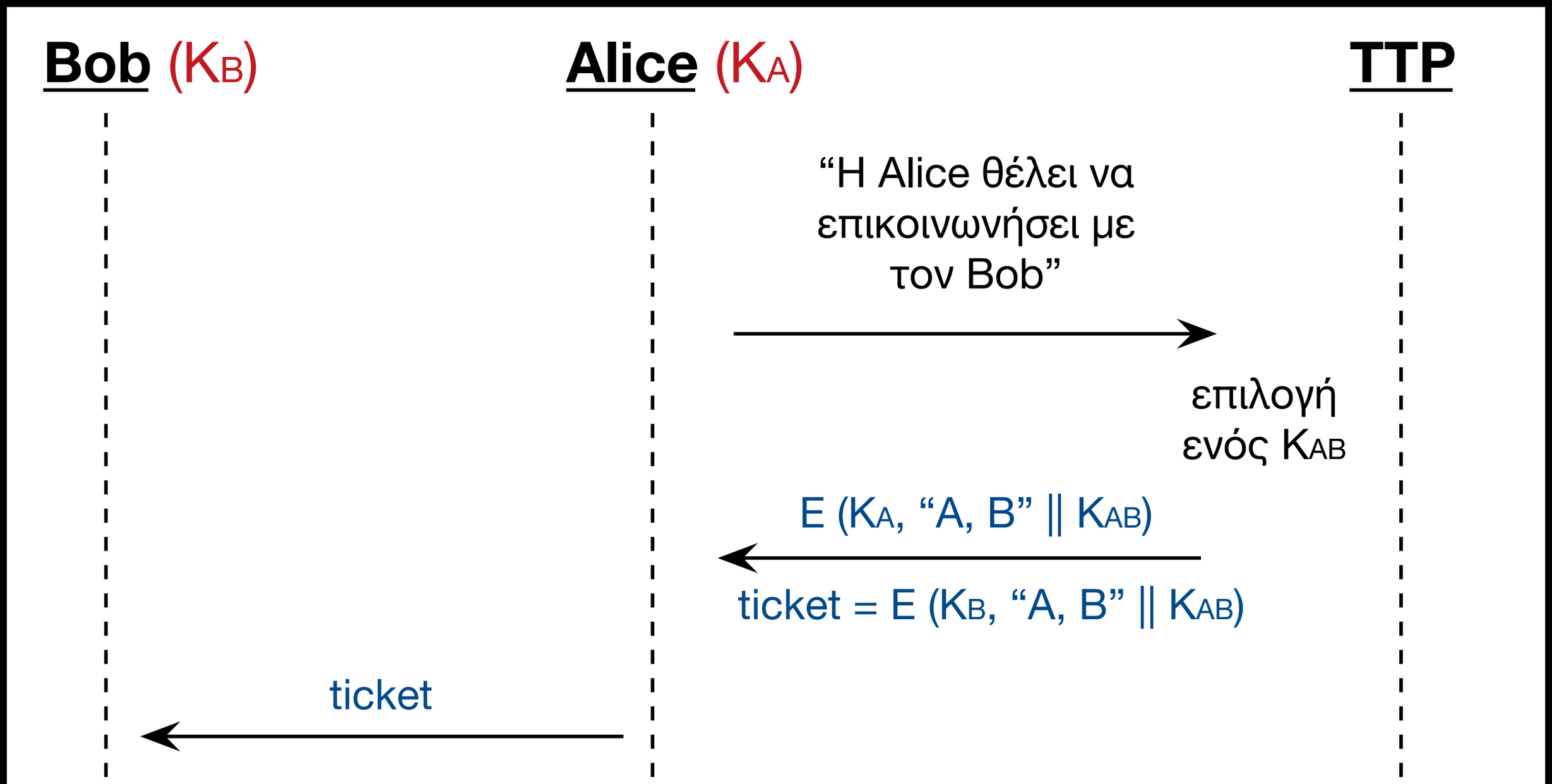
Key Management Challenge



Trusted Third Party
(TTP)



TTP
Δημιουργία Κλειδιού



TTP

Eavesdropping Security

Ο αντίπαλος βλέπει:

$E(K_A, \text{“A, B”} \,||\, K_{AB}), E(K_B, \text{“A, B”} \,||\, K_{AB})$

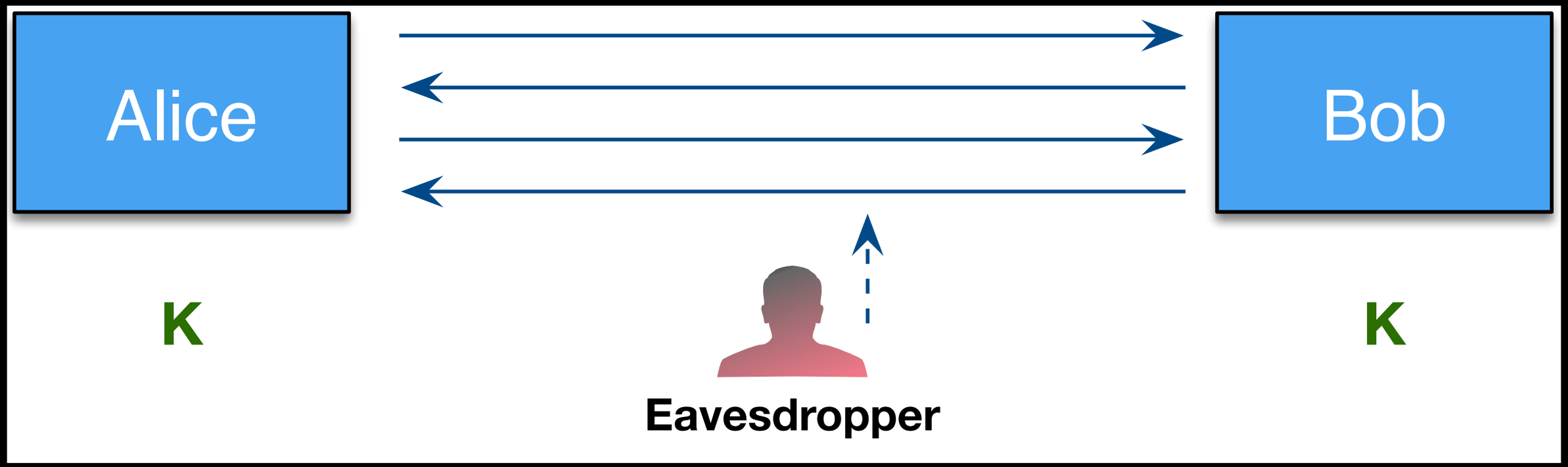
TTP
Active Attacks

Δεν παρέχει ασφάλεια σε replay attacks.
Ο αντίπαλος καταγράφει την παραγγελία ενός βιβλίου κατά την διάρκεια ενός session ανάμεσα στην Alice και τον (έμπορο) Bob. Ύστερα στέλνει ακριβώς τα ίδια μηνύματα και παραγγέλνει το ίδιο βιβλίο για την Alice.

TTP
Παρατηρήσεις

- Το TTP χρειάζεται:
  1. να είναι online για κάθε συναλλαγή.
  2. να γνωρίζει όλα τα κλειδιά.
- Εαν ένας επιτιθέμενος αποκτήσει πρόσβαση στο TTP, αποκτά ταυτόχρονα πρόσβαση σε όλα τα κλειδιά.
- Μπορεί να χρησιμοποιηθεί εσωτερικά σε έναν οργανισμό αλλά όχι στο διαδίκτυο.
- Το πρωτόκολλο Kerberos βασίζεται σε αυτή την προσέγγιση.

Χρησιμοποίηση Συμμετρικού Κλειδιού Χωρίς TTP (;)



Προσοχή: Μιλάμε για την καταπολέμηση κάποιου που απλά παρακολουθεί το δίκτυο χωρίς να μπορεί να παρέμβει!

Merkle Puzzles

- Puzzles: προβλήματα που μπορούν να λυθούν με "μερική" προσπάθεια.
- Π.χ.: Έχουμε ένα **συμμετρικό** cipher E(k, m), με κλειδί: $k \in \{0,1\}^{128}$.
  - **puzzle (P) = E (P, "message")** όπου P = $0^{96} \| b^1 \ldots b^{32}$.
  - Στόχος: να βρεθεί το P (2^{32} προσπάθιες).

Merkle Puzzles
(Ανταλλαγή Κλειδιού)

Alice: ετοιμάζει 2^{32} puzzles:

- Για i = 1, …, 2^{32} διαλέγει ένα $\mathbf{P_i} \in \{0,1\}^{32}$ και ένα ζευγάρι $\mathbf{x_i}$, $\mathbf{k_i} \in \{0,1\}^{128}$.
- Θέτει:

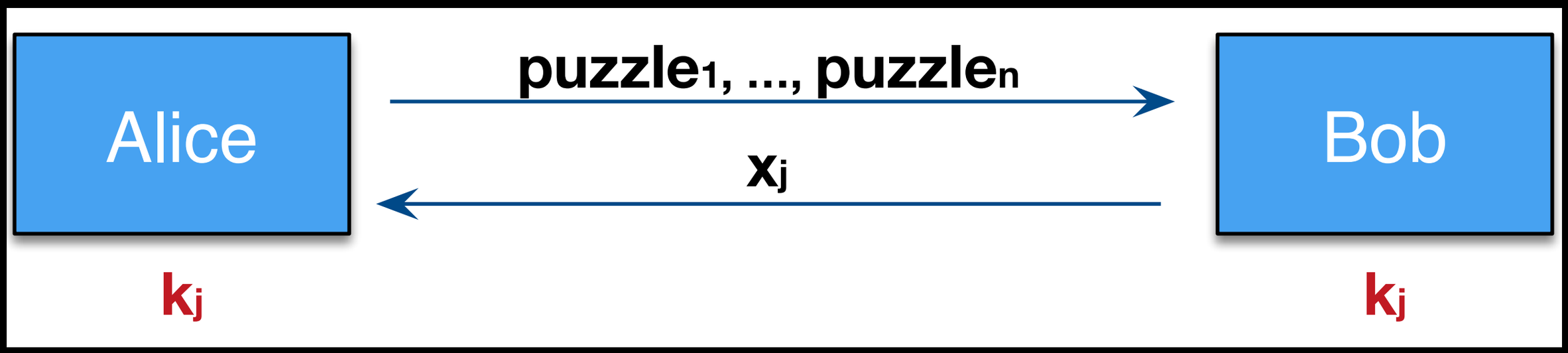
$$\text{puzzle}_i \leftarrow\!\!- E\,(0^{96} \,\|\, P_i,\ \text{“Puzzle \# } x_i\text{”} \,\|\, k_i\text{”})$$

- Στέλνει στον Bob: puzzle_1, …, $\text{puzzle}_{2^{32}}$

Bob: διαλέγει τυχαία ένα puzzle και το λύνει. Αποκτά έτσι το (x_i, k_i). Στέλνει στην Alice το x_i.

Alice: βρίσκει το puzzle με αριθμό x_i. Χρησιμοποιεί σαν κοινό κλειδί το k_i.

Ανάκτηση Κλειδιού από τον Αντίπαλο



- Προετοιμασία των puzzles από την **Alice**: O(n)
- Λύση ενός puzzle από τον **Bob**: O(n)

Προσπάθεια από την πλευρά του αντιπάλου για να ανακτήσει το κλειδί;

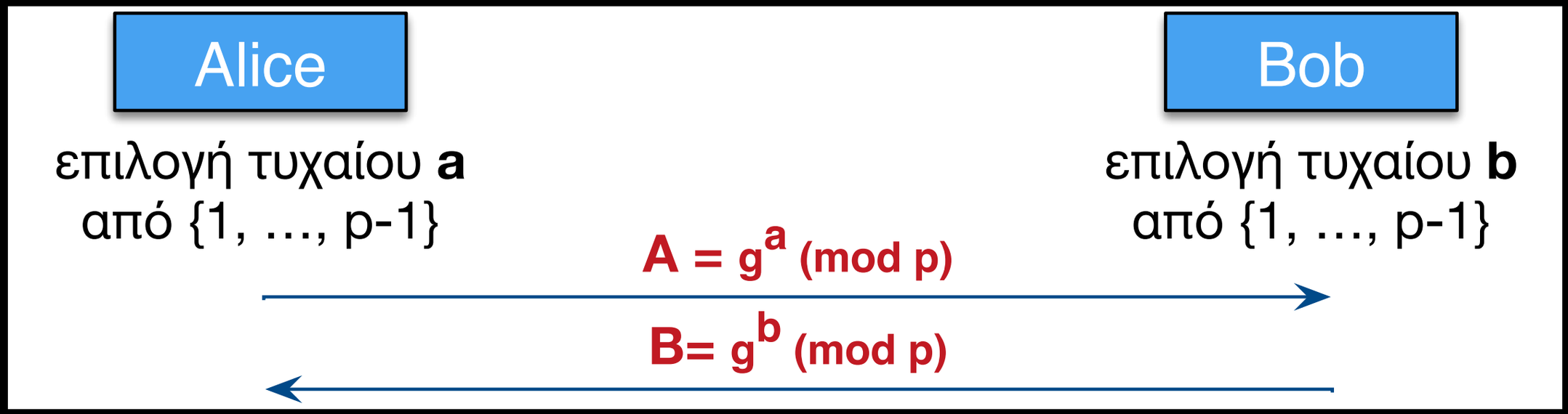
Merkle Puzzles

Παρατηρήσεις

- Η Alice πρέπει να στείλει αρκετά gigabytes στον Bob.
- Ο αντίπαλος θα χρειαστεί πολυωνυμικό χρόνο για να βρει το κλειδί: $O(n^2)$ — στο παράδειγμά μας 2^{64}.
- Μπορούμε να αυξήσουμε το n αλλά μετά ζητάμε πλέον πολλά από την Alice και τον Bob.
- Μπορούμε να πετύχουμε κάτι καλύτερο από το $O(n)$ - $O(n^2)$;

Το Πρωτόκολλο Diffie-Hellman

- Επιλογή ενός (αρκετά μεγάλου) πρώτου αριθμού **p** (π.χ. 600 ψηφία).
- Επιλογή ενός ακεραίου **g** $\in \{1, ..., p\}$.



$B^a \pmod p = (g^b)^a = K_{AB} = g^{ab} \pmod p = (g^a)^b = A^b \pmod p$

Diffie-Hellman
Security

- Ο αντίπαλος βλέπει: p, g, A, B.
- Μπορεί να υπολογίσει το $g^{ab} \pmod p$;
- Πιο γενικά: ορίζουμε την ακόλουθη συνάρτηση:

$$DH_g(g^a, g^b) = g^{ab} \pmod p$$

- Πόσο δύσκολο είναι να υπολογίσουμε την συνάρτηση αυτή;

Diffie-Hellman
Security (2)

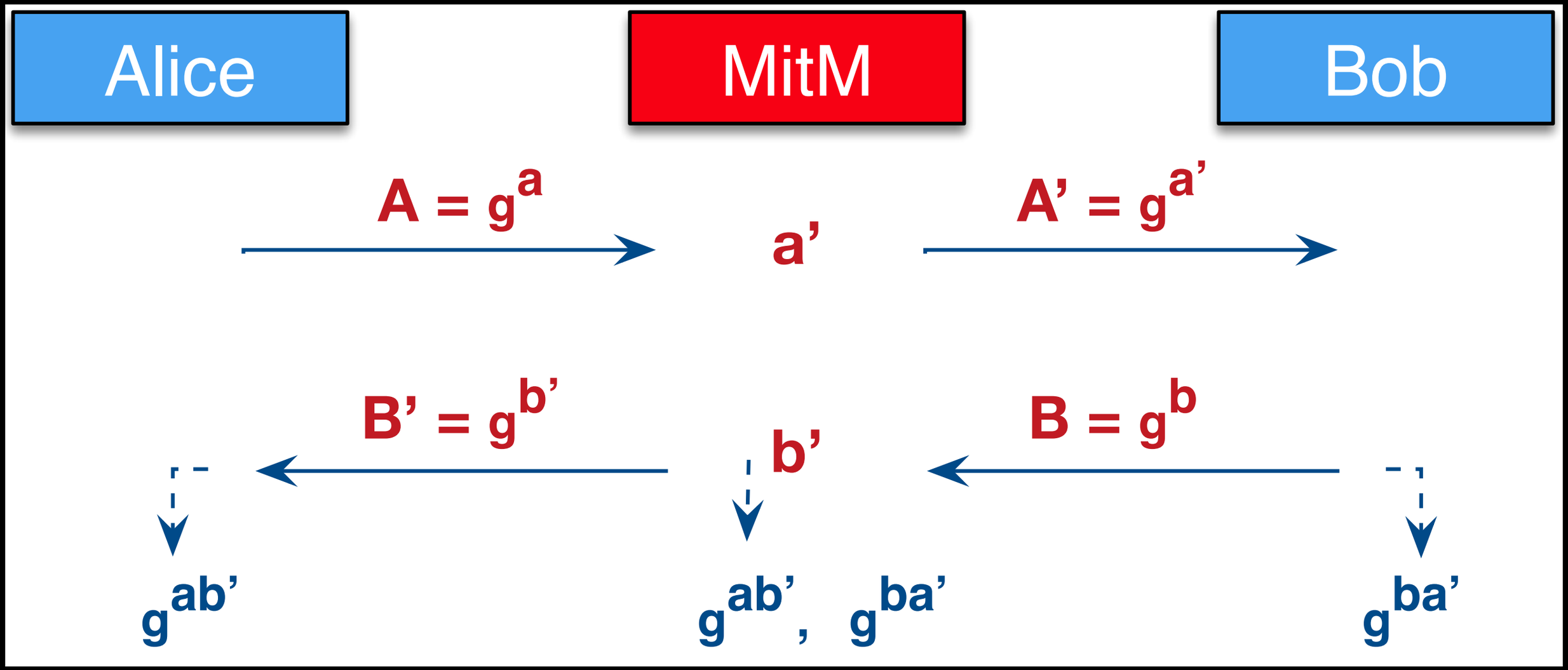
- Υποθέτουμε πως ο p είναι ***n*** bits.
- Ο πιο γνωστός αλγόριθμος για να βρει την συνάρτηση DH_g , είναι ο αλγόριθμος GNFS (General Number Field Sieve).
- Ο χρόνος που χρειάζεται είναι (περίπου): $exp(\mathcal{O}(\sqrt[3]{n}))$.

Cipher Key Size	Modulus Size	Elliptic Curve Size
80 bits	1024 bits	160 bits
128 bits	3072 bits	256 bits
256 bits	**15360** bits	512 bits

(μετάβαση σε ελλειπτικές καμπύλες)

Diffie-Hellman

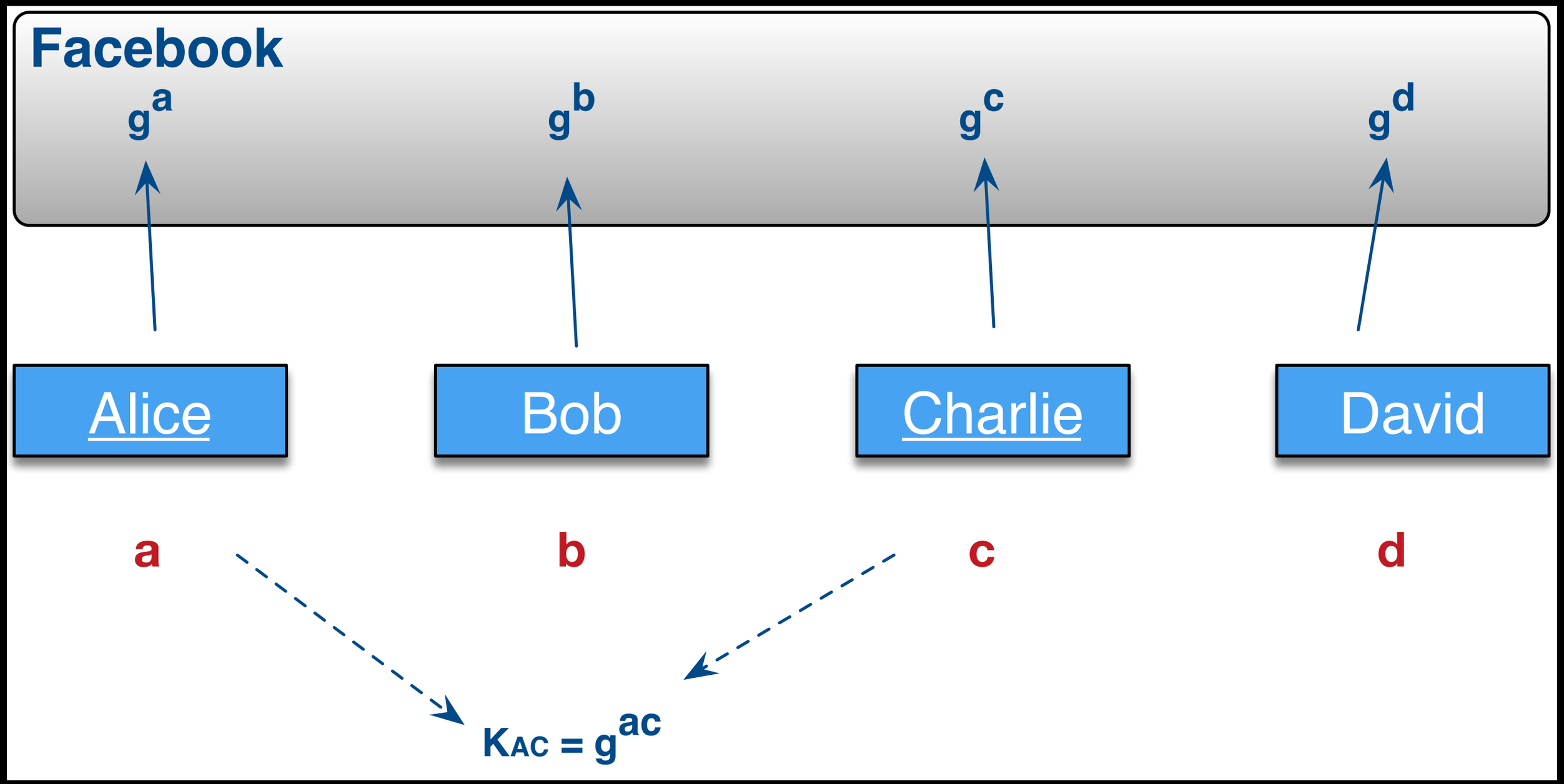
Man-in-the-Middle



Ο Αντίπαλός δεν παρατηρεί πλέον αλλά παρεμβαίνει στο δίκτυο (active attack)!

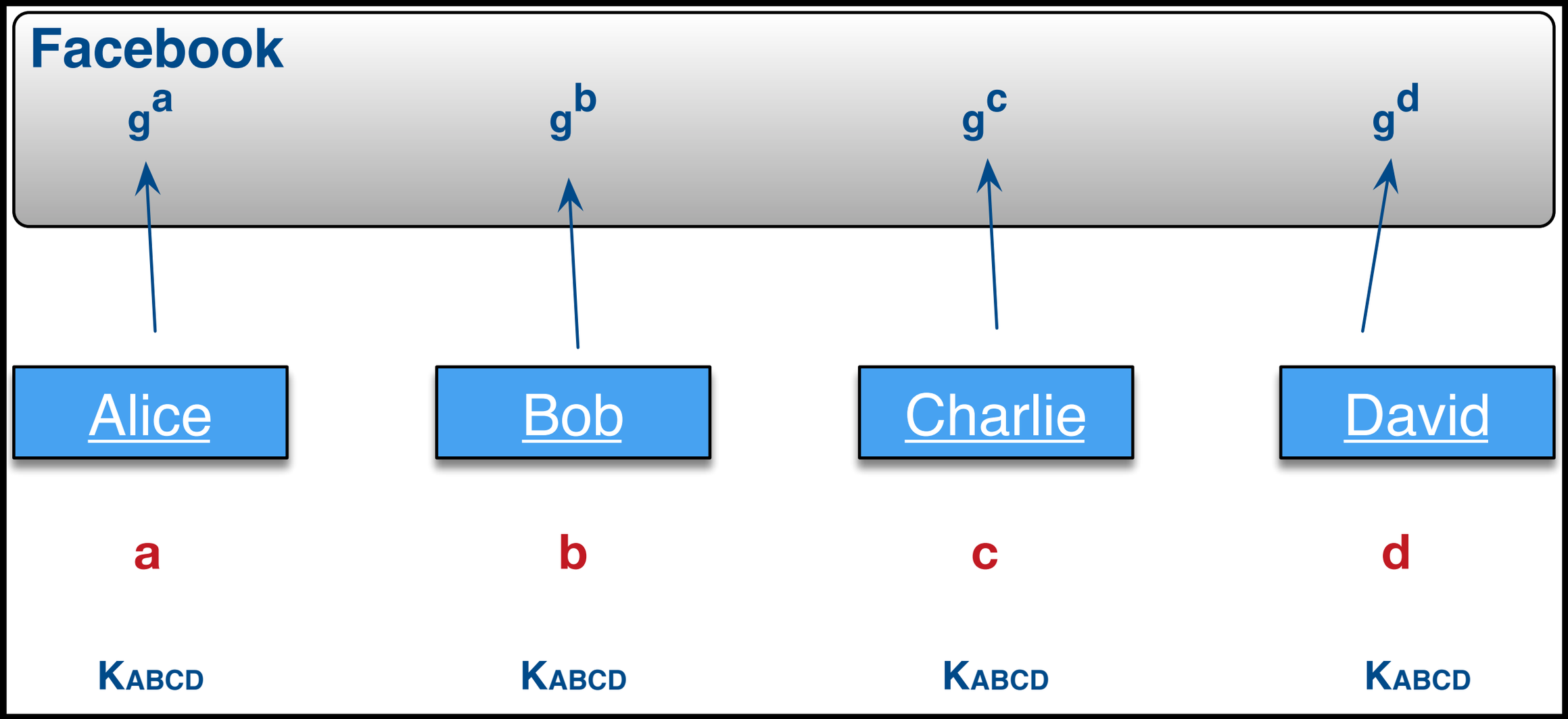
Diffie-Hellman

Μια Διαφορετική Οπτική



Diffie-Hellman

Κοινή Συνομιλία Πολλών Χρηστών (;)

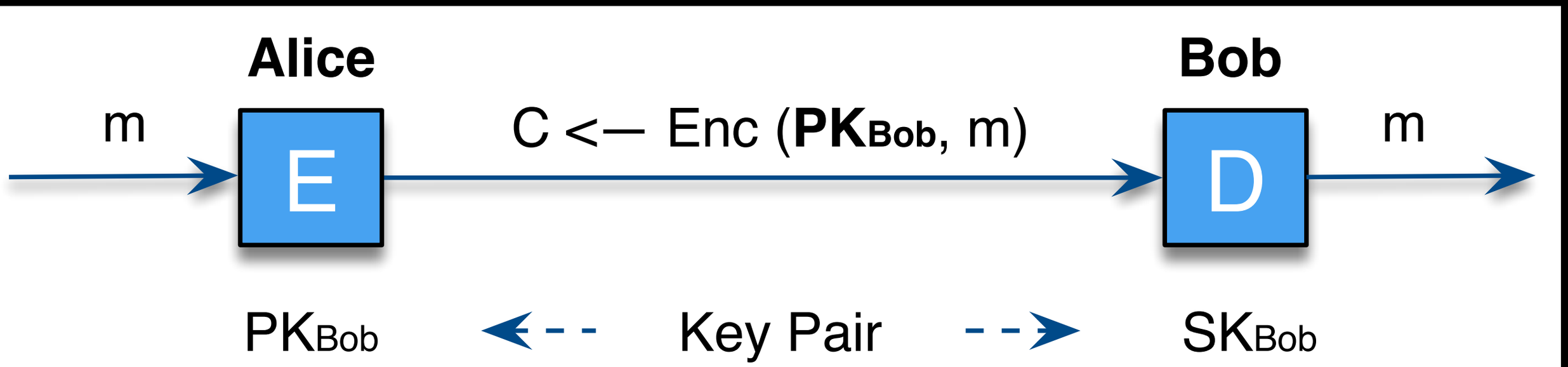


n = 2: DH

n = 3: Λύση από A. Joux (2000)

n > 3: Ανοιχτό πρόβλημα

Public Key Encryption



PK: Public Key
SK: Secret Key

Public Key Encryption
Ορισμοί

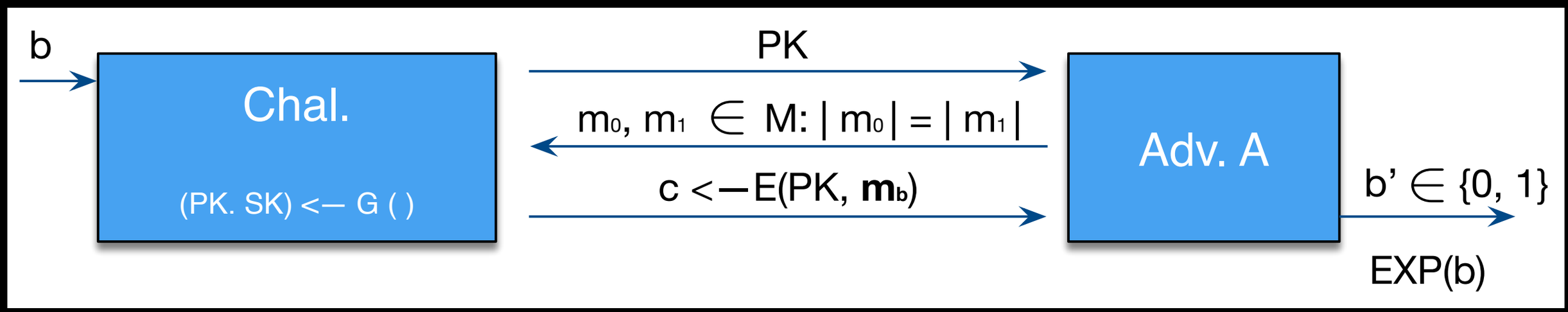
- Ένα σύστημα κρυπτογράφησης δημοσίου κλειδιού απαρτίζεται από μια τριπλέτα αλγορίθμων: (G, E, D)
    1. Όπου G έχουμε έναν ψευδοτυχαίο αλγόριθμο που δίνει ως έξοδο ένα ζευγάρι κλειδιών (PK, SK).
    2. Ο E(PK, m) είναι και αυτός ένας ψευδοτυχαίος αλγόριθμος που παίρνει σαν ορίσματα: το PK και ένα μήνυμα $m \in M$. Επιστρέφει ένα ciphertext $c \in C$.
    3. Ο D(SK, c) παίρνει ως είσοδο: το SK και το c δίνει πίσω το $m \in M$ ή $\perp$.
- Ορθότητα: $\forall$ (PK, SK) που δίνει ο G θα πρέπει
    $\forall m \in M$: D(SK, E(PK, m)) = m

Semantic Security
(Σημασιολογική Ασφάλεια)

Indistinguishability Under Chosen-Plaintext Attack

(IND-CPA)

Για b = 0, 1 έχουμε δυο πειράματα EXP(0) και EXP(1):



Ένα σύστημα $\mathcal{E}$ = (G, E, D) είναι sem. secure εαν για κάθε A:

$Adv_{ss}[A, \mathcal{E}] = | Pr[EXP(0) = 1] - Pr[EXP(1) = 1] | <$ αμελητέο

Public Key Encryption

Εγκαθίδρυση Κοινού Κλειδιού

Alice

Bob

(PK, SK) <— G ( )

“Alice”, PK

επιλογή τυχαίου
$x \in \{0,1\}^{128}$

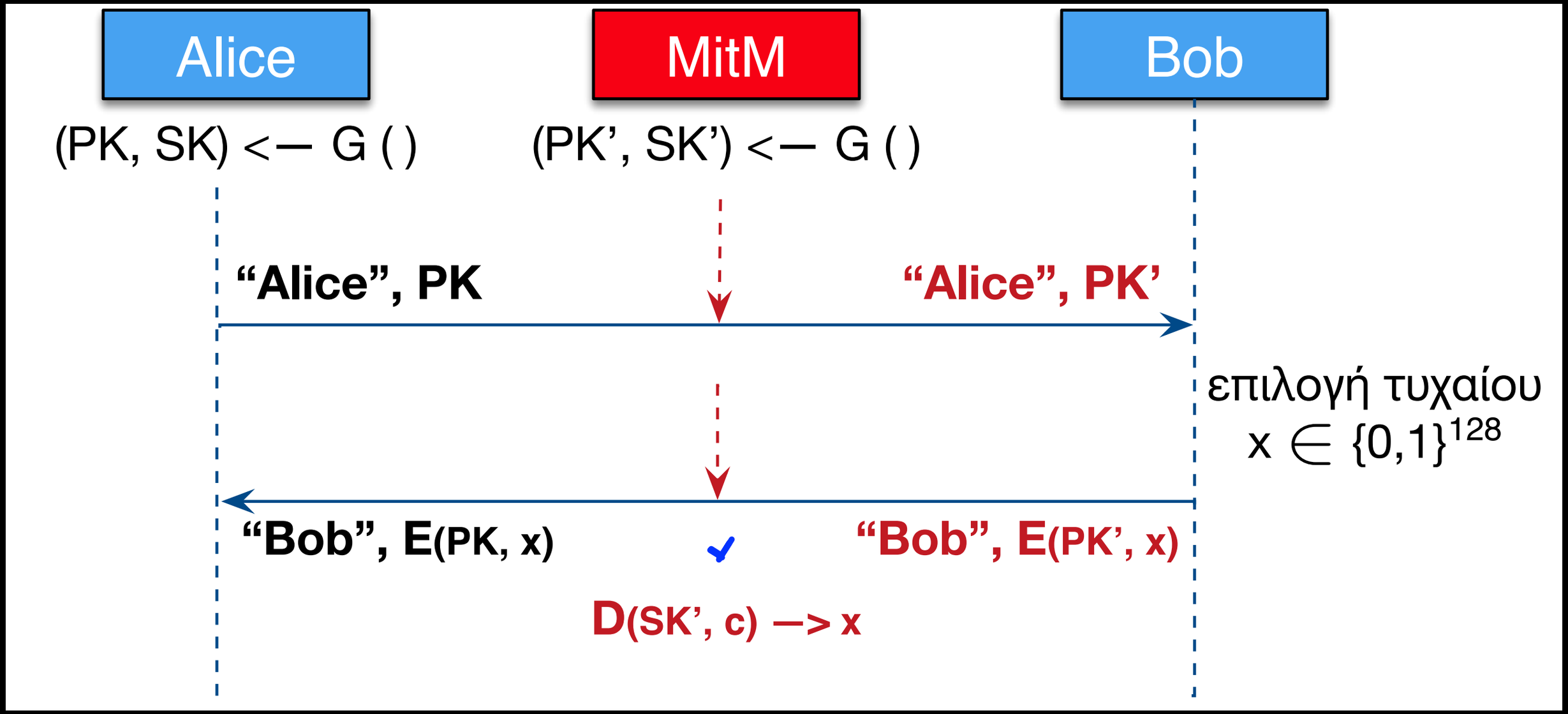
“Bob”, c <— E(PK, x)

D(SK, c) —> x

Public Key Encryption
Security

- Ο αντίπαλος βλέπει: PK, E(PK, x) και θέλει το $x \in M$.
- Δεν μπορεί να ξεχωρίσει όμως το: {PK, E(PK, x), x} από το: {PK, E(PK, x), rand $\in$ M}

Public Key Encryption
Man-in-the-Middle



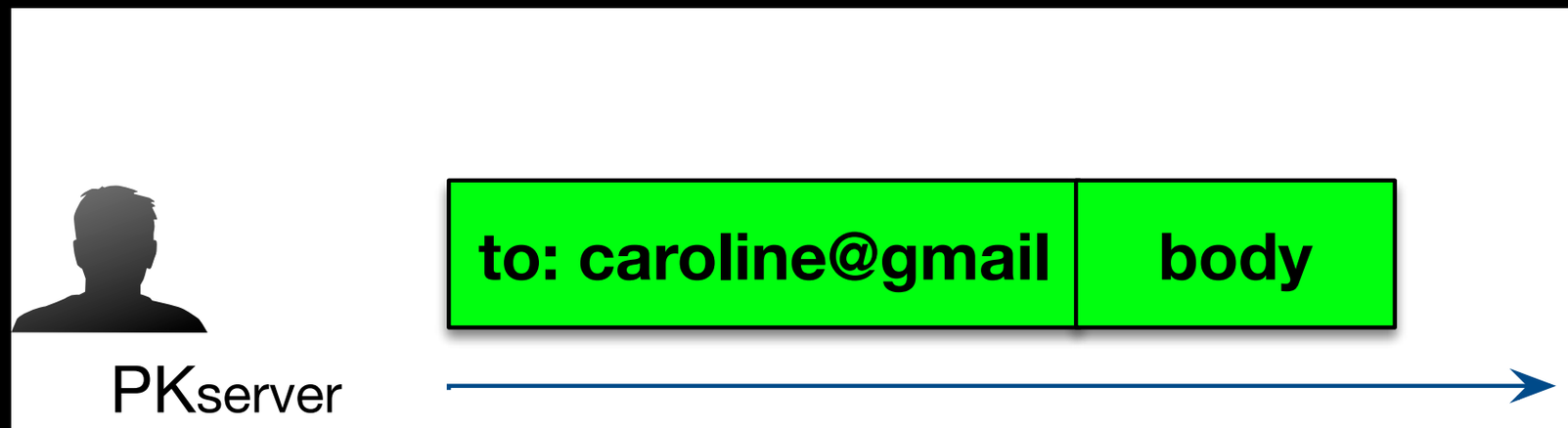
Ο Αντίπαλός παρεμβαίνει στο δίκτυο (active attack)!

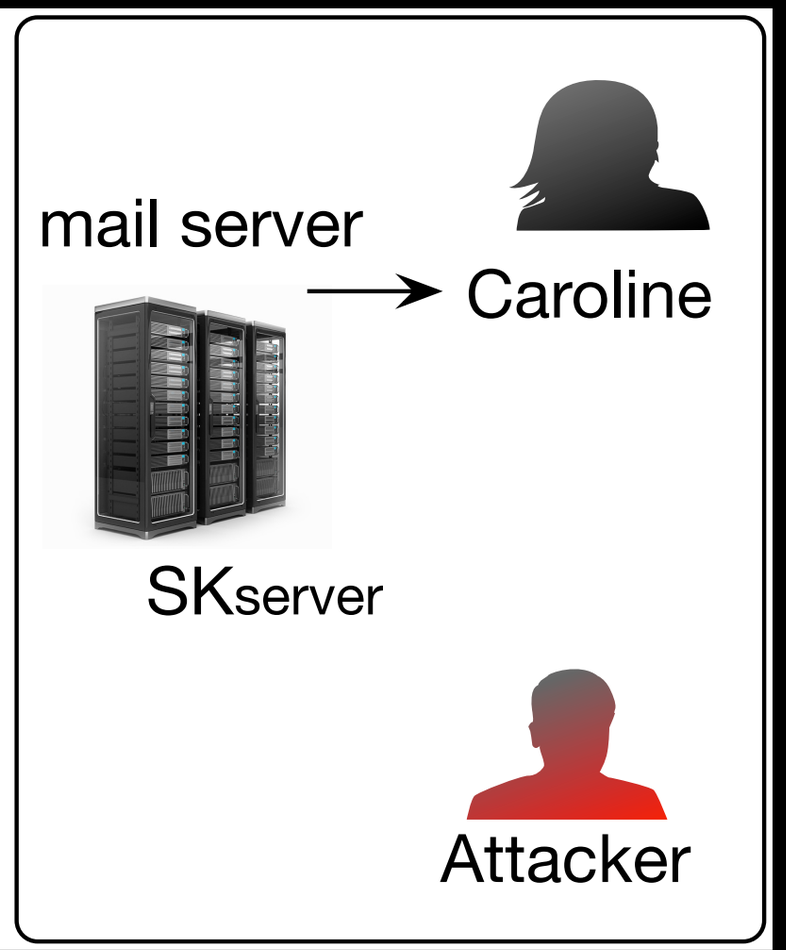
Malleability

- Ένας κρυπτογραφικός αλγόριθος είναι “εύπλαστος” (malleable) εάν ένας αντίπαλος μπορεί να αλλάξει το ciphertext ενός plaintext (m) σε ένα άλλο διαφορετικό το οποίο με τη σειρά του αντιστοιχεί σε ένα άλλο plaintext (f(m)) χωρίς να μάθει (και να μην τον ενδιαφέρει να μάθει) το m.

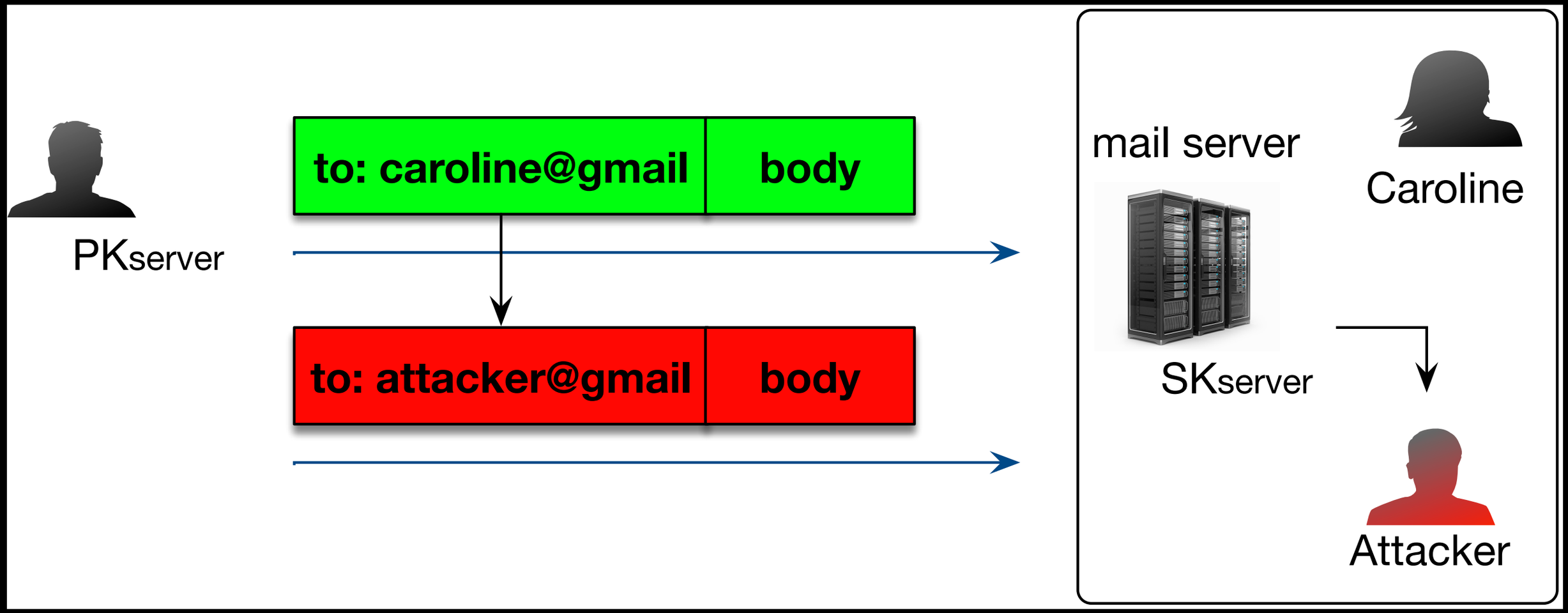
"TRANSFER $0000**1**00.00 TO ACCOUNT #199.

Απλό Σενάριο
(πιθανότητα αλλοίωσης;)





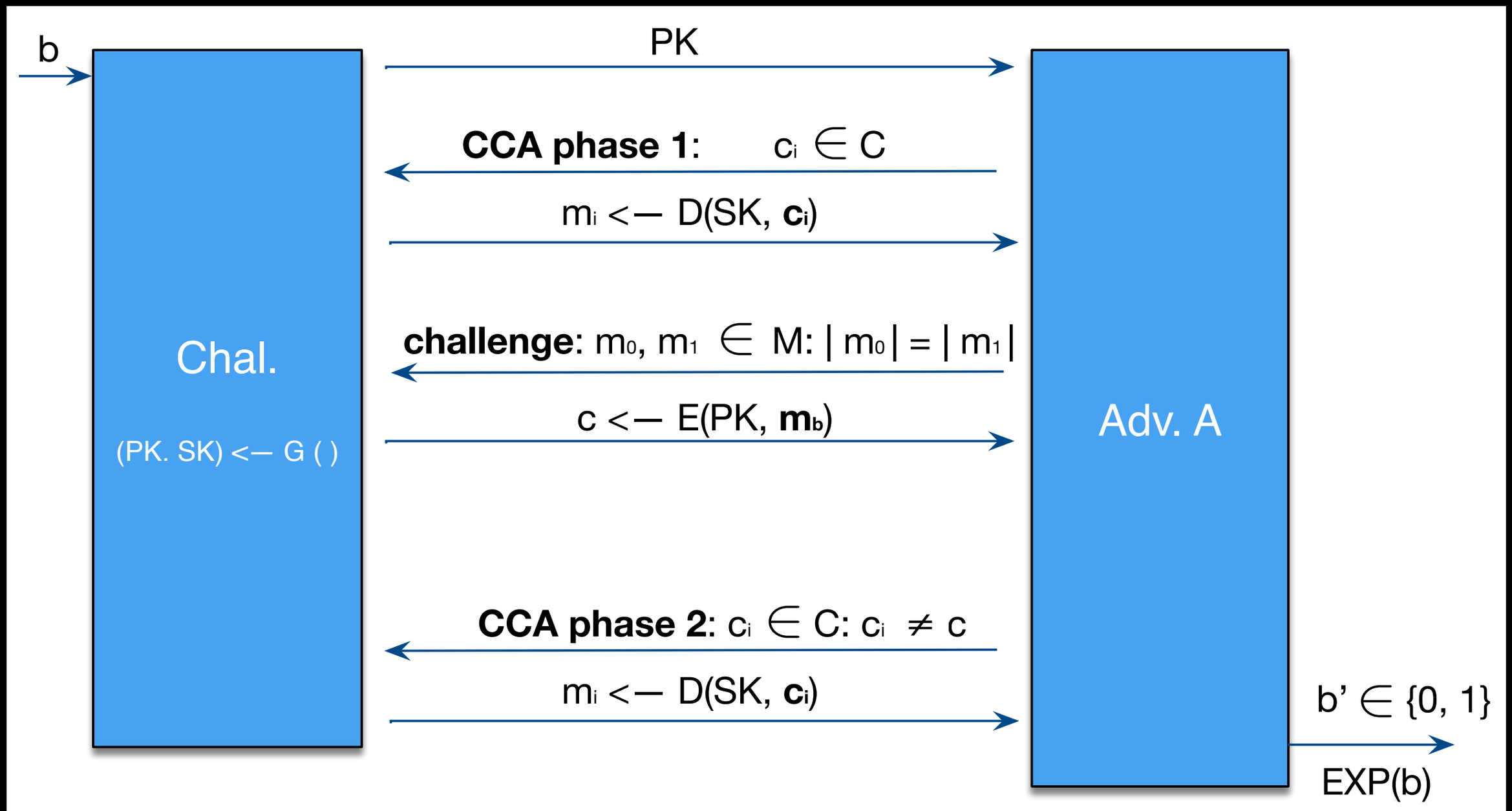
Malleability
(αλλοίωση)



Indistinguishability Under Chosen Ciphertext Attack

(IND-CCA)

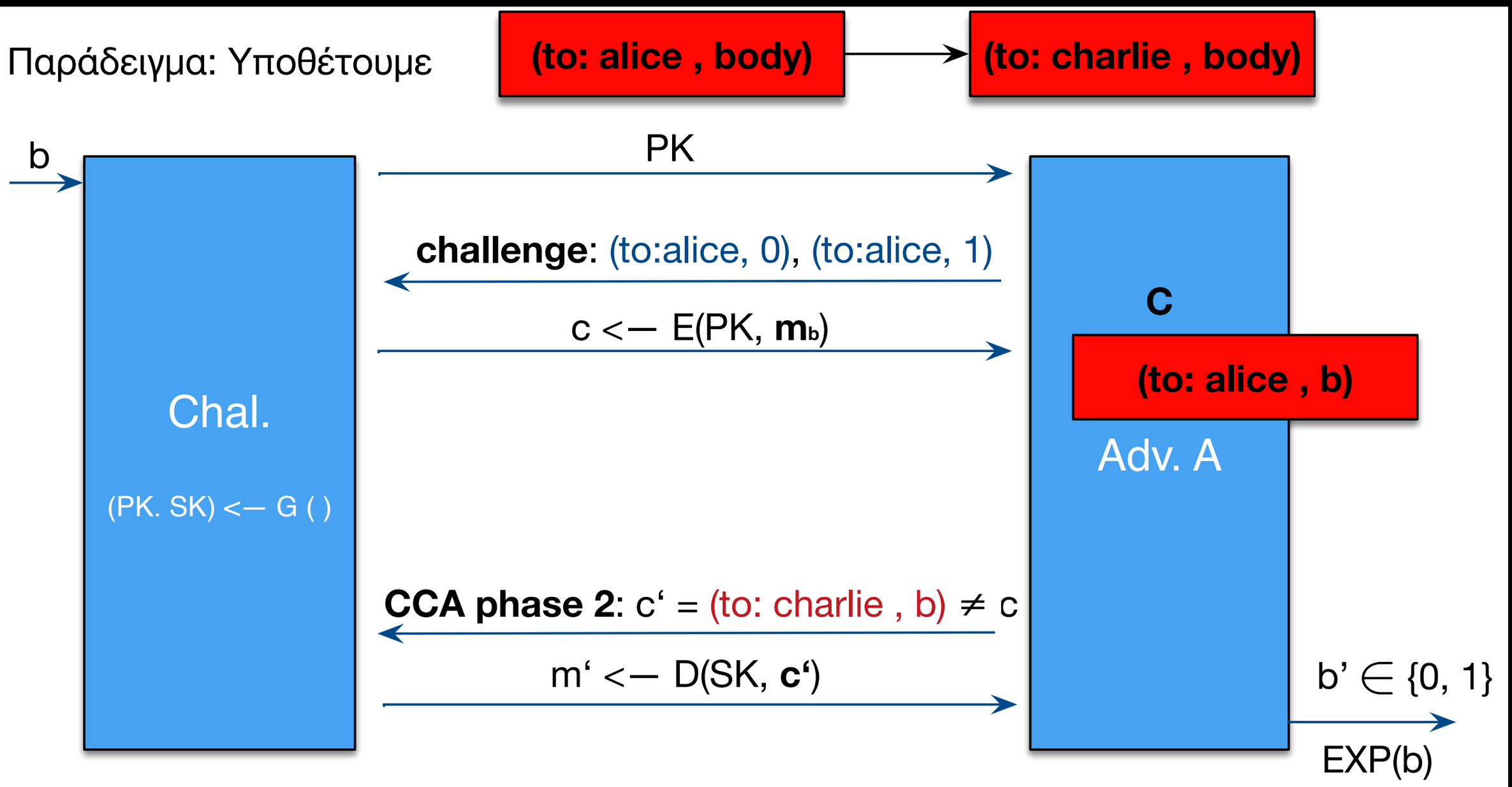
Έχουμε $\mathcal{E}$ = (G, E, D) με (M, C). Για b = 0,1 έχουμε EXP(0) και EXP(1):



IND-CCA

Το $\mathcal{E}$ = (G, E, D) είναι sem. secure εαν για κάθε A:

$Adv_{ss}[A, \mathcal{E}] = | Pr[EXP(0) = 1] - Pr[EXP(1) = 1] | <$ αμελητέο



RSA

- Αναπτύχθηκε από τους Ron Rivest, Adi Shamir, και Leonard Adleman (1977).
- Βασίζεται στη δυσκολία **παραγοντοποίησης** μεγάλων αριθμών (της τάξης των 1024 με 2048 bits).

RSA

Παραγωγή Κλειδιών

1. Επιλογή δυο τυχαίων (μεγάλων) πρώτων αριθμών p και q έτσι ώστε $p \neq q$.
2. Υπολογισμός $n = p*q$.
3. Υπολογισμός συνάρτησης Euler: $\phi(n) = (p-1)(q-1)$.
4. Επιλογή ενός αριθμού $e > 1$ έτσι ώστε: $e^{\phi(n)} \equiv 1 \bmod(n)$.
5. Υπολογισμός του d έτσι ώστε: $d \equiv e^{-1} \pmod{\phi(n)}$.

Δημόσιο Κλειδί: (n, e) — Ιδιωτικό Κλειδί: (n, d)

RSA

Κρυπτογράφηση — Αποκρυπτογράφηση

Ένα κρυπτογραφημένο μήνυμα c υπολογίζεται με τον ακόλουθο τρόπο:

$$c = m^e \bmod(n)$$

Για την αποκρυπτογράφηση:

$$m = c^d \bmod(n)$$

RSA

Διανομή Κλειδιών

Η Alice στέλνει στον Bob το δημόσιο κλειδί της (n, e) μέσα από ένα αξιόπιστο αλλά όχι απαραίτητα κρυφό μονοπάτι.

RSA

Παρατηρήσεις

Ένα plaintext m είναι κρυπτογραφημένο:

$$E(m) = m^e \bmod n$$

όπου (e,n) είναι το δημόσιο κλειδί. Δεδομένου του ciphertext, ο αντίπαλος μπορεί να κρυπτογραφήσει το **mt** για κάθε t:

$$E(m)*t^e \bmod n = (mt)^e \bmod n = E(mt)$$

hint: είναι ο RSA CCA-secure με αυτήν την μορφή;

Βιβλιογραφία

Jonathan Katz and Yehuda Lindell. Introduction to Modern *Cryptography. Chapman and Hall/CRC*; 1 edition (August 31, 2007). ISBN-10: 1584885513.

R. J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. *John Wiley & Sons, Inc.*, New York, NY, USA, 2001. ISBN 0471389226.

B. Clifford Neuman; Theodore Ts'o. "Kerberos: An Authentication Service for Computer Networks". *IEEE Communications*. 32 (9): 33–8. September 1994.

R.C. Merkle. Secure Communications Over Insecure Channels. *Communications of the ACM*, Vol. 21, No. 4, pp. 294-299, April 1978.

Barak B., Mahmoody-Ghidary M. (2009) Merkle Puzzles Are Optimal — An O(n2)-Query Attack on Any Key Exchange from a Random Oracle. In *Advances in Cryptology - CRYPTO 2009*. Lecture Notes in Computer Science, volume 5677. Springer.

Antoine Joux. A One Round Protocol for Tripartite Diffie-Hellman. In *Proceedings of the 4th International Symposium on Algorithmic Number Theory*. Springer-Verlag, London, UK, 385-394. 2000.

Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". *Communications of the ACM*. 21 (2): 120–126.