Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων & Μηχανικων Υπολογιστων

project RSA και Rabin-Williams

Στοιχεία Θεωρίας Αριθμών& Εφαρμογές στην Κρυπτογραφία

Ονοματεπώνυμο Σπουδαστών:

Θανάσης Ανδρεου
Γιώργος Παπαδοπουλος

Κρυπτοσύστημα RSA

- Κρυπτοσύστημα δημοσίου κλειδιού.
- Δημοσιεύτηκε το 1978 απο τους Ron Rivest, Adi Shamir και Leonard Adleman
- Στηρίζεται στη δυσκολία του factoring.

Κρυπτοσυστημα RSA - Παραγωγη κλειδιων

- Επίλογή δύο τυχαίων μεγάλων πρώτων αριθμών p και q.
- Υπολογισμός $N = pq$
- Υπολογισμός του $\phi(N) = (p-1)(q-1)$
- Επιλογή ένος τυχαίου αριθμού e τέτοιου ώστε:
  - $0 <$e$ < \phi(N)$,
  - $($e$,\phi(N)) = 1$.
  - Το e δημοσιεύεται ως το δημόσιο κλειδί για την κρυπτογράφηση του μηνύματος.
- Υπολογισμός του αντιστρόφου του e
  - $ed \equiv 1 \pmod{\phi(N)}$
  - Το d κρατείται κρυφό και είναι το ιδιωτικό κλειδί.

Κρυπτοσύστημα RSA - Κρυπτογράφηση & Αποκρυπτογράφηση

- $E(m) = m^e \underline{\bmod} N.$
- $D(c) = c^d \underline{\bmod} N$

Υλοποιηση RSA - Ευρεση Πρωτων

- Γλώσσα προγραμματισμου: Java
- Ευκολία διαχείρησης μεγάλων αριθμών.με χρήση της κλάσης BigInteger.
- Test Miller-Rabin
- Εκτελέστη για 1000 τυχαίους αριθμούς $\rightarrow$ Πιθανότητα λάθους: $\frac{1}{4^{1000}}$

Υλοποιηση RSA - Υπολογισμος Κλειδιων (1)

- Υπολογισμός πρώτων αριθμων p, q μεγέθους 1024 bits.
- Μορφή πρώτων: $11x...x1$.
  - Εγγυημένα το γινόμενο τους είναι 2048 bits
  - Καλό μέγεθος σύμφωνα με τον Shamir.
- $N = pq$
- $\phi(N) = (p-1)(q-1)$

Υλοποιηση RSA - Υπολογισμος Κλειδιων (2)

- Εύρεση e:
  1. Δημιουργία τυχαίου πρώτου αριθμού.
  2. Έλεγχος, αν είναι σχετικά πρώτος με το $\phi(N)$.
  3. Αν είναι βρήκαμε το e!
  4. Αν δεν είναι πρόσθεσε και πήγαινε στο βήμα 2.
- Υπολογισμός του ιδιωτικού εκθέτη d : $ed \equiv 1 \pmod{\phi(N)}$
  - Χρήση του αλγόριθμου Extended GCD.

Υλοποιηση RSA - Αναγνωση Μηνυματος

- Χρήση κλάσης BufferedInputStream:
  - Ανάγνωση αρχείου σε τμήματα του N.
  - Ανάγνωση ως binary και όχι ώς ASCII.
- Μέγεθος των τμημάτων του μηνύματος επιλέχθηκε αυθαιρετα ώς 1024 bits $=$ 128 bytes
  - Θα μπορούσε να χρησημοποιηθεί οποιόδηποτε μέγεθος από $1 - 255$ bytes
- Βλέπουμε τα τμήματα του μυνήματος ως έναν αριθμό.
  - Μέσω της κλάσης BigInteger μετατρέπουμε το byteArray σε BigInteger.

Υλοποιηση RSA - Αποθηκευση Κρυπτοκειμενου

- Χρήση κλάσης BufferedOutputStream για τους ίδιους λόγους.
- Το κάθε κρυπτογραφημένο τμήμα μύνηματος έχει αυθαίρετη τιμή στο $\mathbb{Z}_N^*$
  - $\Rightarrow$ Αριθμός bytes από $1 - 256$
  - Χρήση αριστερού padding με 0 έτσι ώστε κάθε κρυπτογραφημένο τμήμα να έχει σταθερό μέγεθος 256 bytes.

Υλοποιηση RSA - Παρατηρησεις

- Για τις υπόλοιπες πράξεις με μεγάλους αριθμούς, όπως ύψωση σε δύναμη $\bmod N$ η BigInteger μας παρέχει αποδοτικές και εύχρηστες μεθόδους.
- Η εύρεση των πρώτων είναι σχετικά χρονοβόρα διαδικασία (20-30 δευτερόλεπτα), γιατί η πιθάνοτητα να βρεθεί με τυχαίες δοκιμές τόσο μεγάλος πρώτος είναι σχετικά μικρή.

Κρυπτοσύστημα Rabin-Williams

- Παραλλαγή του Rabin ώστε η κρυπτογράφηση να μην είναι διφορούμενη.
- Δημοσιεύτηκε το 1996 απο τον Hugh Williams.
- Όπως και στο Rabin η αποκατάσταση του αρχικού κειμένου από το κρυπτοκείμενο είναι το ίδιο δύσκολη με το factoring.

Κρυπτοσύστημα Rabin-Williams - Παραγωγη κλειδιων

- Επίλογή δύο τυχαίων μεγάλων πρώτων αριθμών p και q, με $p \equiv 3 \pmod 8$ και $q \equiv 7 \pmod 8$.
- Υπολογισμός δημοσίου κλειδιού $N = pq$, για το οποίο θα ισχύει $N \equiv 5 \pmod 8$
- Υπολογισμός ιδιωτικού κλειδιού $d = \frac{\frac{(p-1)(q-1)}{4}+1}{2}$.

Κρυπτοσύστημα Rabin-Williams - Κρυπτογράφηση

- $E_1 = \begin{cases} 4(2M+1), \text{ αν } (\frac{2M+1}{N}) = 1 \\ 2(2M+1), \text{ αν } (\frac{2M+1}{N}) = -1 \end{cases}$
- $C = {E_1}^2 \underline{\text{mod}} N$

Κρυπτοσύστημα Rabin-Williams - Αποκρυπτογράφηση

- $D_1 = C^d \underline{\mod} N$
- $M = \begin{cases} \frac{\frac{D_1}{4}-1}{2}, \text{ αν } D_1 \equiv 0 \pmod 4 \\ \frac{\frac{N-D_1}{4}-1}{2}, \text{ αν } D_1 \equiv 1 \pmod 4 \\ \frac{\frac{D_1}{2}-1}{2}, \text{ αν } D_1 \equiv 2 \pmod 4 \\ \frac{\frac{N-D_1}{2}-1}{2}, \text{ αν } D_1 \equiv 3 \pmod 4 \end{cases}$

Κρυπτοσύστημα Rabin-Williams - Γενικές Πληροφορίες

- Ασφάλεια: οποιοδήποτε κρυπτογραφικό σχήμα είναι τόσο δύσκολο όσο το factoring, είναι τελείως απροστάτευτο σε Chosen-Ciphertetx Attack.
- Παραλλαγές: αντί να υψώνουμε εις το τετράγωνο το μύνημα, το υψώνουμε είς τον κύβο. Επίσης οι πρώτοι αριθμοί πρέπει να είναι $p \equiv q \equiv 1 \pmod 3$.

Υλοποιηση Rabin-Williams

- Στο μεγαλύτερο μέρος της διαδικασίας χρησιμοποιήθηκαν παρόμοια εργαλεία με αυτά που χρησιμοποιήθηκαν στο RSA.
- Διαφορετική διαδικασία για εύρεση πρώτων
- Υλοποίηση του αλγόριθμου υπολογισμού του συμβόλου Jacobi

Υλοποιηση Rabin-Williams - Ευρεση Πρωτων

- Πριν εκτελεστεί το test Miller-Rabin γίνεται έλεγχος για το άν ο αριθμός που δημιουργήθηκε είναι $\equiv 3 \pmod 8$ για τον πρώτο και $\equiv 7 \pmod 8$ για τον δεύτερο.

Υλοποιηση Rabin-Williams - Σύμβολο Jacobi

- Υλοποίηση αναδρομικού αλγορίθμού με χρησιμοποιώντας τους κανόνες:
  - $(\frac{1}{n}) = 1$.
  - $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$.
  - $(\frac{2}{n}) = 1$ αν $\frac{n^2-1}{8}$ είναι άρτιος, -1 αλλιώς.
  - $(\frac{a}{n}) = (\frac{a \bmod n}{n})$.
  - $(\frac{a}{n_1 n_2}) = (\frac{a}{n_1})(\frac{b}{n_2})$
  - Αν $(a, n) = 1$ και a, b είναι περιττά:
    - $(\frac{a}{n}) = (\frac{n}{a})$, αν $\frac{(a-1)(b-1)}{4}$ είναι άρτιος.
    - $(\frac{a}{n}) = -(\frac{n}{a})$, αν $\frac{(a-1)(b-1)}{4}$ είναι περιττός.

Υλοποιηση Rabin-Williams - Αναγνωση Μηνυματος

- Μέγεθος των τμημάτων του μηνύματος ορίστηκε πάλι ως 1024 bits $=$ 128 bytes
  - Για το M πρέπει να ισχύει $2(2M+1) < N$, αν $(\frac{2M+1}{N}) = -1$ και $4(2M+1) < N$, αν $(\frac{2M+1}{N}) = 1$.
  - Σε κάθε περίπτωση $=$ 128 bytes $< \frac{N}{8} - 1$

Υλοποιηση Rabin-Williams - Παρατηρησεις

- Πιό γρήγορη από την υλοποίηση του RSA:
  - Ίσως ο έλεγχος για $p \equiv 3 \pmod 8$ και $q \equiv 7 \pmod 8$ αυξάνει και την πιθανότητα να είνα ένας αριθμός πρώτος.
  - Απλά υψώνουμε στο τετράγωνο $\rightarrow$ δε χρειάζεται χρόνος για υπολογισμό του e

Ερωτησεις...