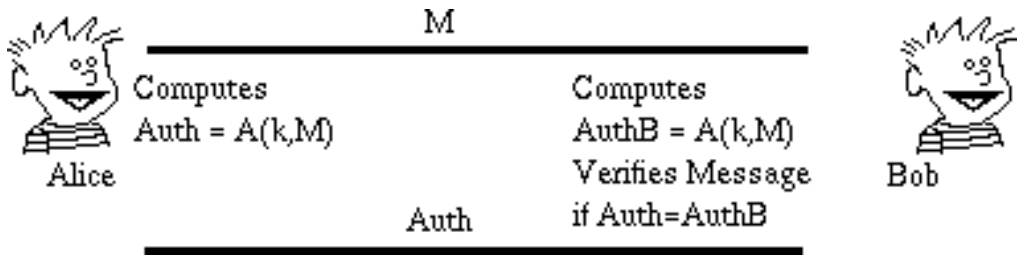
ΕΡΓΑΣΙΑ

στο μάθημα : "ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ"



Μπαλάφας Βασίλειος

Καθηγητής : Μελετίου Γεράσιμος

Μάιος 2000

Περιεχόμενα :

Εισαγωγή - Ιστορική αναδρομή

Οι άνθρωποι χρησιμοποιούν μυστικούς κώδικες στην επικοινωνία τους με κάθε μέσο εδώ και χιλιάδες χρόνια.Σήμερα η επικοινωνία των ανθρώπων τείνει να γίνει πλήρως "ηλεκτρονική" αφού η εξάπλωση των ηλεκτρονικών υπολογιστών και η ανάπτυξη του internet έδωσαν νέα διάσταση στο θέμα επικοινωνία και χρησιμοποιούνται ευρέως σε όλο τον κόσμο.

Φυσικό επακόλουθο ήταν να αναζητηθούν τρόποι για να γίνεται και αυτού του είδους η επικοινωνία με τον πλέον ασφαλή τρόπο έτσι ώστε να προστατεύονται οι πληροφορίες που κυκλοφορούν με ηλεκτρονικό τρόπο.

Είναι γνωστό ότι οι ηλεκτρονικοί υπολογιστές μπήκαν ουσιαστικά στη ζωή μας πριν από λίγες δεκαετίες και η εξέλιξή τους ήταν αλματώδης σε τέτοιο βαθμό που δύσκολα πλέον μπορεί να την παρακολουθήσει ένας μέσος χρήστης.

Έτσι είναι εκπληκτικό ότι το 1976 ο Whitfield Diffie και ο Martin Hellman στο Πανεπιστήμιο του Stanford ανακάλυψαν μια τεράστια νέα εννοιολογική προσέγγιση στην κρυπτογράφηση και αποκρυπτογράφηση : το κοινό κλειδί της κρυπτογραφίας.

Τα κρυπτογραφικά συστήματα βασίζονται τυπικά σε κρυπτογραφημένα κείμενα (κωδικούς),που χρησιμοποιούν κλειδιά για κρυπτογράφηση και αποκρυπτογράφηση. Στα παραδοσιακά κρυπτογραφημένα κείμενα,τα λεγόμενα συμμετρικά κρυπτογραφημένα κείμενα,το κλειδί που χρησιμοποιείται για να κρυπτογραφήσει ένα μήνυμα είναι επίσης το κλειδί που αποκρυπτογραφεί το μήνυμα.

Ως συνέπεια,αν γνωρίζεις πως να κρυπτογραφείς μηνύματα μ'ένα συγκεκριμένο κλειδί,τότε μπορείς εύκολα να αποκρυπτογραφήσεις μηνύματα ,που έχουν κρυπτογραφηθεί με αυτό το κλειδί.

Η ενόραση των Diffie και Hellman ήταν να κατανοήσουν ότι υπάρχουν κρυπτογραφικά συστήματα για τα οποία γνωρίζοντας την κρυπτογράφηση, το κλειδί δεν παρέχει βοήθεια στην αποκρυπτογράφηση μηνυμάτων.

Το γεγονός αυτό έχει τεράστια σημασία.Στα παραδοσιακά κρυπτογραφικά συστήματα,κάποιος μπορεί να σου στείλει κωδικοποιημένα μηνύματα μόνο αν οι δυό σας μοιράζεστε ένα μυστικό κλειδί.Επειδή ο καθένας, ο οποίος μαθαίνει οτι ένα κλειδί μπορεί να είναι ικανό να αποκρυπτογραφήσει τα μηνύματα,τα κλειδιά πρέπει να φυλάσσονται προσεκτικά και να μεταφέρονται μόνο με υψηλή ασφάλεια.

Στο σύστημα των Diffie και Hellman μπορείς να λές το κρυπτογραφικό σου κλειδί ή κοινό κλειδί στον καθένα που επιθυμεί να σου στείλει μηνύματα και να μην ανησυχείς για την ασφάλεια του κλειδιού καθόλου.

Για παράδειγμα αν όλοι στον κόσμο ήξεραν το κοινό σου κλειδί,κανένας δε θα μπορούσε να αποκρυπτογραφήσει μηνύματα σταλμένα σε σένα χωρίς να γνωρίζει κάποια επιπρόσθετη μυστική πληροφορία,την οποία κρατάς ιδιωτική για τον εαυτό σου.

Οι Diffie και Hellman ονόμασαν τέτοιου είδους συστήματα ως κοινού κλειδιού κρυπτογραφικά συστήματα.

Η συνθήκη του συστήματος των Diffie και Hellman

Το κοινού - κλειδιού σύστημα που παρατίθεται παρακάτω είναι βασισμένο στη μέθοδο των Diffie και Hellman για τη συμφωνία του κλειδιού. Αυτή είναι μια μέθοδος για την οποία δύο άνθρωποι μπορούν να σχεδιάσουν ένα από κοινού μυστικό που θα είναι γνωστό μόνο στους δύο τους,παρ'ότι ολόκληρη η επικοινωνία μεταξύ τους θα γίνεται δημοσίως.

Αν λοιπόν η Alyssa και ο Ben επιθυμούν να επικοινωνήσουν συμφωνούν δημόσια σ'έναν μεγάλο αρχικό αριθμό p και σε έναν αριθμό g, ο οποίος είναι παράγωγος του p.Για να είναι το g παράγωγος σημαίνει οτι οι δυνάμεις $g,g^2,g^3,....,g^{p-1}$,παίρνοντας modulo p , παράγει όλους τους ακέραιους 1,2,3,...,p-1 σε τέτοια σειρά.

Η Alyssa διαλέγει ένα μυστικό αριθμό x και υπολογίζει $y \equiv g^x \bmod p$. Ο Ben διαλέγει ένα μυστικό αριθμό x και υπολογίζει $y \equiv g^x \bmod p$. Η Alyssa στέλνει στον Ben το y , και ο Ben στέλνει στην Alyssa το y . Η Alyssa υπολογίζει τώρα $y^x \bmod p$ και ο Ben υπολογίζει $y^x \bmod p$. Αλλά αυτοί είναι οι ίδιοι αριθμοί γιατί :

$$y^x \equiv (g^x)^x \equiv g^{xx} \equiv g^{xx} \equiv (g^x)^x \equiv y^x \bmod p$$

Τώρα που η Alyssa και ο Ben έχουν από κοινού αυτό τον αριθμό, ονομάστε τον κ , μπορούν να χρησιμοποιούν το κ ως ένα κλειδί για να στέλνουν και να λαμβάνουν μηνύματα χρησιμοποιώντας κάποια συνηθισμένα συμμετρικά κρυπτογραφικά συστήματα.

Το σημαντικό σημείο είναι ότι όλες οι επικοινωνίες της Alyssa και του Ben μπορούν να είναι δημόσιες και κάποιος που θέλει να τα υποκλέψει δεν γνωρίζει το κ και έτσι δεν μπορεί να αποκρυπτογραφήσει τα μηνύματα.

Τα μόνα που μπορεί να γνωρίζει κάποιος τρίτος είναι τα p,g,y και y. Αν ο p είναι ένας μεγάλος πρώτος δεν υπάρχει αποτελεσματικός τρόπος να χρησιμοποιήσει τα στοιχεία που γνωρίζει για να υπολογίσει το κ.

Η κρυπτογράφηση και αποκρυπτογράφηση του El Gamal

Τα παραπάνω αναφέρθηκαν ως εισαγωγικές έννοιες για να μπορέσουμε να κατανοήσουμε και τη μέθοδο του El Gamal αλλά και για να δούμε πως εξελίχθηκαν τα συστήματα ασφαλείας κοινού κλειδιού.

Πρίν ξεκινήσουμε την περιγραφή μας ας δούμε τι γράφεται στο διαδίκτυο χαρακτηριστικά για τη μέθοδο του El Gamal και γιατί ήταν απαραίτητο να αναφερθούμε στους Diffie και Hellman :

ElGamal public keys are essentially the same as Diffie-Hellman public keys. Thus the security requirements for, e.g., DH moduli apply also to ElGamal moduli. The strength of the ElGamal schemes versus a direct key recovery attack depends (at a minimum) upon the difficulty of computing discrete logarithms in the group used.

Ας υποθέσουμε λοιπόν ότι η Alyssa θέλει να αρχίσει ένα σύστημα που επιτρέπει στον καθένα σ'όλο τον κόσμο να της στείλει ένα κρυπτογραφημένο μήνυμα το οποίο μόνο αυτή μπορεί να αποκρυπτο - γραφήσει.Μπορεί να το κάνει αυτό με μια μικρή διαφοροποίηση στις παραπάνω συνθήκες.

Όπως και παραπάνω η Alyssa παίρνει έναν πρώτο p,έναν παράγωγο g και έναν μυστικό αριθμό x και υπολογίζει $y \equiv g^x \bmod p$. Κρατάει το x μυστικό για τον εαυτό της και δημοσιοποιεί τις τιμές p,g,y. Αυτές οι δημοσιοποιημένες τιμές σχηματίζουν το κοινό κλειδί της Alyssa.

Υποθέτουμε τώρα ότι ο Ben (η οποιοσδήποτε άλλος) θέλει να στείλει στην Alyssa ένα κρυπτογραφημένο μήνυμα.Παίρνει το κοινό κλειδί της Alyssa το οποίο έχει τις τιμές p,g,y .Μετά παίρνει το δικό του αριθμό x. Από αυτό υπολογίζει $y \equiv y^x \bmod p$ και υπολογίζει επίσης $K \equiv y^x \bmod p$. Ο Ben χρησιμοποιεί το K σαν το κλειδί για να κρυπτογραφήσει το μήνυμα στην Alyssa,χρησιμοποιώντας κάποιους συμμετρικούς αλγορίθμους.

Στέλνει το κρυπτογραφημένο μήνυμα στην Alyssa,καθώς και το y. Όταν η Alyssa λάβει το κρυπτογραφημένο μήνυμα παίρνει το y μέρος που

ήρθε μ'αυτό και υπολογίζει το $K \equiv y^{x} \bmod p$. Σ'αυτό το σημείο πρέπει να τονίσουμε οτι η Alyssa και μόνο η Alyssa γνωρίζει το x.

Τώρα χρησιμοποιεί το K ως το κλειδί για να αποκρυπτογραφήσει το μήνυμα.Άλλοι άνθρωποι που βλέπουν το μήνυμα δεν μπορούν να το αποκρυπτογραφήσουν.Γνωρίζουν τα p,g,y και y , αλλά δε μπορούν να υπολογίσουν το K από αυτά , χωρίς να γνωρίζουν το x ή το x.

Αυτή η μέθοδος που περιγράψαμε αναλυτικά παραπάνω είναι γνωστή ως το σύστημα κοινού κλειδιού του El Gamal.

Τελική υλοποίηση του κρυπτογραφικού συστήματος El Gamal

Το τελικό στοιχείο που χρειαζόμαστε για να εκπληρώσουμε τους όρους του κοινού κλειδιού της κρυπτογραφικής μεθόδου του El Gamal είναι ένα κρυπτογραφικό σύστημα,το οποίο θα χρησιμοποιήσει το μοιρασμένο κλειδί για να κρυπτογραφήσει και να αποκρυπτογραφήσει.

Οι διαδικασίες που πρέπει να ακολουθηθούν είναι οι εξής : συμμετρική κρυπτογράφηση και συμμετρική αποκρυπτογράφηση

Η συμμετρική κρυπτογράφηση παίρνει ένα μήνυμα με κείμενο στοιχειοσειράς και ένα αριθμητικό κλειδί και κρυπτογραφεί το μήνυμα χρησιμοποιώντας το κλειδί για να παράγει ένα κείμενο κρυπτογραφικού συστήματος.Δίνοντας το κείμενο κρυπτογραφικού συστήματος και το ίδιο κλειδί,η συμμετρική αποκρυπτογράφηση θα επανακτήσει το κείμενο μηνύματος.

Η παράξενη ανάστροφη διαγώνιος των αριθμών στο κείμενο κρυπτογραφικού συστήματος είναι ο τρόπος του Scheme για να τυπώσει κωδικούς χαρακτήρων που δεν ανταποκρίνονται απευθείας σε τυπωμένους χαρακτήρες.

Ανακεφαλαιώνοντας,δίνοντας μαζί και της Alyssa το κοινό κλειδί,κρυπτογραφούμε το μήνυμα όπως περιγράψαμε παραπάνω. Διαλέγουμε μια τυχαία αξία για το x (μην το μπερδέψετε με το x από της Alyssa κλειδί συστήματος,το οποίο μόνο η Alyssa γνωρίζει) , χρησιμοποιούμε το y της Alyssa υψωμένο στη δύναμη x mod p όπως το κοινό κλειδί για τα συμμετρικά κρυπτογραφικά συστήματα και στέλνουμε το αποτέλεσμα μαζί με $y \equiv g^{x} \bmod p$.

Σπάζοντας το σύστημα - Το πρόβλημα των διακριτών λογαρίθμων

Υποθέστε πως κάποιος θέλει να αποκρυπτογραφήσει ένα μήνυμα που δεν προοριζόταν για αυτόν.Υποθέστε πως αυτός ο κάποιος είναι το είδος του κάποιου,ο οποίος τυχαίνει να έχει μεγάλη υπολογιστική δύναμη για να αφιερώσει στο πρόβλημα.Πρέπει να ξεκινήσει με το κοινό κλειδί του δέκτη και να ανακαλύψει το μυστικό αριθμό x . Αυτό σημαίνει , παρέχοντας το p,g και y ,οτι πρέπει να βρεί τον αριθμό x , τέτοιον ώστε $y \equiv g^x \bmod p$. Αυτό ονομάζεται πρόβλημα του διακριτού λογαρίθμου.

Πως μπορούμε να υπολογίσουμε διακριτούς λογαρίθμους;

Ένας τρόπος ειναι η λεγόμενη brute - force έρευνα.Δοκιμάζουμε όλες τις τιμές για το x μεταξύ μεταξύ του 2 και του p - 2,μέχρι να βρούμε έναν που να δουλεύει.Δυστυχώς για τον κάποιο που προσπαθεί να σπάσει το σύστημα η υπολογιστική χωριτικότητα είναι απέραστη.

Πρέπει να θυμηθούμε πως αν χρησιμοποιηθούν επιτυχημένα τετράγωνα,ο χρόνος που χρειάζεται για να υψώσουμε έναν αριθμό σε μια δύναμη μέχρι το p έχει ανάπτυξη Θ (log p). Αλλά για να περάσουμε όλους τους αριθμούς μικρότερους από p έχουμε ανάπτυγμα Θ (p). Κάθε φορά που προσθέτουμε ένα ακόμα ψηφίο στον πρώτο αριθμό,αυξάνουμε τους υπολογισμούς για το σπάσιμο διακριτών λογαρίθμων από έναν παράγοντα του 10.

Η ουσία είναι ότι δεν υπάρχει γρήγορη και βέβαιη μέθοδος για τον υπολογισμό αυτών των λογαρίθμων οπότε αυτό το σύστημα του El Gamal θεωρείται εξαιρετικά ασφαλές και επιτυχημένο.

Το scheme του El Gamal

- whilst the ElGamal encryption algorithm is not commutative, a closely related signature scheme exists
- El Gamal Signature scheme
- given prime p, public random number g, private (key) random number x, compute
  - $y = g^x \pmod p$
- public key is (y,g,p)
  - nb (g,p) may be shared by many users

- p must be large enough so discrete log is hard
- private key is (x)
- to **sign** a message M
  - choose a random number k, GCD(k,p-1)=1
  - compute
  - $a = g^k \pmod p$
  - use extended Euclidean (inverse) algorithm to solve
  - $M = x.a + k.b \pmod{p-1}$
  - the signature is (a,b), k must be kept secret
  - (like ElGamal encryption is double the message size)
- to **verify** a signature `(a,b)` confirm:
  - $y^a.a^b \pmod p = g^M \pmod p$

Παράδειγμα εφαρμογής του συστήματος El Gamal

- given p=11, g=2
- choose private key x=8
- compute
  - $y = g^x \pmod p = 2^8 \pmod{11} = 3$
- public key is y=3,g=2,p=11)
- to sign a message M=5
  - choose random k=9
  - confirm gcd(10,9)=1
  - compute
    - $a = g^k \pmod p = 2^9 \pmod{11} = 6$
  - solve
    - $M = x.a+k.b \pmod{p-1}$
    - $5 = 8.6+9.b \pmod{10}$
    - giving b = 3
  - signature is (a=6,b=3)
- to verify the signature, confirm the following are correct:
  - $y^{a.}a^b \pmod p = g^M \pmod p$
  - $3^{6.}6^3 \pmod{11} = 2^5 \pmod{11}$