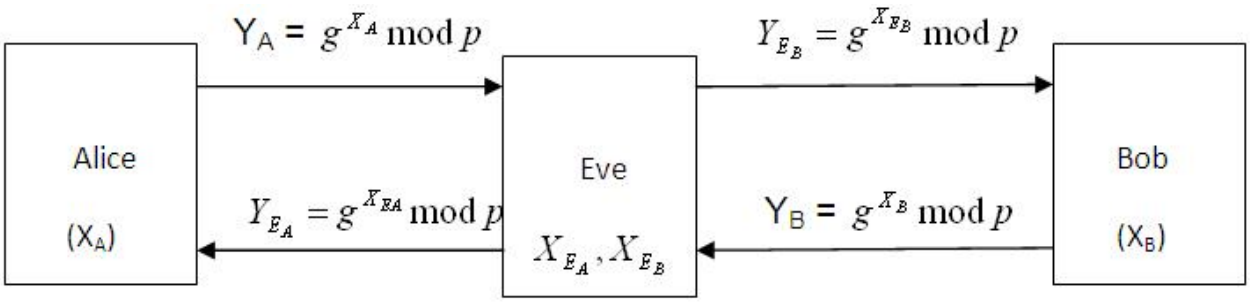
23/3/2017

Μειονέκτημα του πρωτοκόλλου Diffie-Hellman-man in the middle



Η Εύα παρακολουθεί το κανάλι. Παίρνει το g^amodp από την Αλίκη, υποδυόμενη τον Μπόμπο, και της δίνει το g^emodp. Ομοίως παίρνει το g^bmodp από το Μπόμπο. Με αυτό τον τρόπο μπορεί να αποκρυπτογραφήσει και να αλλάξει τα μηνύματά τους.

Η επίθεση αυτή αντιμετωπίζεται με την ταυτοποίηση του αποστολέα. Για να το επιτύχουμε αυτό εισάγουμε οντότητες στο σύστημα οι οποίες κάνουν την ταυτοποίηση και τις εμπιστευόμαστε ανεπιφύλακτα.

Trapdoor function
Πρόκειται για μια one way function με κλειδί.

Δηλαδή: έχουμε μια συνάρτηση f: X→Y

- ξέρω K,x: είναι εύκολο να βρω το $f_K(x)$
- ξέρω $f_K(x)$: δεν μπορώ να βρω εύκολα τα x και K
- ξέρω K,$f_K(x)$: μπορώ εύκολα να βρω ποιο x δίνει $f_K(x)$

Πρωτόκολλα Δημόσιου Κλειδιού
Κάθε χρήστης έχει ένα δημόσιο κλειδί K_e και ένα ιδιωτικό K_d.

1. Βρίσκω το δημόσιο κλειδί του B, έστω K_e
2. C=e_{Ke}(M), όπου C το κρυπτογραφημένο μήνυμα, M το αποκρυπτογραφημένο μήνυμα, e_{Ke} η συνάρτηση κρυπτογράφησης.
3. M=d_{Kd}(C), όπου d_{Kd} η συνάρτηση αποκρυπτογράφησης.

Για να γίνει σωστά η διαδικασία θα πρέπει: M=d_{Kd}(e_{Ke}(M))

γνωστά δημόσια ιδιωτικά

Πρωτόκολλο RSA
Οι Rivest, Shamir, Adleman πρότειναν συγκεκριμένες συναρτήσεις d και e για το πρωτόκολλα δημόσιου κλειδιού, γι' αυτό τα βήματα είναι ίδια:

1. - Επιλέγω δύο μεγάλους πρώτους p και g.

- $n = p \cdot g$
- Επιλέγω e : gcd(e,Φ(n))=1 ή gcd(e,(p-1)(q-1))=1
- Υπολογίζω d : $e \cdot d \equiv 1 (mod \Phi(n))$
- δημόσιο κλειδί: K_e={n, e}
- Ιδιωτικό κλειδί: K_d={p, q, d}

2. $e_{Ke}(M)=M^e mod n$
3. $d_{Kd}(C)=C^d mod n$

Προσοχή: Το μήνυμα θα πρέπει να είναι μικρότερο από το n σε μήκος. Αν δεν είναι, θα πρέπει να το τεμαχίσουμε με μικρότερα τμήματα.

Ορθότητα RSA

Σημαίνει ότι η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης μας δίνουν σωστά το αρχικό μήνυμα, δηλαδή ότι $M=d_{Kd}(e_{Ke}(M))$.

$e_{Ke}(M)=M^e mod n=C$ και $d_{Kd}(C)=C^d mod n=M$

$\Rightarrow M= C^d mod n= (M^e mod n)^d mod n= M^{ed} mod n$

Αρκεί δηλαδή να δείξουμε ότι : 1. $M^{ed}=M mod p$

2. $M^{ed}=M mod q$

Από το κινέζικο θεώρημα των υπολοίπων προκύπτει ότι $M_{ed} \equiv M mod(p \cdot q)$

Απόδειξη:

1. $M^{ed}(mod p)=M^{1+K\Phi(n)}=MM^{K\Phi(n)}=M(M^{\Phi(n)})^K=M(M^{(p-1)(q-1)})^K=M(M^{(p-1)})^{(q-1)K}$

Όμως από το θεώρημα του Euler ισχύει ότι $M^{(p-1)} \equiv 1 (mod p)$ άρα έχουμε:

$M^{ed}(mod p)=M(M^{(p-1)})^{(q-1)K}=M(mod p)$

2. Ομοίως και για το q

Άρα ισχύει ότι $M_{ed} \equiv M mod(p \cdot q)$ δηλαδή απόδείχθηκε η ορθότητα.

Ασφάλεια RSA-Μειονεκτήματα

Στηρίζεται στο ότι το πρόβλημα της παραγοντοποίησης λύνεται δύσκολα.

Η αδυναμία του RSA είναι ότι υπάρχει περίπτωση το μήνυμα να μην κρυπτογραφηθεί καθόλου. Υπάρχουν p, q, e για τα οποία το κρυπτογραφημένο μήνυμα είναι το ίδιο με το αρχικό. Μπορούμε όμως να βρούμε για ποιες τιμές γίνεται αυτό. Ξεκινάμε από το p:

$$M^e \equiv 1 (mod p)$$
$$M^{e-1} \equiv 1 (mod p)$$

Το σύστημα αυτό επιλύεται με τη βοήθεια των ομάδων: $g^{x(e-1)} \equiv g^0 (mod p)$, $x(e-1) \equiv 0 (mod(p-1))$

Θα έχει gcd(p-1,e-1) σε πλήθος λύσεις.

Ακολουθούμε την ίδια διαδικασία για το q και βρίσκουμε ότι το δεύτερο σύστημα θα έχει gcd(q-1,e-1) σε πλήθος λύσεις. Άρα:

[1+gcd(p-1,e-1)][1+gcd(q-1,e-1)]=pq

Ένα άλλο πρόβλημα που παρουσιάζεται είναι όταν έχουμε κοινό e για κάποιους χρήστες, δηλαδή:

$(n_1,3)\ c_1 \equiv m^3 (mod n_1)$
$(n_2,3)\ c_2 \equiv m^3 (mod n_2)$
$(n_3,3)\ c_3 \equiv m^3 (mod n_3)$

Από το κινέζικο θεώρημα των υπολοίπων έχουμε ότι:

$x^3 \equiv c_1 (mod n_1)$
$x^3 \equiv c_2 (mod n_2) \quad \Rightarrow x^3 \equiv A mod(n_1 \cdot n_2 \cdot n_3)$ και γνωρίζουμε ότι $x^3<n_1n_2n_3$ αφού $x<n_1$ και
$x^3 \equiv c_3 (mod n_3)$

$x<n_2$ και $x<n_3$ άρα αρκεί να βρούμε την κυβική ρίζα του Α.

Το 3ο πρόβλημα του RSA είναι ότι μπορεί το μήνυμα να ανακατασκευασθεί από τις συνιστώσες του, ή μπορούν να χρησιμοποιηθούν οι συνιστώσες για να πάρει κάποιος πληροφορία για ένα άλλο μήνυμα.

$M_1 \rightarrow C_1=M_1^e$ modn και $M_2 \rightarrow C_2=M_2^e$ modn Τότε:

$M_1M_2 \rightarrow C_{12}$ modn$=(M_1M_2)^e$modn$=M_1^e\ M_2^e$ modn$=C_1C_2$

Αυτό αντιμετωπίζεται ως εξής:

(πχ) Επιτρέπεται να κρυπτογραφήσουμε μόνο μηνύματα που στο τέλος τους έχουν 64 μηδενικά. Οπότε στο τέλος των M_1 και M_2 θα υπάρχουν 64 μηδενικά, όπως και στο τέλος του M_1M_2. Άρα το C_1C_2 θα είναι διαφορετικό από το C_{12}.