ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΚΡΥΠΤΟΓΡΑΦΙΑ

9η Διάλεξη

Κωνσταντίνου Ελισάβετ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Άδειες Χρήσης

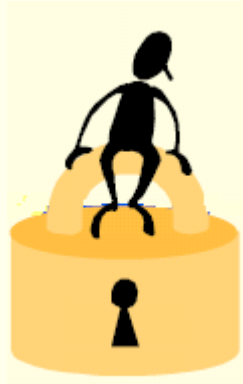
- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Κρυπτογραφία



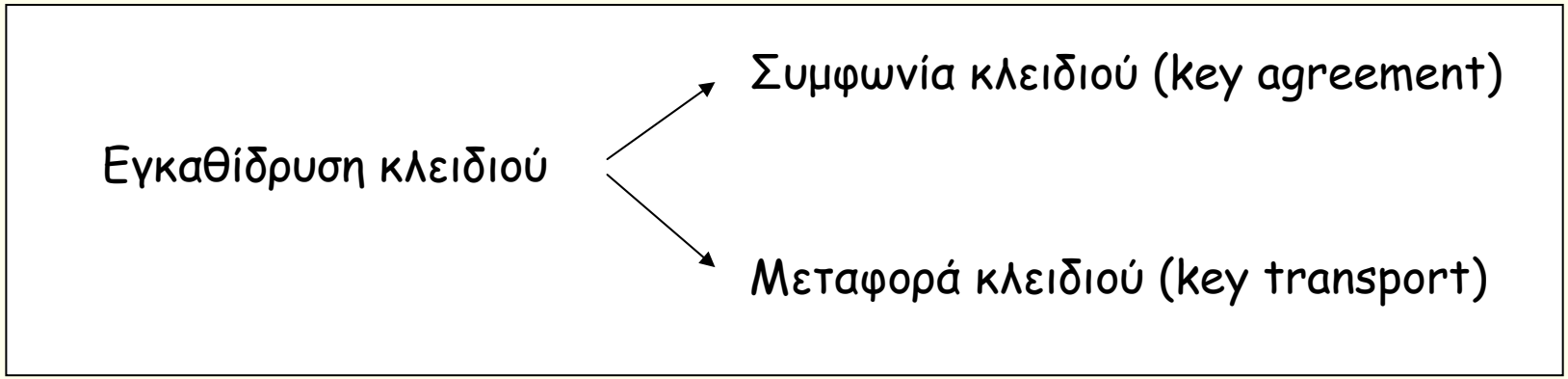
Κωνσταντίνου Ελισάβετ
ekonstantinou@aegean.gr

http://www.icsd.aegean.gr/ekonstantinou

Διαχείριση Κλειδιών

Ορισμός: Εγκαθίδρυση κλειδιού (key establishment) είναι η διαδικασία κατά την οποία ένα μυστικό κλειδί διαμοιράζεται σε δύο ή περισσότερους χρήστες.

Ορισμός: Διαχείριση κλειδιού (key management) είναι το σύνολο των μηχανισμών που υποστηρίζουν την εγκατάσταση, διατήρηση ή αντικατάσταση των κλειδιών.



Ιδιότητες

Entity authentication (πιστοποίηση οντότητας): ένα μέλος επιβεβαιώνει την ταυτότητα ενός δεύτερου που συμμετέχει στο πρωτόκολλο

Key authentication (πιστοποίηση κλειδιού): βεβαιώνεται ότι κανένας άλλος εκτός των πιστοποιημένων μελών δεν μπορεί να έχει πρόσβαση στο μυστικό κλειδί

Key confirmation (επιβεβαίωση κλειδιού): ένα μέλος επιβεβαιώνει ότι ένα δεύτερο κατέχει το μυστικό κλειδί

Explicit key authentication (σαφής πιστοποίηση κλειδιού): αν ισχύουν μαζί key authentication+key confirmation

Ιδιότητες

Ορισμός: Ένα κρυπτογραφικό σύστημα παρέχει τέλεια μυστικότητα προς τα εμπρός (perfect forward secrecy), όταν η ανακάλυψη ενός μακροπρόθεσμου μυστικού κλειδιού (long-term secret key) δεν συνεπάγεται την αποκάλυψη των κλειδιών συνόδου (session keys).

Ορισμός: Ένα κρυπτογραφικό σύστημα παρέχει τέλεια μυστικότητα προς τα πίσω (perfect backward secrecy), όταν η ανακάλυψη ενός κλειδιού συνόδου (session key) δεν συνεπάγεται την αποκάλυψη των μακροπρόθεσμων μυστικών κλειδιών (long-term secret keys).

Όταν ένα σύστημα δεν παρέχει τέλεια forward-backward μυστικότητα, τότε η ανακάλυψη ενός κλειδιού συνόδου σημαίνει και την ανακάλυψη όλων των μελλοντικών κλειδιών συνόδου

σύστημα ευπαθές σε known-key attacks

Μεταφορά κλειδιού με τεχνικές Δ.Κ.

Απλή λύση: Ένα μέλος Α επιλέγει ένα συμμετρικό κλειδί, το κρυπτογραφεί με το δημόσιο κλειδί του μέλους Β και του το στέλνει.

Το πρωτόκολλο παρέχει μόνο Πιστοποίηση κλειδιού από τη μεριά του Α. Δεν παρέχει για κανένα μέλος Πιστοποίηση οντότητας και Επιβεβαίωση κλειδιού.

Για να ικανοποιηθούν όλες αυτές οι ιδιότητες μπορούν να χρησιμοποιηθούν ψηφιακές υπογραφές ή επιπλέον ανταλλαγές μηνυμάτων (π.χ. το πρωτόκολλο των Needham-Schroeder)

Πρωτόκολλο των Needham-Schroeder

Protocol Needham-Schroeder public-key protocol

SUMMARY: A and B exchange 3 messages.
RESULT: entity authentication, key authentication, and key transport (all mutual).

1. *Notation.* $P_X(Y)$ denotes public-key encryption (e.g., RSA) of data Y using party X's public key; $P_X(Y_1, Y_2)$ denotes the encryption of the concatenation of Y_1 and Y_2. k_1, k_2 are secret symmetric session keys chosen by A, B, respectively.
2. *One-time setup.* Assume A, B possess each other's authentic public-key. (If this is not the case, but each party has a certificate carrying its own public key, then one additional message is required for certificate transport.)
3. *Protocol messages.*

$$\begin{array}{lll} A \rightarrow B: & P_B(k_1, A) & (1) \\ A \leftarrow B: & P_A(k_1, k_2) & (2) \\ A \rightarrow B: & P_B(k_2) & (3) \end{array}$$

4. *Protocol actions.*
   (a) A sends B message (1).
   (b) B recovers k_1 upon receiving message (1), and returns to A message (2).
   (c) Upon decrypting message (2), A checks the key k_1 recovered agrees with that sent in message (1). (Provided k_1 has never been previously used, this gives A both entity authentication of B and assurance that B knows this key.) A sends B message (3).
   (d) Upon decrypting message (3), B checks the key k_2 recovered agrees with that sent in message (2). The session key may be computed as $f(k_1, k_2)$ using an appropriate publicly known non-reversible function f.

Εδραίωση κλειδιού με τεχνικές Δ.Κ.

Diffie-Hellman key agreement

Protocol Diffie-Hellman key agreement (basic version)

SUMMARY: A and B each send the other one message over an open channel.
RESULT: shared secret K known to both parties A and B.

1. *One-time setup.* An appropriate prime p and generator α of $\mathbb{Z}_p^*$ ($2 \leq \alpha \leq p-2$) are selected and published.
2. *Protocol messages.*

$$A \rightarrow B : \alpha^x \bmod p \quad (1)$$
$$A \leftarrow B : \alpha^y \bmod p \quad (2)$$

3. *Protocol actions.* Perform the following steps each time a shared key is required.
   (a) A chooses a random secret x, $1 \leq x \leq p-2$, and sends B message (1).
   (b) B chooses a random secret y, $1 \leq y \leq p-2$, and sends A message (2).
   (c) B receives α^x and computes the shared key as $K = (\alpha^x)^y \bmod p$.
   (d) A receives α^y and computes the shared key as $K = (\alpha^y)^x \bmod p$.

Εδραίωση κλειδιού με τεχνικές Δ.Κ.

ElGamal key agreement in one-pass

Protocol ElGamal key agreement (half-certified Diffie-Hellman)

SUMMARY: A sends to B a single message allowing one-pass key agreement.
RESULT: shared secret K known to both parties A and B.

1. *One-time setup (key generation and publication).* Each user B does the following:
   Pick an appropriate prime p and generator α of $\mathbb{Z}_p^*$.
   Select a random integer b, $1 \leq b \leq p-2$, and compute $\alpha^b \bmod p$.
   B publishes its public key (p, α, α^b), keeping private key b secret.
2. *Protocol messages.*

$$A \rightarrow B: \quad \alpha^x \bmod p \quad (1)$$

3. *Protocol actions.* Perform the following steps each time a shared key is required.
   (a) A obtains an authentic copy of B's public key (p, α, α^b).
   A chooses a random integer x, $1 \leq x \leq p-2$, and sends B message (1).
   A computes the key as $K = (\alpha^b)^x \bmod p$.
   (b) B computes the same key on receipt of message (1) as $K = (\alpha^x)^b \bmod p$.

Εδραίωση κλειδιού με τεχνικές Δ.Κ.

MTI/A0

Protocol MTI/A0 key agreement

SUMMARY: two-pass Diffie-Hellman key agreement secure against passive attacks.
RESULT: shared secret K known to both parties A and B.

1. *One-time setup.* Select and publish (in a manner guaranteeing authenticity) an appropriate system prime p and generator α of $\mathbb{Z}_p^*$, $2 \leq \alpha \leq p-2$. A selects as a long-term private key a random integer a, $1 \leq a \leq p-2$, and computes a long-term public key $z_A = \alpha^a \bmod p$. (B has analogous keys b, z_B.) A and B have access to authenticated copies of each other's long-term public key.
2. *Protocol messages.*

$$A \rightarrow B: \quad \alpha^x \bmod p \quad (1)$$
$$A \leftarrow B: \quad \alpha^y \bmod p \quad (2)$$

3. *Protocol actions.* Perform the following steps each time a shared key is required.
   (a) A chooses a random secret x, $1 \leq x \leq p-2$, and sends B message (1).
   (b) B chooses a random secret y, $1 \leq y \leq p-2$, and sends A message (2).
   (c) A computes the key $k = (\alpha^y)^a z_B{}^x \bmod p$.
   (d) B computes the key $k = (\alpha^x)^b z_A{}^y \bmod p$. (Both parties now share the key $k = \alpha^{bx+ay} \bmod p$.)

Εδραίωση κλειδιού με τεχνικές Δ.Κ.

Station to station protocol (STS)

3. *Protocol messages.*

$$
\begin{array}{lll}
A \rightarrow B: & \alpha^x \bmod p & (1) \\
A \leftarrow B: & \alpha^y \bmod p,\ E_k(S_B(\alpha^y,\ \alpha^x)) & (2) \\
A \rightarrow B: & E_k(S_A(\alpha^x,\ \alpha^y)) & (3)
\end{array}
$$

4. *Protocol actions.* Perform the following steps each time a shared key is required. The protocol is aborted (with failure) immediately upon any signature failure.
   (a) A generates a secret random x, $1 \leq x \leq p-2$, and sends B message (1).
   (b) B generates a secret random y, $1 \leq y \leq p-2$, and computes the shared key $k = (\alpha^x)^y \bmod p$. B signs the concatenation of both exponentials ordered as in (2), encrypts this using the computed key, and sends A message (2).
   (c) A computes the shared key $k = (\alpha^y)^x \bmod p$, decrypts the encrypted data, and uses B's public key to verify the received value as the signature on the hash of the cleartext exponential received and the exponential sent in message (1). Upon successful verification, A accepts that k is actually shared with B, and sends B an analogous message (3).
   (d) B similarly decrypts the received message (3) and verifies A's signature therein. If successful, B accepts that k is actually shared with A.

Διαμοίραση μυστικού (Secret Sharing)

Πρωτοεμφανίστηκαν για την εξής εφαρμογή: για να εξασφαλιστούν τα κρυπτογραφικά κλειδιά από απώλειες, είναι επιθυμητό να κρατάμε backup copies. Αν ο αριθμός τους είναι μεγάλος μπορεί ένας επιτιθέμενος να ανακτήσει κάποιο, αν ο αριθμός είναι μικρός μπορεί να χαθούν όλα.

Η ιδέα είναι να ξεκινάμε από ένα «μυστικό», αυτό να διαιρείται σε τμήματα που καλούνται shares (μερίδια) και να διαμοιράζονται στους χρήστες.

Όταν χρειαστεί, ορισμένοι χρήστες π.χ. t από n, μπορούν να συνδυάσουν τα μερίδιά τους και να φτιάξουν ξανά το «μυστικό».

Διαμοίραση μυστικού (Secret Sharing)

(1) Διττός έλεγχος (Dual control):

έστω S ένας μυστικός αριθμός με $S < m$ για κάποιον ακέραιο m. Ένα έμπιστο μέλος Τα δημιουργεί έναν τυχαίο αριθμό $S_1 < m$ και διαμοιράζει τα μερίδια S_1 και $(S-S_1) \bmod m$ σε δύο χρήστες A και B.

Κανείς από τους δύο χρήστες δεν μπορεί να βρει το S, αλλά αν αθροίσουν και οι δύο τα μερίδια τους modulo m, τότε προκύπτει το S.

(2) Έλεγχος ομόφωνης συγκατάθεσης (unanimous consent control):

Αποτελεί γενίκευση της προηγούμενης περίπτωσης. Ο Τ μπορεί να δημιουργήσει t-1 τιμές $S_i < m$, να τις μοιράσει σε t-1 χρήστες και στον τελευταίο (t) να στείλει την τιμή $S-(S_1+\ldots+S_{t-1}) \bmod m$. Το μυστικό μπορεί να ανακτηθεί με το άθροισμα όλων των μεριδίων.

Διαμοίραση μυστικού (Secret Sharing)

3) Πρωτόκολλα κατωφλίου (threshold schemes):

Ένα (t,n) threshold scheme με $t \leq n$ είναι μια μέθοδος με την οποία ένα έμπιστο μέλος υπολογίζει με μυστικό τρόπο μερίδια S_i, με $1 \leq i \leq n$ ενός μυστικού S και τα διανέμει σε n χρήστες αντίστοιχα. Κάθε ομάδα από t ή παραπάνω χρήστες μπορεί εύκολα να βρει το μυστικό S, αλλά για κάθε μικρότερη ομάδα αυτό είναι υπολογιστικά αδύνατο.

Ένα perfect threshold scheme δεν προσφέρει καμία επιπλέον πληροφορία σε έναν επιτιθέμενο η γνώση t-1 ή λιγότερων μεριδίων του μυστικού.

Τα προηγούμενα πρωτόκολλα είναι παραδείγματα (2,2) και (t,t) πρωτοκόλλων κατωφλίου.

Shamir's threshold scheme

Mechanism Shamir's (t, n) threshold scheme

SUMMARY: a trusted party distributes shares of a secret S to n users.
RESULT: any group of t users which pool their shares can recover S.

1. *Setup*. The trusted party T begins with a secret integer $S \geq 0$ it wishes to distribute among n users.
   (a) T chooses a prime $p > \max(S, n)$, and defines $a_0 = S$.
   (b) T selects $t-1$ random, independent coefficients $a_1, \ldots, a_{t-1}$, $0 \leq a_j \leq p-1$, defining the random polynomial over $\mathbb{Z}_p$, $f(x) = \sum_{j=0}^{t-1} a_j x^j$.
   (c) T computes $S_i = f(i) \bmod p$, $1 \leq i \leq n$ (or for any n distinct points i, $1 \leq i \leq p-1$), and securely transfers the share S_i to user P_i, along with public index i.
2. *Pooling of shares*. Any group of t or more users pool their shares (see Remark 12.70). Their shares provide t distinct points $(x, y) = (i, S_i)$ allowing computation of the coefficients a_j, $1 \leq j \leq t-1$ of $f(x)$ by Lagrange interpolation (see below). The secret is recovered by noting $f(0) = a_0 = S$.

Παράδειγμα

Άσκηση: Δίνονται τα ακόλουθα μερίδια μυστικού ενός σχήματος (3, 6) – κατωφλίου: (1,26), (2,8), (3,23), (4,13), (5,7), (6,5).

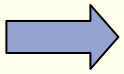
Το δημόσιο modulus είναι ίσο με 29. Βρείτε το αρχικό μυστικό.

Λύση: $f(x) = a_0 + a_1x + a_2x^2$. Κάθε σημείο είναι της μορφής $(x, f(x) \bmod 29)$. Άρα παίρνω 3 σημεία και υπολογίζω τον άγνωστο a_0.

Ιδιότητες πρωτοκόλλου του Shamir

1. Τέλειο (perfect): Γνωρίζοντας κανείς είτε t-1 ή λιγότερα μερίδια, πάλι όλες οι τιμές του μυστικού S παραμένουν εξίσου πιθανές.

2. Ιδανικό (ideal): Το μέγεθος κάθε μεριδίου είναι ίδιο με το μέγεθος του μυστικού.



η αποδοτικότητα ενός σχήματος διαμοίρασης μυστικού μετριέται με τον ρυθμό πληροφορίας (information rate), δηλαδή το αποτέλεσμα (μέγεθος σε bits του μυστικού)/(μέγεθος σε bits του μεριδίου ενός χρήστη). Ο ρυθμός πληροφορίας για όλο το πρωτόκολλο είναι ο μικρότερος ρυθμός μεταξύ όλων των χρηστών. Σε ένα τέλειο σχήμα διαμοίρασης μυστικού θα πρέπει για όλα τα μερίδια να ισχύει (μέγεθος μυστικού σε bits) ≤ (μέγεθος μεριδίου σε bits). Γιατί?

Άρα, όλα τα τέλεια σχήματα διαμοίρασης μυστικού έχουν ρυθμό πληροφορίας ≤ 1 και τα ιδανικά έχουν ρυθμό πληροφορίας ίσο με 1.

Ιδιότητες πρωτοκόλλου του Shamir

3. Εύκολα επεκτάσιμο για νέους χρήστες: Νέα μερίδια για νέους χρήστες μπορούν να δημιουργηθούν εύκολα, χωρίς να επηρεάσουν τα μερίδια των προηγούμενων χρηστών.

4. Διαφορετικά επίπεδα ελέγχου σε κάθε χρήστη: Όσα περισσότερα μερίδια έχει κάποιος, τόσο μεγαλύτερο έλεγχο έχει πάνω στο μυστικό.

5. Δεν βασίζεται σε μη αποδεδειγμένες υποθέσεις: Π.χ. στη δυσκολία επίλυσης ενός προβλήματος θεωρίας αριθμών (primality testing, factoring κ.τ.λ.)

Conference Keying

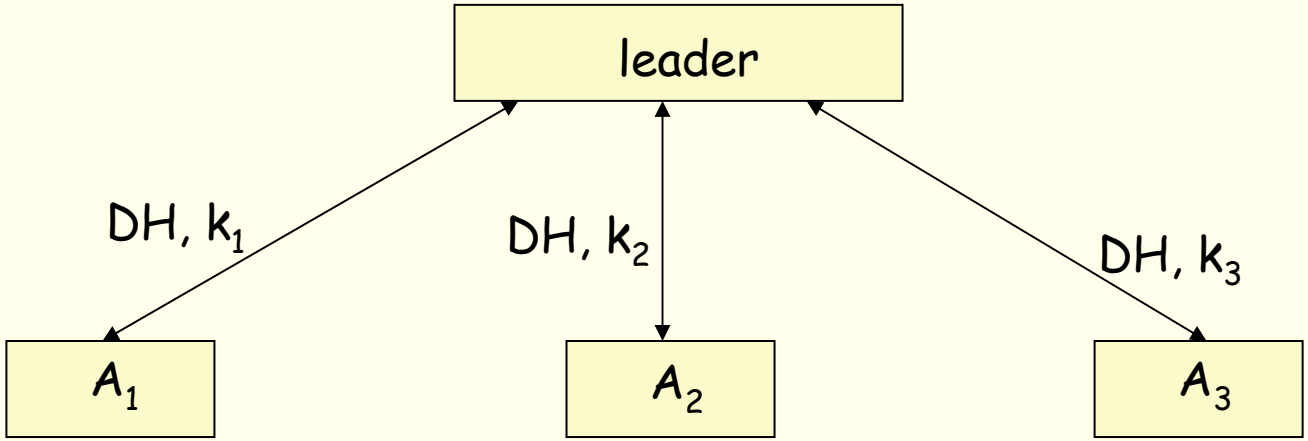
Ορισμός: Ένα πρωτόκολλο conference keying (ή group key agreement) αποτελεί μία γενίκευση της εδραίωσης κλειδιού μεταξύ 2 χρηστών, για την εδραίωση ενός μυστικού κλειδιού σε 3 ή περισσότερα μέλη.

Διαφορές τους με τα πρωτόκολλα secret sharing:

a) Διαφορετικές ομάδες χρηστών υπολογίζουν διαφορετικά κλειδιά (session keys).
b) Η πληροφορία που ανταλλάσσεται μεταξύ των χρηστών δεν είναι μυστική.
c) Κάθε χρήστης ξεχωριστά μπορεί να υπολογίσει το μυστικό κλειδί.

Conference Keying

Απλή προσέγγιση…



Μειονέκτημα: μεγάλο κόστος πάνω στον leader, δεν υπάρχει energy balance

GDH.3 Protocol

1. Κάθε μέλος M_i δημιουργεί μία τυχαία τιμή k_i. Ο M_1 επιλέγει ένα γεννήτορα α και στέλνει στον M_2 την τιμή $A_1 = \alpha^{k1} \bmod p$. Ο M_2 στέλνει στον M_3 την τιμή $A_2 = (\alpha^{k1})^{k2} \bmod p$ και ούτω καθεξής μέχρι να φτάσει στον M_{n-1}.
2. Ο M_{n-1} υπολογίζει την τιμή $A_{n-1} = \alpha^{k1k2\ldots kn-1} \bmod p$ και τη στέλνει σε όλα τα υπόλοιπα μέλη της ομάδας.
3. Κάθε μέλος M_i (εκτός του M_n) υπολογίζει την τιμή $B_i = (\alpha^{k1k2\ldots kn-1})^{1/ki} \bmod p$ και τη στέλνει στο τελευταίο μέλος της ομάδας M_n.
4. Ο M_n υπολογίζει όλες τις τιμές $B_i^{kn} \bmod p$ και τις στέλνει στο αντίστοιχο μέλος M_i της ομάδας. Τώρα κάθε μέλος μπορεί να υπολογίσει το τελικό μυστικό κλειδί από τη σχέση $K = (B_i^{kn})^{ki} \bmod p$.

Κάντε ένα παράδειγμα για 4 χρήστες.

Burmester-Desmedt (BD) protocol

Conference key generation. Any group of $t \leq n$ users (typically $t \ll n$), derive a common conference key K as follows. (Without loss of generality, the users are labeled U_0 through U_{t-1}, and all indices j indicating users are taken modulo t.)

(a) Each U_i selects a random integer r_i, $1 \leq r_i \leq p-2$, computes $z_i = \alpha^{r_i} \bmod p$, and sends z_i to each of the other $t-1$ group members. (Assume that U_i has been notified *a priori*, of the indices j identifying other conference members.)

(b) Each U_i, after receiving z_{i-1} and z_{i+1}, computes $X_i = (z_{i+1}/z_{i-1})^{r_i} \bmod p$ (note $X_i = \alpha^{r_{i+1}r_i - r_i r_{i-1}}$), and sends X_i to each of the other $t-1$ group members.

(c) After receiving X_j, $1 \leq j \leq t$ excluding $j = i$, U_i computes $K = K_i$ as

$$K_i = (z_{i-1})^{tr_i} \cdot X_i^{t-1} \cdot X_{i+1}^{t-2} \cdots X_{i+(t-3)}^{2} \cdot X_{i+(t-2)}^{1} \bmod p \qquad (12.6)$$

Κάντε ένα παράδειγμα για 4 χρήστες.

Σύγκριση πρωτοκόλλων

Communication cost: πλήθος γύρων (rounds), πλήθος μηνυμάτων που στέλνονται και λαμβάνονται, μέγεθος μηνυμάτων.

Computational cost: πλήθος exponentiations, scalar multiplication. Συνήθως δεν λαμβάνονται υπόψη οι πράξεις συμμετρικής κρυπτογράφησης-αποκρυπτογράφησης, οι συναρτήσεις κατακερματισμού κ.τ.λ.

Ποιο το κόστος των δύο πρωτοκόλλων GDH.3 και BD για κάθε μέλος της ομάδας και συνολικά?

Ασφάλεια Πρωτοκόλλων

Πρόβλημα Διακριτού Λογαρίθμου (Discrete Logarithm Problem - DLP): Δοθέντος ενός πρώτου p, ενός γεννήτορα α του $\mathbb{Z}_p^*$ και ενός στοιχείου β του $\mathbb{Z}_p^*$, να βρεθεί ακέραιος x, με $0 \le x \le p-2$, για τον οποίο $\alpha^x \equiv \beta \bmod p$.

Πρόβλημα Diffie-Hellman (Diffie-Hellman Problem - DHP): Δοθέντος ενός πρώτου p, ενός γεννήτορα α του $\mathbb{Z}_p^*$ και δύο στοιχείων $g = \alpha^x \bmod p$ και $h = \alpha^y \bmod p$, να βρεθεί η τιμή $\alpha^{xy} \bmod p$.

Τα δύο πρωτόκολλα βασίζουν την ασφάλειά τους σε γενικεύσεις του προβλήματος Diffie-Hellman.

Διάβασμα…

Κεφάλαια 12.1, 12.2, 12.5.1, 12.6-12.8 του Handbook of Applied Cryptography