ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Η κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography) επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρέχει ένα εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται ιδιωτικό κλειδί (private key) και το άλλο δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το ανακοινώνει σε όλη την διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP Key Server 0.9.6

mQGiBDmXx8cRBADd0Dko7J7Gb5G/FINwO48AgrlYE87wCT5dlqSXl2uoDmR0/dKp
pJmvDeLQw+Z02yGx7TKf7PC5dfh61tIHyeI0SfCZVA5DtRDk3keNXy2WLnLMg2yS
J44JG3I/o1QKXL8PKD2bkv/vUl7gtXe3qa57oC+2ZmxzptnLeBh08QrWXwCg/8A2
L7WHGKbhYKCApM+0FJStYrcD/1iTYhNsiZnW2tc86e/uHiX8rg7tD7VGm/Wg2E4V
Hadsb4wMLhlfi/vC5EZmlH3hFxvGk6YCWXkdFxzqhq2ZJRWQStqZqjSPWTI3Hv0K
Nzjq5DbRMQY2O025g1FyWB62ZDrUWXqzybi4okoEdXT/lQA7Xe95T8uy1zfTUmBg
ieTtA/0RU3MYboVOyDgGvJ7fVyFNdk8+v6Hzcn6EZMWYJifE5hw/tSLnRAXb7ejh
wsLDDCGsjloUj4TnMHH0LUTZSWbgDZwCF6tig3mbhk7YH21zWrVQwPidSpS5O3Oh
85V3nJx5r0406nM4N1cp46yKUMekE6nhubCpVme6o+f9sUMXkLQhR2VydCBLYXNw
ZXJzZW4gPGdla2FzQHdtkGF0YS5jb20+iQBLBBARAgALBQI5l8fHBAsDAgEACgkQ
Ls3rBj/p+6oQGwCgv5ML3xAatvJtY1mKnwz1SH2YbJ8AoPeBkUY73P+QDc5aFdHC
rCkobzlYuQQNBDmXx8cQEAD5GKB+WgZhekOQldwFbIeG7GHszUUfDtjgo3nGydx6
C6zkP+NGllYwSlPXfAIWSIC1FeUpmamfB3TT/+0hxZYgTphluNgN7hBdq7YXHFHY
UMoiV0MpvpXoVis4eFwL2/hMTdXjqkbM+84X6CqlFGHjhKlP0YOEqHm274+nQ0YI
xswdd1ck0ErixPDojhNnl06SE2H22+slDhf99pj3yHx5sHId0HX79sFzxIMRJitD
YMPj6NYK/aEoJguuqa6zZQ+iAFMBoHzWq6MSHvoPKs4fdIRPyvMX86RA6dfSd7ZC
LQI2wSbLaF6dfJgkCo1+Le3kXXn11JJPmxiO/CqnS3wy9kJXtwh/CBdyorrWqULz
Bej5UxE5T7bxbrlLOCDaAadWoxTpj0BV89AHxstDqZSt90xkhkn4DIO9ZekX1KHT
UPj1WV/cdlJPPT2N286Z4VeSWc39uK50T8X8dryDxUcwYc58yWb/Ffm7/ZFexwGq
01uejaClcjrUGvC/RgBYK+X0iP1YTknbzSC0neSRBzZrM2w4DUUdD3yIsxx8Wy2O
9vPJI8BD8KVbGI2Ou1WMuF040zT9f8dXQ6MdGGzeMyEstSr/POGxKUAYEY18hKcK
ctaGxAMZyAcpesqVDNmWn6vQClCbAkbTCD1mpF1Bn5x8vYlLIhkmuquiXsNV6z3W
FwACAhAAumPF6HT301BhkfuMTVI2jFXUJ7prdWy4pwZArvdDVYQ35M8sG/ISJjwg
B2GdpK9i02B25Cen309snDSj/aJkz7PQgD8CyB1V0KiDFX+KxR8S0le2k1tdbiP3
wNYxw7MDiz757IY9/hmv6YDwSeS2sWnyjgfQXR5z2RBs4r+UZ8YWk8h4YQsLSL2B
Z/PImaiopMScDJy1m4AzasXNdyr1SywU4tlwOXZhZh6ccZB/z6nlZJgMnwfVw1fZ
8wyiTKGoyOp5eh9edDFwtcAVNHVoI0hj9kDfa5sfA9zcKfeLH7TouYLuMcdws9Uc
fNeJI6AgzUvGwzvG9HVuVGf7n5b1j9Kp+jcSjvWqpQX1/iDEN8KG6/yk5mtok4lv
JBieGM2SahP1cTk1P4kcrlwJ419EhKtC6xZS96J0+TmyLBTSrJHazWR+n/lQsXvz
g7wNUycZx+/v1QDGO3HyekqZR76BSMVrpNEYEWcBclTeJ6nBJCPTGxqvP4IQhzhJ
3znANVOsViJZ7rG3DrygE+8vQ32GjbBZzouN/gHxmSKOuvw6yjFdk1SMNNdlIeKm
05Z5aVSXPuE7+TfkbFGHy+GCxjsH6FNhU/8QKtr712NO9laDARGCVaOiVvBVevVO
PXajFSW19F7Rswmh7kD5jUEy9E7ANAa0YD5i07ee0wvmaGSwfKKIRgQYEQIABgUC
OZfHxwAKCRAuzesGP+n7qj2kAJ48xQqu8b8kzQHmmUvMFr8z+bfivQCgxXhBHUT1
Lsvbbxb TJ/Da6n5YSYE=
=9v+B
-----END PGP PUBLIC KEY BLOCK-----
```

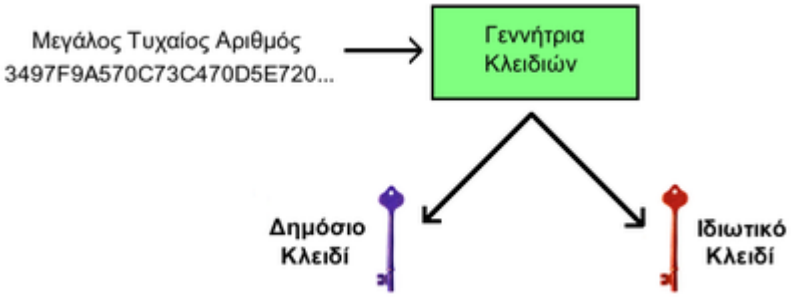
Ένα δημόσιο κλειδί 1024 bits το οποίο αναπαρίσταται ως μία ακολουθία αλφαριθμητικών χαρακτήρων.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

Η κρυπτογράφηση δημοσίου κλειδιού λύνει ένα σημαντικότατο πρόβλημα που υπήρχε στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού. Συγκεκριμένα, οι κρυπτογραφικοί αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούν ένα κοινό μυστικό κλειδί, το οποίο το γνωρίζουν τόσο ο αποστολέας του κρυπτογραφημένου μηνύματος όσο και ο παραλήπτης. Αυτό το κοινό μυστικό κλειδί χρησιμοποιείται κατά την διαδικασία κρυπτογράφησης και αποκρυπτογράφησης του μηνύματος. Προκύπτει όμως το εξής πρόβλημα: Εάν υποθέσουμε ότι το κανάλι επικοινωνίας δεν είναι ασφαλές, τότε πως γίνεται ο αποστολέας να στείλει το κλειδί κρυπτογράφησης στον παραλήπτη για να μπορέσει αυτός με την σειρά του να αποκρυπτογραφήσει το μήνυμα; Αυτό το πρόβλημα είναι ιδιαίτερα έντονο στις σύγχρονες ψηφιακές επικοινωνίες όπου σε πολλές περιπτώσεις ο αποστολέας δεν γνωρίζει καν τον παραλήπτη και απέχει από αυτόν αρκετές χιλιάδες χιλιόμετρα. Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού λύνουν αυτό το πρόβλημα και ανοίγουν νέους δρόμους για εφαρμογές της κρυπτογράφησης.

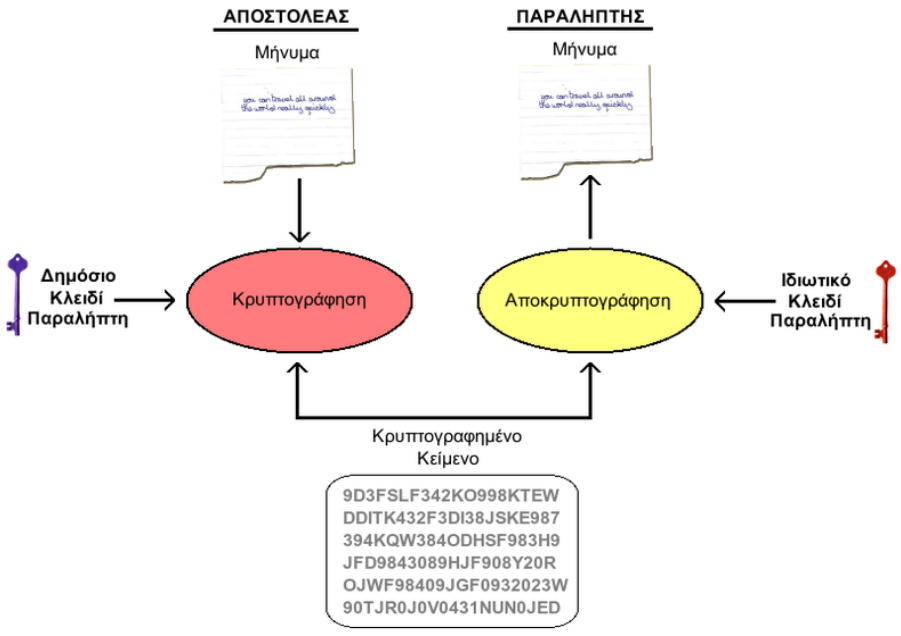
Δημιουργία κλειδιών

Η δημιουργία του δημόσιου και του ιδιωτικού κλειδιού γίνεται από ειδικές συναρτήσεις οι οποίες δέχονται ως είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών. Είναι προφανές ότι όσο πιο τυχαίος είναι ο αριθμός που παρέχεται ως είσοδος στην γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται. Σε σύγχρονα προγράμματα κρυπτογράφησης ο τυχαίος αριθμός παράγεται ως εξής: Κατά την διαδικασία κατασκευής των κλειδιών, το πρόγραμμα σταματάει για 5 λεπτά και καλεί τον χρήστη να συνεχίσει να εργάζεται με τον υπολογιστή. Στην συνέχεια για να δημιουργήσει τον τυχαίο αριθμό συλλέγει στα 5 αυτά λεπτά τυχαία δεδομένα που εξαρτώνται από την συμπεριφορά του χρήστη (κινήσεις ποντικιού, πλήκτρα του πληκτρολογίου που πατήθηκαν, κύκλοι μηχανής που καταναλώθηκαν κοκ). Με βάση αυτά τα πραγματικά τυχαία δεδομένα υπολογίζεται ο τυχαίος αριθμός και εισάγεται στην γεννήτρια κλειδιών για να κατασκευαστεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη.



Εμπιστευτικότητα - Κρυπτογράφηση

Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού μπορούν να εγγυηθούν εμπιστευτικότητα (confidentiality), δηλαδή ότι το κρυπτογραφημένο μήνυμα που θα στείλει ο αποστολέας μέσω του διαδικτύου στον παραλήπτη θα είναι αναγνώσιμο από αυτόν και μόνο. Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας θα πρέπει να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα. Στην συνέχεια στέλνει το κρυπτογραφημένο



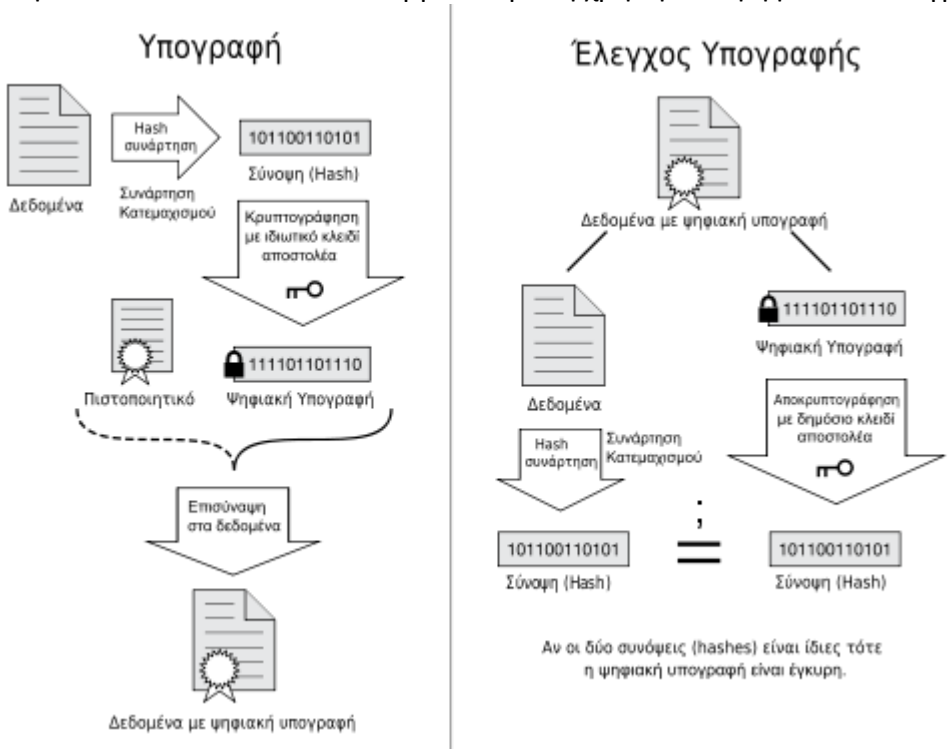
μήνυμα στον παραλήπτη και ο τελευταίος μπορεί να το αποκρυπτογραφήσει με το ιδιωτικό κλειδί του. Δεδομένου ότι το ιδιωτικό κλειδί του παραλήπτη είναι γνωστό μονάχα στον ίδιο και σε

κανέναν άλλον, μονάχα ο παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα και να το διαβάσει. Άρα λοιπόν με αυτόν τον τρόπο ο αποστολέας γνωρίζει ότι το κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη και έτσι διασφαλίζεται η εμπιστευτικότητα του μηνύματος.

Η παραπάνω μέθοδος μπορεί να εξασφαλίσει την εμπιστευτικότητα αλλά όχι την πιστοποίηση του αποστολέα. Αυτό με λίγα λόγια σημαίνει πως η παραπάνω μέθοδος δεν μπορεί να εγγυηθεί την ταυτότητα του αποστολέα. Πράγματι, ο αποστολέας μπορεί να δηλώσει ψευδή ταυτότητα και ο παραλήπτης να νομίσει ότι το συγκεκριμένο μήνυμα προήλθε από άλλο πρόσωπο.

Πιστοποίηση, Ακεραιότητα - Ψηφιακή Υπογραφή

Χρησιμοποιώντας κατάλληλα τους κρυπτογραφικούς αλγορίθμους δημοσίου κλειδιού μπορεί να επιτευχθεί πιστοποίηση (authentication), δηλαδή ο παραλήπτης να γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα. Αυτό συμβαίνει με τη χρήση των ψηφιακών υπογραφών.



Για να υπογραφεί ψηφιακά ένα αρχείο ή μήνυμα, χρησιμοποιείται αρχικά μία συνάρτηση κατατεμαχισμού (hash function) από την οποία προκύπτει η σύνοψη (digest) του μηνύματος. Η σύνοψη αυτή είναι στην ουσία ένας αριθμός, ο οποίος προκύπτει από την εφαρμογή της συνάρτησης στο αρχείο, και χαρακτηρίζει μοναδικά (σχεδόν) αυτό το αρχείο. Μπορούμε να το σκεφτούμε σαν το δακτυλικό αποτύπωμα ή το DNA του αρχείου. Αυτή η σύνοψη του μηνύματος κρυπτογραφείται στη συνέχεια με το ιδιωτικό κλειδί του αποστολέα (ο οποίος με αυτήν την ενέργεια υπογράφει ψηφιακά το μήνυμα έγγραφο). Η κρυπτογραφημένη σύνοψη είναι η ψηφιακή υπογραφή η οποία επισυνάπτεται στο μήνυμα-έγγραφο.

Όταν ληφθεί το μήνυμα, η ψηφιακή υπογραφή αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα και εξάγεται η σύνοψη. Το γεγονός ότι κατάφερε να αποκρυπτογραφηθεί η σύνοψη με το δημόσιο κλειδί του αποστολέα, αποδεικνύει ότι ο αποστολέας είναι αυτός που έβαλε την υπογραφή, αφού θα πρέπει να έχει κρυπτογραφηθεί με το αντίστοιχο ιδιωτικό. Παράλληλα υπολογίζεται η σύνοψη του ληφθέντος μηνύματος-εγγράφου. Αν οι δύο συνόψεις είναι ίδιες σημαίνει ότι το μήνυμα-έγγραφο έχει την υπογραφή του αποστολέα (που ανήκει το δημόσιο κλειδί) και ότι το μήνυμα-έγγραφο δεν έχει παραποιηθεί κατά την μεταφορά.

Μία ταχυδρομική αναλογία

Για να κατανοήσουμε καλύτερα τις διαφορές μεταξύ συμμετρικής και ασύμμετρης κρυπτογράφησης, μπορούμε να φανταστούμε δύο ανθρώπους, την Alice και τον Bob που θέλουν να ανταλλάξουνε κρυφά μηνύματα μέσω του ταχυδρομείου.

Με ένα σύστημα συμμετρικού κλειδιού, η Alice πρώτα βάζει το μυστικό μήνυμα που θέλει να στείλει σε ένα κουτί, το οποίο κλειδώνει με μία κλειδαριά για την οποία έχει το κλειδί. Στη συνέχεια το στέλνει στον Bob μέσω ταχυδρομείου. Όταν ο Bob λάβει το μήνυμα, χρησιμοποιεί ένα κλειδί πανομοιότυπο με αυτό της Alice (το οποίο έχει αποκτήσει προηγουμένως, ίσως σε πρόσωπο με πρόσωπο συνάντηση με την Alice) για να ξεκλειδώσει και να διαβάσει το μήνυμα. Στη συνέχεια ο Bob μπορεί να χρησιμοποιήσει το ίδιο λουκέτο για να στείλει την κρυφή του απάντηση στην Alice.

Σε ένα σύστημα ασυμμετρικού κλειδιού, η Alice και ο Bob έχουν ξεχωριστές κλειδαριές. Πρώτα, η Alice ζητάει από τον Bob να της στείλει το ξεκλείδωτο λουκέτο του μέσω απλού ταχυδρομείου, ενώ το κλειδί για το λουκέτο αυτό το κρατάει για τον εαυτό του. Όταν η Alice το λάβει, το χρησιμοποιεί για να κλειδώσει ένα κουτί το οποίο περιέχει το μήνυμά της και στέλνει το κλειδωμένο κουτί στον Bob. Όταν αυτός το λάβει, είναι ο μόνος που έχει το κλειδί για το λουκέτο, και άρα ο μόνος που μπορεί να το διαβάσει. Για να απαντήσει στην Alice, θα πρέπει αντίστοιχα και αυτός να πάρει ένα ανοιχτό λουκέτο από την Alice.

Το κρίσιμο πλεονέκτημα που μας προσφέρει η ασυμμετρική κρυπτογραφία είναι ότι η Alice και ο Bob δεν χρειάζεται να ανταλλάξουν κλειδιά. Αυτό αποτρέπει κάποιον τρίτο (ίσως, στο παράδειγμά μας, κάποιον διεφθαρμένο ταχυδρομικό υπάλληλο) από το να υποκλέψει το κλειδί καθώς αυτό μεταφέρεται, κάτι το οποίο θα επέτρεπε σε αυτόν τον τρίτο να κατασκοπεύει όλα τα μελλοντικά μηνύματα μεταξύ του Bob και της Alice. Οπότε, στο σύστημα δημοσίου κλειδιού, η Alice και ο Bob δε χρειάζεται να εμπιστεύονται ιδιαίτερα το ταχυδρομείο (και γενικά τον οποιο-δήποτε δίαυλο επικοινωνίας).

Αδυναμίες

Φυσικά, υπάρχει πάντα το ενδεχόμενο κάποιος να παραβιάσει την κλειδαριά της Alice ή του Bob. Μεταξύ των αλγορίθμων κρυπτογράφησης συμμετρικού κλειδιού, μόνο ο One-time pad είναι απόλυτα ασφαλής απέναντι σε οποιονδήποτε αντίπαλο, ανεξαρτήτως της υπολογιστικής ισχύος που αυτός μπορεί να διαθέτει. Δυστυχώς, δεν υπάρχει αλγόριθμος κρυπτογράφησης δημόσιου κλειδιού με αυτή την ιδιότητα, και έτσι όλοι αυτοί οι αλγόριθμοι είναι ευάλωτοι σε Brute-force attack (επίθεση ωμής βίας).

Η brute-force attack αναφέρεται στην εξαντλητική δοκιμή πιθανών κλειδιών που παράγουν ένα κρυπτογράφημα, ώστε να αποκαλυφθεί το αρχικό μήνυμα. Τέτοιου είδους επιθέσεις, οι οποίες χρησιμοποιούν όλα τα δυνατά κλειδιά, μπορούν πάντοτε να πραγματοποιηθούν. Τέτοιου είδους επιθέσεις, ωστόσο, δεν είναι πρακτικές αν ο όγκος των υπολογισμών (κόστος υπολο-γισμού) που απαιτείται για να επιτύχει η επίθεση, είναι πέραν των δυνατοτήτων των αντιπάλων. Σε πολλές περιπτώσεις, το κόστος υπολογισμού μπορεί να αυξηθεί απλά επιλέγοντας μεγαλύτερο κλειδί.

Στην πράξη, η παραπάνω ανασφάλεια αντιμετωπίζεται με την επιλογή κλειδιών αρκετά μεγάλων, ώστε η καλύτερη γνωστή επίθεση να έπαιρνε τόσο χρόνο που να μην άξιζε το χρόνο και τα χρήματα για τον αντίπαλο. Για παράδειγμα, κανένας δε θα έμπαινε στον κόπο να προσπαθήσει με brute force επίθεση να σπάσει την κρυπτογράφηση των μηνυμάτων σου, όσο σημαντικές πληροφορίες κι αν περιείχαν, αν η επίθεση θα έπαιρνε κατά μέσο όρο 1000 χρόνια.

Δημοσιοποίηση κλειδιών

Το δημόσιο κλειδί, όπως λέει και η λέξη, προορίζεται στο να είναι προσβάσιμο από τον καθένα ο οποίος θέλει να έρθει σε επαφή μαζί μας. Το δημόσιο κλειδί του ζεύγους χρησιμοποιείται είτε για την κρυπτογράφηση του μηνύματος από τον αποστολέα προς τον παραλήπτη χρησιμοποιώντας το δημόσιο κλειδί του τελευταίου, είτε για την επαλήθευση της ψηφιακής υπογραφής του αποστολέα χρησιμοποιώντας το δημόσιο κλειδί του πρώτου.

Ιδανικά η Alice μοιράζει εκ του φυσικού στις επαφές της το δημόσιο κλειδί της, χέρι με χέρι σε ένα USB stick ή ακόμα και σε χαρτί. Στην πράξη το δημόσιο κλειδί μοιράζεται κυρίως με ηλεκτρονικά μέσα. Η Alice μπορεί να στείλει το δημόσιο κλειδί της με e-mail στις επαφές της ή να το ανεβάσει στην προσωπική της ιστοσελίδα. Αυτές οι μέθοδοι όμως είναι δυσλειτουργικές στην περίπτωση που κάποιος θέλει να επικοινωνήσει για πρώτη φορά με την Alice άρα δεν έχει λάβει προηγουμένως το public key της και ταυτόχρονα δεν γνωρίζει την προσωπική της ιστοσελίδα, αν υπάρχει.

Για τους λόγους αυτούς, δημιουργήθηκε η ανάγκη να υπάρχουν στο web προσυμφωνημένοι, δημόσιοι και προσβάσιμοι σε όλους ιστότοποι όπου θα συγκεντρώνουν δημόσια κλειδιά χρηστών. Αυτοί είναι οι public key servers, που παρέχουν τη δυνατότητα σε χρήστες να ανεβάζουν το δημόσιο κλειδί τους και ταυτόχρονα τη δυνατότητα αναζήτησης κλειδιών με βάση την διεύθυνση email ή το key ID.

Οι key servers είναι πολύτιμοι και για έναν επιπλέον λόγο. Όταν ένα δημόσιο κλειδί καταχωρείται στον server είτε δημιουργείται μια νέα εγγραφή, είτε το κλειδί αυτό μαζί με τις υπογραφές που το συνοδεύουν συγχωνεύεται με την υπάρχουσα εγγραφή. Με αυτό τον τρόπο ο Bob μπορεί να υπογράψει το δημόσιο κλειδί της Alice με το δικό του (καθώς την γνωρίζει και την εμπιστεύεται) και να στείλει το υπογεγραμμένο κλειδί στην Alice. Εάν η Alice το επιθυμεί θα ανεβάσει ξανά το κλειδί της στον key server, προσθέτοντας στην ουσία την υπογραφή του Bob. Πλέον στην αναζήτηση του public key της Alice, θα έχει προστεθεί η υπογραφή του Bob. Με τον τρόπο αυτό οι ψηφιακές υπογραφές κλειδιών μεταξύ ατόμων γνωστοποιούνται σε τρίτους, δίνοντας την δυνατότητα να υφανθεί ένας ιστός εμπιστοσύνης μεταξύ χρηστών (Web of Trust). Για παράδειγμα ο χρήστης Carlos γνωρίζει τον Bob και αναζητώντας το δημόσιο κλειδί της Alice βλέπει την υπογραφή του Bob. Αν ο Carlos εμπιστεύεται τον Bob, μπορεί να εμπιστευθεί (σε όποιο βαθμό επιθυμεί) και την Alice.

Αρκετοί από τους public key servers επικοινωνούν μεταξύ τους ανταλλάσοντας δεδομένα, οπότε το ανέβασμα ενός κλειδιού σε έναν από τους γνωστούς key servers συνήθως αρκεί για την διάδοσή του στους υπόλοιπους. Κάποιοι από τους γνωστούς key servers είναι οι: pgp.mit.edu, zimmermann.mayfirst.org, keys.riseup.net, pool.sks-keyservers.net .

Συμπερασματικά υπάρχουν οι ακόλουθοι τρόποι διαμοιρασμού του δημοσίου κλειδιού :

εκ του φυσικού σε μια συσκευή αποθήκευσης

με e-mail ως συνημμένο

με ανάρτηση σε μια προσωπική ιστοσελίδα

με ανάρτηση σε έναν ή περισσότερους public key servers

Κανένας από τους παραπάνω τρόπους δεν είναι υποχρεωτικός και ταυτόχρονα ο ένας τρόπος δεν αποκλείει τον άλλον. Το OpenPGP δίνει τη δυνατότητα και την ελευθερία στον χρήστη να καθορίσει τους τρόπους που θα διαμοιράσει το δημόσιο κλειδί του, τον βαθμό που θα εκθέσει το δημόσιο κλειδί του και σε ποιους, χτίζοντας το δικό του δίκτυο εμπιστοσύνης.

Ψηφιακά Πιστοποιητικά

Ψηφιακό πιστοποιητικό (ή πιστοποιητικό δημοσίου κλειδιού) είναι ένα ηλεκτρονικό έγγραφο, το οποίο κάνει χρήση της λειτουργίας των ψηφιακών υπογραφών, για να αντιστοιχίσει δεσμευτικά ένα δημόσιο κλειδί με μια ταυτότητα προσώπου, οργανισμού ή εταιρείας. Με άλλα λόγια το ψηφιακό πιστοποιητικό, πιστοποιεί ότι ένα συγκεκριμένο δημόσιο κλειδί αντιστοιχεί πράγματι σε μια συγκεκριμένη ταυτότητα. Το ψηφιακό πιστοποιητικό, περιέχει το δημόσιο κλειδί του υποκειμένου που πιστοποιείται και την ψηφιακή υπογραφή της οντότητας που πιστοποιεί την ταυτότητα του υποκειμένου.

Ας χρησιμοποιήσουμε και εδώ το γνωστό σχήμα με την Alice και τον Bob. Η Alice έχει ένα δημόσιο κλειδί. Ο Bob θέλει να αποκτήσει το δημόσιο κλειδί της Alice για να επικοινωνήσει μαζί της, αλλά θέλει με κάποιο τρόπο να πιστοποιήσει ότι πρόκειται πράγματι για το δημόσιο κλειδί της Alice και όχι κάποιου τρίτου κακόβουλου.

Υπάρχουν δύο σχήματα εμπιστοσύνης για τη διανομή των δημοσίων κλειδιών και κατ' επέκταση και των πιστοποιητικών με ψηφιακές υπογραφές :

Το πρώτο σχήμα (PKI - Public Key Infrastructure) είναι συγκεντρωτικό και ιεραρχικό και βασίζεται στις Αρχές Πιστοποίησης (CA - Certification Authorities). Στο σχήμα αυτό, τα πιστοποιητικά παράγονται από τις αρχές πιστοποίησης, δηλαδή συγκεκριμένες ευρέως αναγνωρισμένες εταιρείες, όπως είναι η Verisign. Το υποκείμενο που θέλει να πιστοποιηθεί, η Alice, απευθύνεται σε μια Αρχή Πιστοποίησης, παρέχοντας το δημόσιο κλειδί της και κάποια στοιχεία της ταυτότητάς της. Η Αρχή Πιστοποίησης, παίρνει το δημόσιο κλειδί της Alice και το υπογράφει ψηφιακά. Όταν ο Bob θέλει να επικοινωνήσει με την Alice, λαμβάνει το πιστοποιητικό της. Με την προϋπόθεση ότι ο Bob εμπιστεύεται την Αρχή Πιστοποίησης που παρήγαγε και υπέγραψε το πιστοποιητικό, με την προϋπόθεση ότι ο Bob είναι ήδη γνώστης του δημοσίου κλειδιού της Αρχής Πιστοποίησης, τότε είναι σε θέση να χρησιμοποιήσει το δημόσιο κλειδί της Alice που περιέχεται στο πιστοποιητικό, όντας σίγουρος για την αυθεντικότητά του.

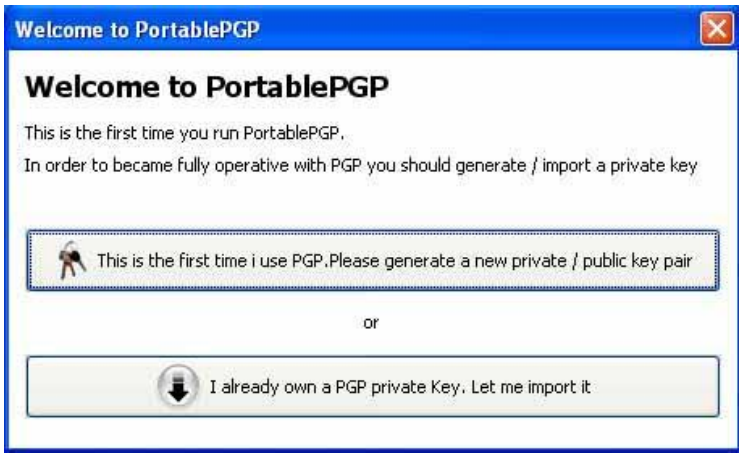
Το δεύτερο σχήμα είναι οριζόντιο και αποκεντρωμένο, είναι το λεγόμενο Δίκτυο Εμπιστοσύνης (Web of Trust). Στο σχήμα αυτό δεν υπάρχουν κεντρικά σημεία που οι συμμετέχοντες οφείλουν να αναγνωρίσουν, όπως οι Αρχές Πιστοποίησης παραπάνω. Στο σχήμα αυτό, ένα δημόσιο κλειδί υπογράφεται είτε από τον ίδιο του τον κάτοχο είτε συνηθέστερα από τρίτα ομότιμα πρόσωπα. Η ψηφιακή υπογραφή ενός δημοσίου κλειδιού, υποδεικνύει ότι ο υπογράφων το δημόσιο κλειδί, είναι σε θέση να γνωρίζει και να εγγυάται για τη ταυτότητα του κατόχου του δημοσίου κλειδιού. Οι ψηφιακές υπογραφές σε δημόσια κλειδιά μεταξύ ομότιμων, συνθέτουν ένα δίκτυο εμπιστοσύνης. Με πιο απλά λόγια, η Alice γνωρίζει τον Bob και επιπλέον γνωρίζει με βεβαιότητα και εγκυρότητα το δημόσιο κλειδί του Bob, το οποίο της έχει παραδώσει αυτοπροσώπως. Έτσι η Alice υπογράφει ψηφιακά το δημόσιο κλειδί του Bob. Εάν τώρα ο Charlie, θέλει να αποκτήσει το δημόσιο κλειδί του Bob, και εμπιστεύεται την Alice η οποία το έχει υπογράψει όπως είδαμε, τότε θεωρεί έγκυρο το δημόσιο κλειδί του Bob.

Χρησιμοποιώντας το PortablePGP

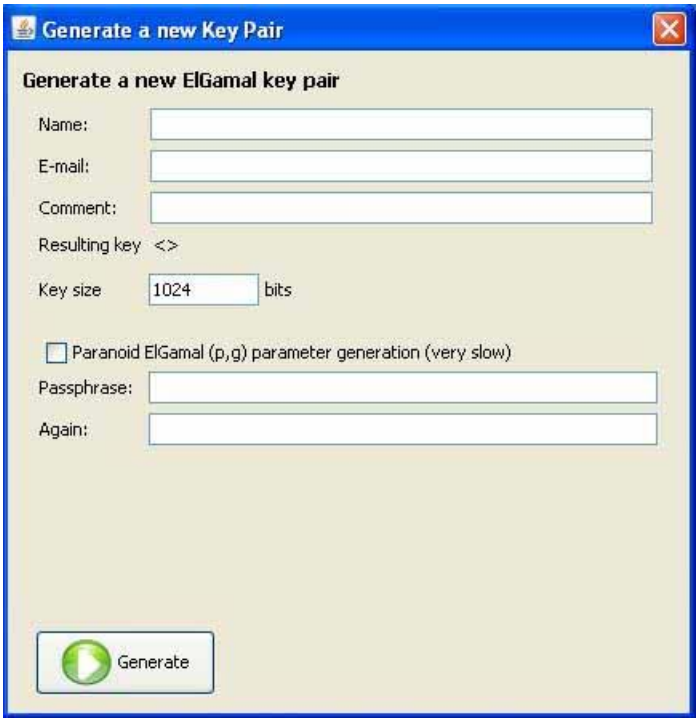
Το πρόγραμμα PortablePGP (http://ppgp.sourceforge.net/) είναι μια δωρεάν, ανοιχτού κώδικα εφαρμογή που μπορεί να χρησιμοποιηθεί για την παραγωγή κλειδιών, την κρυπτογράφηση, αποκρυπτογράφηση και πιστοποίηση της αυθεντικότητας μηνυμάτων. Η εφαρμογή είναι γραμμένη σε Java και υπάρχει σε φορητή έκδοση για USB που μπορεί να εκτελεστεί χωρίς τροποποιήσεις σε συστήματα Windows και Linux.

Για να τη χρησιμοποιήσετε θα χρειαστεί αρχικά να εμφανίσετε τις επεκτάσεις αρχείων των Windows που είναι κρυμμένες από προεπιλογή. Για συστήματα Windows 7 ανοίξτε το Windows Explorer και επιλέξτε Εργαλεία > Επιλογές φακέλων, κάντε κλικ στην καρτέλα Προβολή και

καταργήστε την επιλογή «Απόκρυψη επεκτάσεων για γνωστούς τύπους αρχείων». Αποσυμπιέστε το αρχείο που κατεβάσατε σε ένα δίσκο USB. Αυτό δημιουργεί ένα φάκελο με τίτλο usb_version (απλό κλικ στο φάκελο ή F2 για να τον μετονομάσετε). Κάντε διπλό κλικ στο PortablePGP.exe μέσα στο φάκελο για να ξεκινήσει η εφαρμογή.



Κάντε κλικ στο επάνω κουμπί αν δεν έχετε ήδη ένα ιδιωτικό κλειδί PGP που να μπορεί να εισαχθεί από ένα αρχείο κειμένου. Εισάγετε ένα όνομα και μια συνθηματική φράση - όσο μεγαλύτερη, τόσο καλύτερα.



Για να εξαγάγετε το δημόσιο κλειδί σας: Για να εξάγετε το δημόσιο κλειδί σας, πατήστε στην επιλογή Keyring του μενού και στη συνέχεια επιλέξτε το όνομα σας στο πλαίσιο Public Keys και κάντε κλικ στο κουμπί με τη δισκέτα για να εξαχθεί σε ένα αρχείο. Πληκτρολογήστε ένα όνομα με επέκταση .txt και αποθηκεύστε το αρχείο. Ανοίξτε το αρχείο και επιλέξτε όλο το κείμενο (μαζί με τις παύλες), με [Ctrl + A]. Το κείμενο αυτό είναι το δημόσιο κλειδί και μπορείτε να το επικολλήσετε στον e-mail client σας ή να το συνδέσετε με ένα μήνυμα ηλεκτρονικού ταχυδρομείου.

Για να εισάγετε ένα δημόσιο κλειδί: Επιλέξτε και αντιγράψτε το κλειδί, μαζί με τις παύλες. Ανοίξτε το Σημειωματάριο κάντε επικόλληση και αποθηκεύστε το σαν αρχείο κειμένου. Βεβαιωθείτε ότι δεν υπάρχουν κενά ή κενές γραμμές πριν από το ----- BEGIN PGP PUBLIC KEY BLOCK -----. Πατήστε keyring στο αριστερό μενού και στη συνέχεια κάντε κλικ στο κουμπί με το κάτω βέλος, στην ενότητα Δημόσια Κλειδιά, για την εισαγωγή από αρχείο.

Για να στείλετε ένα κρυπτογραφημένο μήνυμα: Πατήστε στην επιλογή Encrypt στο αριστερό μενού και στη συνέχεια Κρυπτογράφηση Κάντε κλικ στο μενού PortablePGP και επιλέξτε το στρογγυλό κουμπί «Encrypt a file» αν θέλετε να κρυπτογραφήσετε ένα αρχείο, ή το «Encrypt Text» αν θέλετε να πληκτρολογήσετε ή να επικολλήσετε κείμενο για κρυπτογράφηση. Επιλέξτε το αρχείο ή πληκτρολογήστε το μήνυμά σας, επιλέξτε τον παραλήπτη προορισμού (το Δημόσιο κλειδί του οποίου θα πρέπει να έχετε εισάγει) και κάντε κλικ στο κουμπί Κρυπτογράφηση. Θα ανοίξει ένας διορθωτής κειμένου που θα περιέχει το κρυπτογραφημένο μήνυμα, το οποίο μπορείτε να αντιγράψετε στο Πρόχειρο ή να αποθηκεύσετε σαν αρχείο κειμένου.

Για να διαβάσετε ένα κρυπτογραφημένο μήνυμα: Για να διαβάσετε ένα μήνυμα, επιλέξτε Decrypt στο μενού του PortablePGP και επιλέξτε το στρογγυλό κουμπί «Decrypt a file» αν θέλετε να αποκρυπτογραφήσετε ένα αρχείο ή το «Decrypt ASCII-Armored Text» αν θέλετε να επικολλήσετε το προς αποκρυπτογράφηση κείμενο. Θα σας ζητηθεί να εισάγετε την συνθηματική φράση σας (που είχατε ορίσει όταν δημιουργήσατε τα κλειδιά) και θα ανοίξει ο editor με το μήνυμα.

Για να διαγράψετε μηνύματα ασφάλεια: Το PortablePGP δεν περιλαμβάνει ασφαλή ολοκληρωτική διαγραφή μηνυμάτων, οπότε θα πρέπει να χρησιμοποιήσετε μια εφαρμογή σαν το File Shredder (www.fileshredder.org).

Πηγές

http://www.pgpguide.20m.com
https://skytal.es/wiki/Κρυπτογράφηση_δημόσιου_κλειδιού