# Διαχείριση Κωδικών & Κρυπτογράφηση Αρχείων

Athens CryptoParty #1
23/12/12
hackerspace.gr

CRYPTO PARTY

# Λίγα εισαγωγικά

- Η ψηφιακή ασφάλεια είναι ένα ιδιαίτερα πολύπλοκο ζήτημα, καθώς αφορά εξειδικευμένη τεχνολογία, είτε σε επίπεδο software είτε hardware. Επιπλέον το πεδίο αυτό είναι υπό διαρκή και ταχεία εξέλιξη. Δεν υπάρχει όμως λόγος παραίτησης ή απελπισίας...
- Η τεχνολογία είναι μέρος της καθημερινότητας. Είναι δυνατό και χρήσιμο, να κατανοήσουμε στοιχειωδώς τον τρόπο λειτουργίας των τεχνολογικών εργαλείων, να έχουμε συναίσθηση των κινδύνων που προκύπτουν, και γιατί όχι να μάθουμε να προφυλασσόμαστε.

Disclaimer : Τα όσα αναφέρονται στην παρουσίαση που ακολουθεί έχουν προκύψει από προσωπική αναζήτηση και ενασχόληση. Πιθανόν να υπάρχουν λάθη ή ανακρίβειες. Αναζητήστε περισσότερες πληροφορίες επί των θεμάτων στο διαδίκτυο, ελέγξτε, ρωτήστε ανθρώπους που εμπιστεύεστε, δοκιμάστε.

# Το λογισμικό που θα χρειαστούμε σε λίγο

- Windows – Κατεβάστε το keepass από εδώ http://keepass.info/download.html
- Linux – κατεβάστε από τα repos το keepass2 ή το keepassx

- Windows or Linux – Κατεβάστε το Truecrypt από εδώ http://www.truecrypt.org/downloads -

# Κωδικοί

- Οι κωδικοί χρησιμοποιούνται παντού. Από το ATM μέχρι το κινητό, το email, τον υπολογιστή. Ένας μέσος χρήστης υπολογιστή και διαδικτύου θα συναντήσει αρκετές δεκάδες φορές την εισαγωγή username και password,
- Οι κωδικοί εν γένει χρησιμοποιούνται για να ασφαλίσουν κάποιο σύστημα ή κάποια δεδομένα από μη εξουσιοδοτημένη πρόσβαση.
- Συνήθως είναι ακολουθίες χαρακτήρων (νούμερα, γράμματα, σύμβολα).
- Οι κωδικοί, συχνά, είναι το αδύνατο σημείο ενός συστήματος ασφαλείας. Ο μόνος, χρονικά υλοποιήσιμος τρόπος, να παραβιάσεις ένα σύστημα. Είτε διότι ο κωδικός είναι προβλέψιμος, είτε αδύναμος, είτε γιατί ο χρήστης μπορεί να εξαναγκαστεί να τον αποκαλύψει.

# Κωδικοί, καλές και κακές πρακτικές

- Είναι κακή πρακτική να επαναχρησιμοποιείται ο ίδιος κωδικός για διαφορετικά πράγματα πχ ίδιο κωδικό στο email, στο PC, στο κρυπτογραφημένο αρχείο.
- Είναι καλή πρακτική  ένας χρήστης να χρησιμοποιεί διαφορετικό κωδικό για κάθε υπηρεσία. Πχ. Αν παραβιαστεί /υποκλαπεί/ μαθευτεί ο κωδικός για το email ενός χρήστη δεν θα κινδυνεύει το PC με το ίδιο login.
- Ταυτόχρονα είναι καλή πρακτική, κάθε ένας από τους διαφορετικούς κωδικούς να είναι μην είναι απλός ή/και προβλέψιμος.

# Πολυπλοκότητα Κωδικών

- Ένας ισχυρός κωδικός είναι πολύπλοκος. Η πολυπλοκότητα ενός κωδικού έχει να κάνει με το πόσο χρόνο ή επεξεργαστική ισχύ πρέπει να δαπανήσει κάποιος, για να βρει τον κωδικό που προστατεύει ένα σύστημα
- Ένας κωδικός έχει δύο βασικά χαρακτηριστικά : το μήκος και τη βάση. Μήκος είναι ο αριθμός των χαρακτήρων που τον απαρτίζουν. Βάση είναι το σύνολο των στοιχείων από το οποίο ο χρήστης μπορεί να επιλέξει χαρακτήρες. Παράδειγμα :

  Gijoe56 → η βάση είναι τα μικρά και κεφαλαία γράμματα και οι αριθμοί
- Όσο μεγαλύτερο το μήκος και η βάση, τόσο πιο πολύπλοκος είναι ο κωδικός.
- Γενικά πιο σημαντικό είναι το μήκος ενός κωδικού. Φτιάξτε φράσεις κλειδιά (passphrases) και όχι απλούς κωδικούς (passwords), με μήκος πάνω από 15 χαρακτήρες.
- Ο κωδικός δεν πρέπει να είναι προβλέψιμος. Αντικαταστάσεις του τύπου a > 4 , o > 0 κλπ είναι συνήθεις, σε βαθμό που ακόμα και προγράμματα σπασίματος κωδικών τις έχουν ενσωματώσει.
- Ιδανικά ένας κωδικός έχει πολύ μεγάλο μήκος και τυχαία ακολουθία χαρακτήρων. Παράδειγμα : *l;k(%#ggsSgf^&AMmks^%^ad90JHAr6h]-=2*0asmd&s=_!2jm;a*

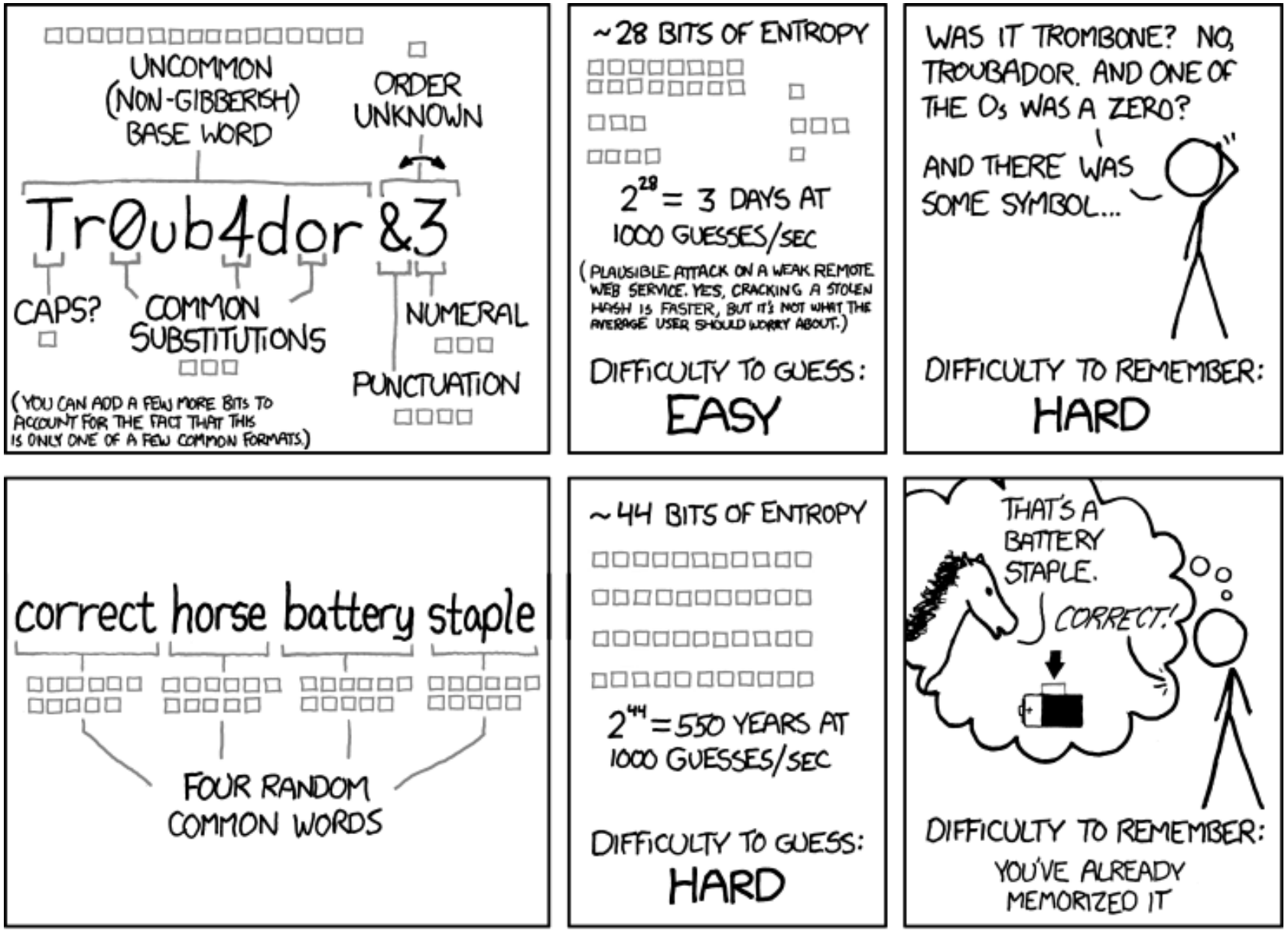
# Διαχείριση Κωδικών – Keepass

- Με βάσει τα όσα είπαμε πριν ο χρήστης χρειάζεται δεκάδες, μεγάλους και σχεδόν τυχαίους κωδικούς.
- Η απομνημόνευση τους αδύνατη...
- Για τον λόγο αυτό υπάρχουν προγράμματα δημιουργίας, αποθήκευσης και διαχείρισης κωδικών.
- Ένα τέτοιο είναι το Keepass. Είναι ανοικτού κώδικα και προσφέρει τη δυνατότητα να δημιουργήσεις μια κρυπτογραφημένη βάση δεδομένων (ένα αρχείο) μέσα στο οποίο θα αποθηκεύονται όλοι οι κωδικοί.
- Είναι φιλικό στη χρήση, μπορείς να κατηγοριοποιείς του κωδικούς. Ακόμα παρέχει γεννήτρια τυχαίων κωδικών.
- http://keepass.info/download.html < το εκτελέσιμο για εγκατάσταση σε Windows

# Διαχείριση Κωδικών – Απομνημόνευση κωδικών

- Χρησιμοποιώντας ένα διαχειριστή κωδικών, μπορούμε να έχουμε ένα διαφορετικό κωδικό για κάθε υπηρεσία, ο οποίος επιπλέον να είναι μεγάλος και τυχαίος.
- Και πάλι όμως θα χρειαστεί να απομνημένευσουμε κάποιους κωδικούς, πχ της βάσης του keepass
- Για τη δημιουργία και απομνημόνευση ενός κωδικού χρειάζεται να βρούμε ένα pattern που θα μας ταιριάζει, θα το θυμόμαστε και θα είναι δύσκολο να το προβλέψει κάποιος αντίπαλος.
- Αποφεύγετε patterns του τύπου secretpass@gmail, secretpass@yahoo κλπ
- Σκεφτείτε μια οικεία φράση που θα βγάζει νόημα για εσάς. Προσθέστε κάποιο σύμβολο ανάμεσα στις λέξεις, αυξάνοντας το μήκος και την πολυπλοκότητα. Προσπαθήστε να αλλάξετε την ορθογραφία των λέξεων για να αποφύγετε επιθέσεις λεξικού.

# Password strength by xkcd.com




THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

# Στη πράξη

# Δεδομένα, ένα πρόβλημα

- Δεδομένα είναι δομές συμβόλων που εμπεριέχουν χρήσιμη πληροφορία. Δεδομένα είναι ένα αρχείο κειμένου, εικόνας ή ήχου, είναι τα στοιχεία login σε ένα site(username/password), είναι ο αριθμός του τηλεφώνου μας, ακόμα και η διάρκεια μιας κλήσης μας...
- Το πρόβλημα : η αποθήκευση ή ανταλλαγή δεδομένων με τρόπο ούτως ώστε να μην είναι δυνατή η μη εξουσιοδοτημένη ανάγνωσή τους
  & να μην είναι δυνατή η αλλοίωση τους.
- Παράδειγμα : Η Αλίκη θέλει να αποθηκεύσει στον υπολογιστή της, αρχεία ήχου και να είναι αδύνατο για οποιονδήποτε πέραν αυτής να τα ακούσει.
- Παράδειγμα 2 : Ο Φοίβος θέλει να στείλει ένα αρχείο κειμένου στην Αλίκη, και να είναι σίγουρος ότι η Αλίκη και μόνο αυτή, θα μπορέσει να το διαβάσει.

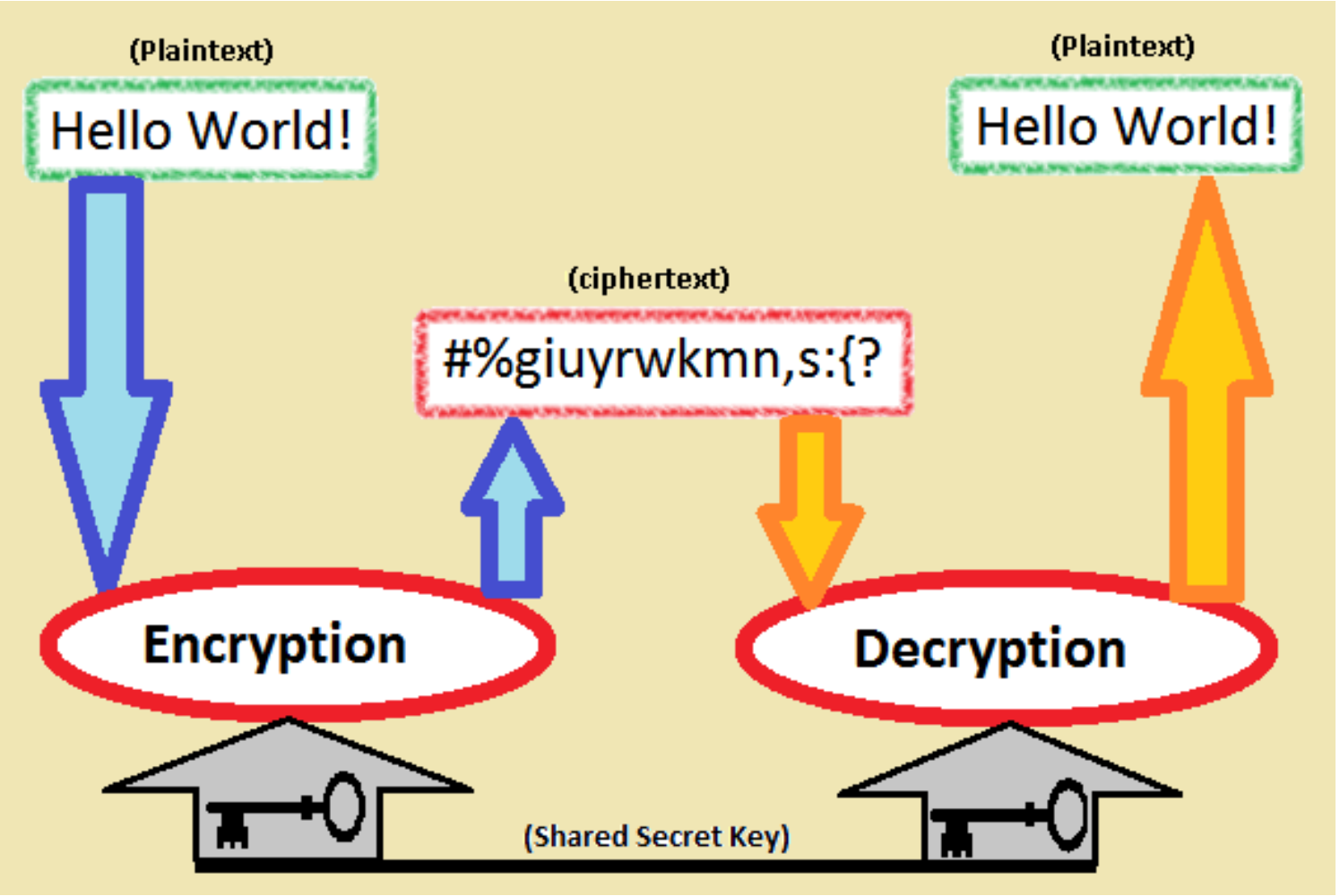
# Κρυπτογραφία, μια κάποια λύση

- Η κρυπτογραφία είναι κλάδος των μαθηματικών που μελετάει τεχνικές για την ασφαλή επικοινωνία (δεδομένων) σε εχθρικό περιβάλλον
- Πιο συγκεκριμένα, στην κρυπτογραφία μελετάται ο τρόπος με τον οποίον τα δεδομένα μπορούν να μετασχηματιστούν σε κάτι που ο εχθρός θα είναι αδύνατο να καταλάβει και να αλλοιώσει.
- Τα δεδομένα κρυπτογραφούνται με βάση κάποιον αλγόριθμο, δηλαδή μια ακολουθία μετασχηματισμών. Υπάρχουν πολλοί κρυπτογραφικοί αλγόριθμοι.

# Συμμετρική Κρυπτογραφία

- Στους κρυπτογραφικούς αλγόριθμούς περιλαμβάνεται η εισαγωγή ενός κλειδιού
- Συμμετρική κρυπτογραφία έχουμε στην περίπτωση που το ίδιο κλειδί χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση δεδομένων.
- Παράδειγμα : Η Αλίκη χρησιμοποιεί ένα κλειδί για να κρυπτογραφήσει ένα αρχείο ήχου στον υπολογιστή της. Με το ίδιο κλειδί το αποκρυπτογραφεί.
- Παράδειγμα 2 : Ο φοίβος κρυπτογραφεί με ένα κλειδί το αρχείου κειμένου που στέλνει στην Αλίκη. Η Αλίκη έχει το ίδιο κλειδί με τον Φοίβο, αποκρυπτογραφεί και διαβάζει το κείμενο.

# Συμμετρική κρυπτογραφία, σχήμα



# Κρυπτογράφηση αρχείων

- Η συμμετρική κρυπτογραφία βρίσκει εφαρμογή στην κρυπτογράφηση των δεδομένων που έχουμε στο PC μας. Παραδειγμα, η κρυπτογράφηση αρχείων ή/και ολόκληρου του σκληρού δίσκου
- Χρήση συγκεκριμένων προγραμμάτων που υλοποιούν κρυπτογραφικούς αλγόριθμους
- Ένα τέτοιο πρόγραμμα λαμβάνει ένα αρχείο που επιλέγει ο χρήστης καθώς και μια φράση κλειδί (passphrase) και παράγει δεδομένα μη αναγνώσιμα για κάποιον τρίτο.

# Κρυπτογράφηση αρχείων (2)

- Τα δεδομένα προστατεύονται μόνο όσο βρίσκονται σε κρυπτογραφημένη μορφή. Όταν ο χρήστης χρησιμοποιήσει το κλειδί για να αποκρυπτογραφήσει τότε αυτό καθίσταται ευάλωτο πχ μολυσμένος υπολογιστής που καταγράφει περιεχόμενο αρχείων, χτύπημα πλήκτρων, printscreen πχ κλοπή laptop ενώ τα αρχεία ειναι σε μη κρυπτογραφημένη μορφή
- Το passphrase είναι το αδύνατο σημείο της κρυπτογράφησης. Είτε είναι αδύναμο, είτε προβλέψιμο, είτε απλώς ο χρήστης εξαναγκαστεί να το παραδώσει.

# Κρυπτογράφηση αρχείων (2)

Τι επιλογές υπάρχουν :

- Μη κρυπτογραφημένο λειτουργικό σύστημα αλλά κρυπτογράφηση μεμονωμένων αρχείων που θεωρούνται ευαίσθητα και βρίσκονται στο ιδιο κομμάτι του δίσκου με το λειτουργικό σύστημα
- Μη κρυπτογραφημένο partition με το λειτουργικό και κρυπτογραφημένο partition με αρχεία
- Μη κρυπτογραφημένο λειτουργικό σύστημα και εξωτερικός κρυπτογραφημένος δίσκος
- Πλήρης κρυπτογράφηση συστήματος, δηλαδή κρυπτογράφηση και του ίδιου του λειτουργικού συστήματος και των αρχείων στο ίδιο κομμάτι του δίσκου (η καλύτερη λύση)

# Λογισμικό κρυπτογράφησης αρχείων και δίσκων

- Ένα σωστό πρόγραμμα κρυπτογράφησης, χρησιμοποιεί γνωστούς και δημοσιοποιημένους αλγόριθμους που δεν έχουν σπάσει πχ AES, Blowfish, Serpent
- Ένα τέτοιο πρόγραμμα, έχει ανοικτό πηγαίο κώδικα, ο οποίος ιδανικά έχει δοκιμαστεί/αναλυθεί απο άλλους προγραμματιστές
- Αποφεύγετε κλειστά (proprietary) προγράμματα κρυπτογράφησης και πολύ περισσότερο προγράμματα που χρησιμοποιούν άγνωστους αλγόριθμους κρυπτογράφησης

# Λογισμικό κρυπτογράφησης αρχείων και δίσκων

- Για συστήματα Windows, δημοφιλής λύση κρυπτογράφησης είναι το Truecrypt. Ειναι ανοικτού κώδικα, προσφέρει μια πλειάδα επιλογών (κρυπτογράφηση usb ή ολόκληρου δίσκου, hidden volumes) και αρκετά φιλικό στη χρήση. Άλλη λύση είναι το DiskCryptor και FreeOTFE
- Για συστήματα Linux, διάφορες επιλογές όπως LUKS, EncFS και Truecrypt, FreeOTFE, GPG
- Ακόμα, αρκετές διανομές Linux, προσφέρουν τη δυνατότητα πλήρους ή μερικής  κρυπτογράφησης του συστήματος κατά την εγκατάσταση πχ Debian, Ubuntu, Fedora
- Στις περισσότερες περιπτώσεις, αρχεία κρυπτογραφημένα με ένα πρόγραμμα είναι ασύμβατα/μη αναγνώσιμα με ένα άλλο

# Truecrypt

- Το εκτελέσιμο αρχείο για την εγκατάσταση κατεβαίνει από το http://www.truecrypt.org/ . Αυτό ισχύει για όλες τις πλατφόρμες, Windows, Linux ή Mac.
- Δεν είναι ενσωματωμένο σε καμία Linux διανομή λόγω προβληματικής άδειας με την οποία διανέμεται. Αν και κατά καιρούς έχουν υπάρξει συζητήσεις σχετικά με την αξιοπιστία των developpers και του ίδιου του λογισμικού, το Truecrypt παραμένει μια κοινώς αποδεκτή λύση (μέχρι αποδείξεως του εναντίου...). Ευτυχώς σε Linux διανομές υπάρχουν αρκετές και αξιόπιστες λύσεις για κρυπτογράφηση.
- Υπάρχει μια υποσχόμενη εναλλακτική. Το tcplay https://github.com/bwalex/tc-play free BSD-licenced fully featured Truecrypt implementation. Αν μπορείς, βοήθα γράφοντας κώδικα!

# Truecrypt

- Δυνατότητες : ecrypted file container, hidden volumes, full system encryption σε Windows
- Encrypted File Container : Δημιουργείται ένα κρυπτογραφημένο αρχείο-δοχείο. Αυτό με την χρήση κωδικού, αποκρυπτογραφείται και χρησιμοποιείται σαν εξωτερικος δίσκος. Αφού αποθηκεύσει ο χρήστης ό,τι χρειάζεται, τον κλείνει. Το δοχείο αυτό μπορεί να είναι οποιουδήποτε μεγέθους επιλέξει ο χρήστης, και συμπεριφέρεται σαν κανονικό αρχείο (μπορείς να το μεταφέρεις, να το διαγράψεις κοκ).
- Hidden Volumes : Υπό ορισμένες συνθήκες ένας χρήστης μπορεί να αναγκαστεί να παραδώσει τον κωδικό του File Container που έφτιαξε με το Truecrypt, και να αποκαλύψει όλα τα περιεχόμενα που ήθελε να προστατεύσει. Για τον λόγο αυτό το Truecrypt υποστηρίζει τα Hidden Volumes, δηλαδή κρυφούς τομείς σε ένα αρχείο file container.  Το hidden volume ειναι κρυφό container μέσα στο container. Φυσικά έχει διαφορετικό κωδικό από το εξωτερικό container. Έτσι, ανοίγοντας το αρχείο με το Truecrypt, ανάλογα με ποιον κωδικό θα δώσει ο χρήστης, ανοίγει το κανονικό ή το hidden.

# Στη πράξη