Τμήμα Μηχανικών Η/Υ και Πληροφορικής Πανεπιστημίου Πατρών
CEID_NE4117: *Κατανεμημένα Συστήματα*
Ακαδημαϊκό Έτος 2025-26
Διδάσκων: Σπύρος Κοντογιάννης

2η Προγραμματιστική Άσκηση για το Σπίτι
Κατανεμημένο Σύστημα Ανταλλαγής Σύντομων Μηνυμάτων

Ανακοίνωση: Παρασκευή, 19 Δεκεμβρίου 2025 **Παράδοση:** Κυριακή, 25 Ιανουαρίου 2026
Τελευταία Ενημέρωση: Πέμπτη, 18 Δεκεμβρίου 2025

1. ΣΤΟΧΟΣ ΑΣΚΗΣΗΣ

Στην παρούσα άσκηση καλείστε να εξασκηθείτε με τη χρήση μοτίβων επικοινωνίας, τεχνικών marshalling/unmarshalling, και πρωτοκόλλων προστασίας επικοινωνιών, προκειμένου να δημιουργήσετε μια στοιχειώδη υπηρεσία (ας την ονομάσουμε **myChat**) για ανταλλαγή σύντομων μηνυμάτων κειμένου.

2. ΤΙ ΠΡΕΠΕΙ ΝΑ ΚΑΝΕΤΕ

Αν και ένα ολοκληρωμένο σύστημα ανταλλαγής σύντομων μηνυμάτων είναι ιδιαίτερα πολύπλοκο και απαιτεί να λάβει κανείς υπόψη του πολλές διαφορετικές πτυχές (πρακτικά, σχεδόν όλες) των κατανεμημένων συστημάτων, στην παρούσα εργασία θα εστιάσουμε την προσοχή μας κατά κύριο λόγο μόνο σε δύο πτυχές, στα **μοτίβα επικοινωνίας** που απαιτούνται για την υποστήριξη διάφορων μορφών ανταλλαγής μηνυμάτων, καθώς επίσης και σε θέματα **προστασίας της ιδιωτικότητας** των μηνυμάτων κατά την ανταλλαγή τους μέσα από «θορυβώδη» μέσα (π.χ., δημόσια κανάλια επικοινωνίας).

Για την υπηρεσία σας θεωρήστε τις εξής οντότητες:

- **Οντότητα Χρήστη:** Εκπροσωπεί τον πελάτη ενός τελικού χρήστη.
- **Οντότητα Μεσίτη Μηνυμάτων:** Αναλαμβάνει τον ρόλο του «μεσίτη μηνυμάτων» για την υπηρεσία myChat.

Θεωρήστε ότι ο μεσίτης μηνυμάτων έχει στην κατοχή του ένα μοναδικό **RSA-ζεύγος δημόσιου-ιδιωτικού κλειδιού** (msgBrokerPK,msgBrokerSK), το οποίο είναι αποθηκευμένο σε κρυπτογραφημένη μορφή τοπικά, με βάση κάποιο συνθηματικό κρυπτογράφησης, ώστε να ανακαλείται ΜΟΝΟ από την οντότητα που το κατέχει. Το δημόσιο κλειδί msgBrokerPK είναι εκ των προτέρων γνωστό σε όλες τις οντότητες της υπηρεσίας myChat. Κάθε χρήστης θεωρούμε ότι έχει μια μοναδική ουρά εισερχομένων, το όνομα της οποίας είναι γνωστό μόνο στον ίδιο και στον μεσίτη μηνυμάτων (δείτε πώς ακριβώς γίνεται αυτό, κατά την εγγραφή του χρήστη στην υπηρεσία). Όλες οι ουρές και τα ανταλλακτήρια που θα χρειαστείτε για την υλοποίηση των μοτίβων επικοινωνίας που θα χρειαστείτε, θα πρέπει να είναι στην πλατφόρμα της RabbitMQ. Θα χρειαστεί λοιπόν να την εγκαταστήσετε στον υπολογιστή σας, προκειμένου να υλοποιήσετε την παρούσα εργασία.

- Για κάθε <u>νέο χρήστη</u> στην υπηρεσία myChat, θα πρέπει πρώτα να προηγηθεί <u>αίτημα εγγραφής</u> του πριν από οποιαδήποτε άλλη ενέργεια:
    1. Ο χρήστης δημιουργεί (μία φορά, κατά την εγγραφή), αν δεν υπάρχει ήδη, το δικό του **RSA-ζεύγος δημόσιου-κλειδιού και ιδιωτικού-κλειδιού**, έστω (myPK,mySK). Επίσης, δημιουργεί ένα **δημόσιο αναγνωριστικό** myName (αλφαριθμητικό που παράγεται από την επιστρεφόμενη τιμή μιας συνάρτησης κατακερματισμού) από το δημόσιο κλειδί του, π.χ., εφαρμόζοντας μια συνάρτηση κατακερματισμού στο myPK, καθώς και ένα **κρυφό αναγνωριστικό μυστικής ουράς εισερχομένων**

myQueue (επίσης αλφαριθμητικό, όπως και το myName) που προκύπτει από την τιμή κατακερματισμού του ιδιωτικού κλειδιού mySK.

2. Η αίτηση εγγραφής προς τον μεσίτη μηνυμάτων περιλαμβάνει την πλειάδα [myName, myPK, myQueue], κρυπτογραφημένη με το δημόσιο κλειδί msgBrokerPK, και αποστέλλεται ασύγχρονα στον μεσίτη μηνυμάτων.

- Για κάθε νέο αίτημα εγγραφής [userName, userPublicKey, userQueue], ο μεσίτης πρώτα ελέγχει τη μοναδικότητα των πεδίων στο δικό του λεξικό αποθηκευμένων δημόσιων κλειδιών, έστω publicKeysDict, και στη συνέχεια (εφόσον είναι πράγματι μοναδικά) αποθηκεύει το ζεύγος [userPublicKey, userQueue] στο λεξικό με κλειδί-αναζήτησης το userName. Για εξασφάλιση συνέπειας στη λειτουργία του (stateful mode), ο μεσίτης, μετά από κάθε εγγραφή, αποθηκεύει το λεξικό δημόσιων κλειδιών σε κάποιο τοπικό αρχείο του, ώστε να το επαναφορτώνει σε κάθε (επαν)εκκίνησή του. Τέλος, ενημερώνει τον χρήστη για την επιτυχή ολοκλήρωση της εγγραφής.

- Για κάθε ήδη εγγεγραμμένο χρήστη, προσφέρονται οι εξής λειτουργίες:

1. **Αποστολή μεμονωμένου μηνύματος προς ήδη εγγεγραμμένο παραλήπτη.** Ο παραλήπτης υποδεικνύεται με το όνομά του, αν ο αποστολέας δεν γνωρίζει ήδη το δημόσιο κλειδί του (το οποίο θα παραλάβει από τον μεσίτη).
    a. Αν ο αποστολέας έχει ήδη το δημόσιο κλειδί του παραλήπτη, τότε υποβάλλει (μέσα από το δημόσιο κανάλι) στον μεσίτη μηνυμάτων την πλειάδα [senderName, receiverName, msgTheme, encrypted_for_recipient(msgBody)]. Η συγκεκριμένη πληροφορία θα πρέπει να κρυπτογραφηθεί με το msgBrokerPK πριν αποσταλεί στον μεσίτη.
    b. Αν ο αποστολέας δεν έχει το δημόσιο κλειδί του παραλήπτη, θα πρέπει πρώτα να ζητήσει από τον μεσίτη μηνυμάτων να του το αποστείλει.
    c. Ο μεσίτης παραλαμβάνει την πλειάδα [senderName, receiverName, msgTheme, encrypted_for_recipient(msgBody)] και ελέγχει αν είναι εγγεγραμμένοι τόσο ο αποστολέας όσο και ο παραλήπτης. Αν όχι, αποστέλλεται μήνυμα απόρριψης στον αποστολέα, μέσω του δημόσιου καναλιού, κρυπτογραφημένο με το senderPK. Διαφορετικά, προωθεί το [senderName, receiverName, msgTheme, encrypted_for_recipient(msgBody)] στην κρυφή ουρά εισερχομένων του παραλήπτη.

2. **Παραλαβή εισερχόμενων μηνυμάτων από γραμματοκιβώτιο εισερχομένων.** Κάθε εγγεγραμμένος χρήστης, όταν συνδέεται στην υπηρεσία myChat, παραλαμβάνει όλα τα εκκρεμή μηνύματα από τη δική του κρυφή ουρά εισερχομένων. Αν έχει ζητηθεί κάτι τέτοιο, απαντά με δικό του μήνυμα επιβεβαίωσης-παραλαβής προς τον αποστολέα.

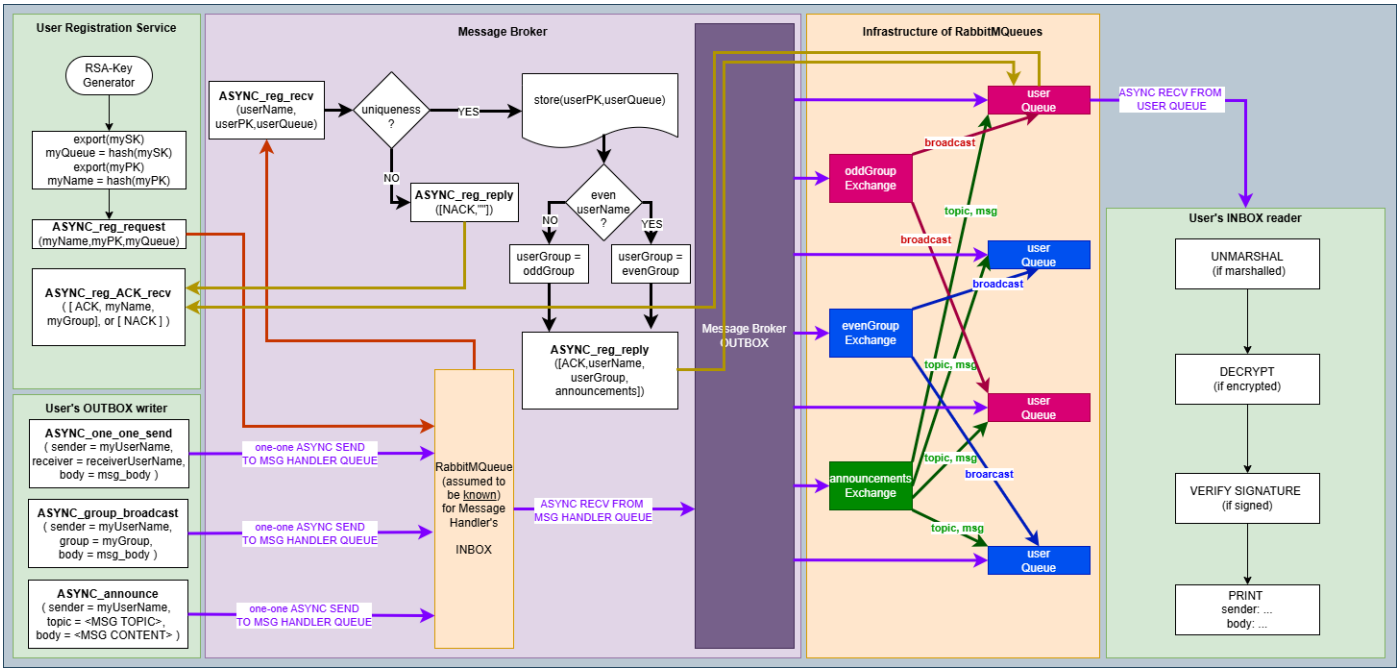
3. **Υποβολή πρόσκαιρων (transient) ανακοινώσεων.** Κάθε εγγεγραμμένος χρήστης μπορεί να «αναρτήσει» μια νέα ανακοίνωση σε έναν **πίνακα πρόσκαιρων ανακοινώσεων**, την οποία θα παραλάβουν όσοι από τους ήδη συνδεδεμένους χρήστες έχουν εκδηλώσει ενδιαφέρον για το θέμα (topic) της συγκεκριμένης ανάρτησης (οι μη συνδεδεμένοι χρήστες τη στιγμή της ανακοίνωσης απλά θα χάσουν το συγκεκριμένο μήνυμα). Αρχικά στέλνεται στον μεσίτη μηνυμάτων η ανακοίνωση, ο οποίος αναλαμβάνει στη συνέχεια να την υποβάλει στο **ανταλλακτήριο πρόσκαιρων ανακοινώσεων** που θα χρησιμοποιηθεί για τον συγκεκριμένο πίνακα πρόσκαιρων ανακοινώσεων. Οι χρήστες που ενδιαφέρονται θα πρέπει να συνδεθούν στο **ανταλλακτήριο πρόσκαιρων ανακοινώσεων** με δική τους πρωτοβουλία.

4. **Υποβολή εμμενουσών (persistent) ανακοινώσεων.** Κάθε εγγεγραμμένος χρήστης μπορεί να «αναρτήσει» (όχι άμεσα, αλλά μέσω του μεσίτη) μια νέα ανακοίνωση σε έναν **πίνακα εμμενουσών ανακοινώσεων**, την οποία θα παραλάβουν στις λίστες εισερχομένων τους όσοι από τους (συνδεδεμένους ή μη) χρήστες έχουν εκδηλώσει ενδιαφέρον για το θέμα (topic) της συγκεκριμένης ανάρτησης. Κάθε εμμένουσα ανακοίνωση αποστέλλεται στον μεσίτη μηνυμάτων, ο οποίος αναλαμβάνει στη συνέχεια να την υποβάλει στο κατάλληλο ανταλλακτήριο που θα χρησιμοποιηθεί για τον συγκεκριμένο πίνακα εμμενουσών ανακοινώσεων. Οι χρήστες που ενδιαφέρονται θα πρέπει να συνδεθούν στο **ανταλλακτήριο εμμενουσών ανακοινώσεων** με δική τους πρωτοβουλία.

5. **Πρόσκαιρη πολυμετάδοση**. Αποστολή μηνύματος προς όλα τα μέλη της ομάδας χρηστών evenGroup, στην οποία εγγράφονται όλοι οι χρήστες με άρτιο userName.

6. **Εμμένουσα πολυμετάδοση.** Αποστολή μηνύματος προς όλα τα μέλη της ομάδας χρηστών oddGroup, στην οποία εγγράφονται όλοι οι χρήστες με περιττό userName.

Ακολουθεί μια (πολύ συνοπτική, περισσότερο για να δώσει τη βασική ιδέα) περιγραφή της αρχιτεκτονικής για τη ζητούμενη υπηρεσία myChat (στην αναφορά σας, αρκετά πράγματα θα πρέπει να γίνουν πιο συγκεκριμένα).



3. ΒΟΗΘΗΤΙΚΟ ΥΛΙΚΟ

Για την εκπόνηση της παρούσας εργασίας, θα σας φανούν ενδεχομένως χρήσιμες οι εξής βιβλιοθήκες της Python:

- Socket: https://docs.python.org/3/library/socket.html
- Pickle: https://docs.python.org/3/library/pickle.html
- RabbitMQ: https://www.rabbitmq.com/
- Erlang / OTP: https://www.erlang.org/
- Cryptodome: https://pypi.org/project/pycryptodomex/

Επίσης, στα ΕΓΓΡΑΦΑ του e-class θα βρείτε τον φάκελο LAB-2 : Συνοδευτικό Υλικό όπου έχει τοποθετηθεί βοηθητικός κώδικας επίδειξης (demo) για την εφαρμογή βασικών τεχνικών κρυπτογράφησης /

αποκρυπτογράφησης / υπογραφής εγγράφων, με χρήση RSA-ζεύγους δημόσιου-ιδιωτικού κλειδιού και προσωρινών AES-κλειδιών συνόδου.

4. ΠΑΡΑΔΟΣΗ ΕΡΓΑΣΙΑΣ

Δημιουργήστε τα εξής αρχεία:

(α) Ένα **ZIP αρχείο** με το όνομα **LAB2_CODE_<STUDENT NAME>_<STUDENT ID>.zip** με τον κώδικά σας.

(β) Μια **αναφορά** (το πολύ 10 σελίδες) με το όνομα **LAB2_REPORT_<STUDENT NAME>_<STUDENT ID>.docx** όπου θα αποτυπώνετε όλες τις λεπτομέρειες του δικού σας σχεδιασμού της υπηρεσίας myChat, αναδεικνύοντας και αιτιολογώντας κάθε φορά όλες τις δικές σας σχεδιαστικές επιλογές. Επίσης, στη γραπτή αναφορά σας θα πρέπει να δώσετε, συνοπτικά, και τα εξής:

- Ένα υποτυπώδες **εγχειρίδιο χρήστη** για το πρόγραμμά σας, δίνοντας τη σύνταξη, την είσοδο, την έξοδο των μεθόδων που υλοποιήσατε.
- Κάποια **παραδείγματα εκτέλεσης** για την τεκμηρίωση των προτερημάτων και των αδυναμιών για κάθε μέθοδο επίλυσης, σχολιάζοντας τις επιδόσεις τους.