30/3/2017

Χρήση του RSA

Έστω ότι η Αλίκη έχει δημοσιοποιήσει τα n, e μέσω του RSA. Ο Μπόμπος μπορεί να χρησιμοποιήσει ένα πιο γρήγορο πρωτόκολλο που είναι πιο γρήγορο από το RSA για να επικοινωνήσει μαζί της. Η διαδικασία που θα πρέπει να ακολουθήσει είναι η εξής:

1. Ο Β δημιουργεί αυθαίρετα το K.
2. Ο Β κρυπτογραφεί το K με $C=K^e \bmod n$.
3. Ο Β κρυπτογραφεί το K με κάποιο γρήγορο πρωτόκολλο C'=encrypt(M,K).
4. Ο Β στέλνει τα (C, C') στην Α.
5. Η Α αποκρυπτογραφεί το C με $K=C^d \bmod n$.
6. Η Α αποκρυπτογραφεί το C' με M=decrypt(C',K)

Στην ουσία χρησιμοποιούμε το RSA σε συνδυασμό με ένα πρωτόκολλο συμμετρικού κλειδιού.

Γιατί και αυτή η μορφή του RSA είναι ανασφαλής;

- Το RSA είναι ντετερμινιστικό πρωτόκολλο.

- Είναι ευάλωτο σε επιθέσεις όπως οι παρακάτω:

Έστω ότι το K έχει μήκος 64 bit. Τότε μπορούμε να βρούμε την τιμή του αν προσπαθήσουμε να αποκρυπτογραφήσουμε το C με όλους τους δυνατούς συνδυασμούς. Ένας τρόπος να αντιμετωπίσουμε αυτή την επίθεση είναι να αυξήσουμε το μήκος του σε 2^{64}.

Όμως υπάρχει πιθανότητα (περίπου 20%) το $K=K_1K_2$ όπου $K_1, K_2 \leq 2^{34}$

$$K = K_1 \cdot K_2 \Rightarrow$$
$$C = K^e = (K_1 \cdot K_2)^e \Rightarrow$$

Τότε:
$$C = K^e = K_1^e \cdot K_2^e \Rightarrow$$
$$C(K_1^{-1})^e = K_1^e K_2^e (K_1^{-1})^e \Rightarrow$$
$$C(K_1^{-1})^e = K_2^e$$

Άρα μπορούμε να φτιάξουμε ένα λεξικό: $C(1^{-1})^e$
$C(2^{-1})^e$
.
.
.
$C(2^{-34})^e$

Και ένα άλλο λεξικό : 1^e
2^e

.
.
.
$(2^{34})^e$

Για να βρούμε το K_1 αρκεί να βρούμε ποιά τιμή του 2ου λεξικού ισούται με ποιά τιμή του 1ου.

Το RSA δεν χρησιμοποιείται με τον παραπάνω τρόπο, αλλά με padding τυχαίων bit στο μήνυμα.

Πρωτόκολλο Rabin

1. Η Α δημιουργεί το κειδί: Διαλέγει 2 μεγάλους πρώτους, p,q έτσι ώστε:
   $p \equiv 3 (mod\, 4)$
   $q \equiv 3 (mod\, 4)$
   και υπολογίζει n=pq, P_A={n}, S_A=(p,q}
2. Κρυπτογράφηση: $C=M^2 mod n$
3. Αποκρυπτογράφηση:
   Λύνουμε:
   1. $C=M^2 mod p$ -> 2 λύσεις (r, -r)
   2. $C=M^2 mod q$ -> 2 λύσεις (s, -s)
   3. Αφού οι p και q είναι πρώτοι μεταξύ τους, τότε gcd(p,q)=1 και υπάρχουν ακέραιοι α, β ώστε αp+βq=1
4. x=αps+βqr και y=αps-βqr

Λύση: x, -x, y, -y (modn)

Πώς θα ξέρουμε ποιά είναι η πραγματική λύση; Επιβάλλουμε συγκεκριμένη δομή στο μήνυμα.

Πώς υπολογίζουμε τα βήματα 1 και 2

$x^2 \equiv a (mod n)$ Όπου n είναι σύνθετος **ΔΥΣΚΟΛΟ ΠΡΟΒΛΗΜΑ**

Έστω p πρώτος ώστε $x^2 \equiv a (mod p)$

αν $\alpha^{\frac{1}{2}(p-1)} \equiv 1 (mod p)$ τότε υπάρχουν Q_p=(p-1)/2 α που έχουν λύση και $\overline{Q}_{\bar{p}}$=(p-1)/2 που δεν έχουν λύση.

Η λύση θα είναι: $x \equiv a^{\frac{1}{4}(p+1)} (mod p)$ όπου $p \equiv 3 mod\, 4$

Παράδειγμα:
p=7, q=11, n=77

Έστων M=10, άρα $C=M^2 \bmod n=100 \bmod 77=23$

Αποκρυπτογράφηση:

1. $M^2 \equiv 23 \bmod 7 \Rightarrow M^2 \equiv 1 \bmod 77 \quad r=2^{\frac{1}{4}8} \bmod 7=2^2 \bmod 7=4$ και
2. $M^2 \equiv 23 \bmod 11 \Rightarrow M^2 \equiv 1 \bmod 11 \quad s=1^{\frac{1}{4}12} \bmod 11=1$
3. gcd(7, 11)=1 άρα υπάρχουν α,β ώστε 7α+11β=1 ... α=-3, β=2
4. $x=-3 \cdot 7 \cdot 1+2 \cdot 11 \cdot 4=-21+88=67 \,(mod\, 77)$ άρα x=67, y=45
   $y=-21-88=-109 \,(mod\, 77)=45$

   Οι λύσεις είναι: {67, 10, 45, 32}

Ισχυρισμός
Το πρόβλημα παραγοντοποίησης είναι ισοδύναμη με το πρόβλημα εύρεσης τετραγωνικών ριζών.

Έστω ότι έχουμε έναν αλγόριθμο A (a,n) που λύνει το πρόβλημα εύρεσης τετραγωνικής ρίζας. Για να αποδείξουμε τον ισχυρισμό, θα πρέπει να δείξουμε ότι μέσω αυτού του αλγορίθμου μπορούμε να λύσουμε και το πρόβλημα της παραγοντοποίησης.

1. Διαλέγω αυθαίρετα ένα x και υπολογίζω το $x^2 \bmod n$.
2. Θέτω $\alpha=x^2 \bmod n$ και εκτελώ τον A(α, n).
3. Παίρνω πιθανές λύσεις x, -x, y, -y
4. Αν A(α, n) =±x, ξαναδοκιμάζω.
5. Αν A(α, n) =±y τότε είτε ο gcd(x+y,n) είτε ο gcd(x-y,n) είναι παράγοντας του n. Για να είναι ένας αριθμός παράγοντας του n, θα πρέπει να είναι διαφορατικός από το 1 και από το n.
   1. Αν gcd(x+y,n)=n ⇒ x+y=kn ⇒ x+y=0(modn) ⇒ x≡y(modn) ΑΤΟΠΟ γιατί αν ίσχυε θα ήμασταν στο βήμα 4.
   2. Αν gcd(x-y,n)=n ⇒ x-y=kn ⇒ x-y=0(modn) ⇒ x≡y(modn) ΑΤΟΠΟ γιατί αν ίσχυε θα ήμασταν στο βήμα 4.
   3. Αν gcd(x+y)=1 τότε υπάρχουν α,β ώστε α(x+y)+βn=1 (1)
   4. Αν gcd(x-y)=1 τότε υπάρχουν α',β' ώστε α'(x-y)+β'n=1 (2)
   5. Πολλαπλασιάζουμε κατά μέλη τις (1) και (2) και έχουμε:

      $\alpha\alpha'(x^2-y^2)+\beta\beta'n^2+\alpha\beta'(x+y)n+\alpha'\beta(x-y)n=1$

      παίρνουμε το υπόλοιπο των δύο μελών με το n και έχουμε:

αα’$(x^2-y^2)\equiv 1 (mod n)$ ΑΤΟΠΟ επειδή έχουμε θεωρήσει ότι τα x και y είναι λύσεις, δηλαδή ότι είναι ρίζες του n, άρα αα’$0\equiv 1$ που είναι άτοπο