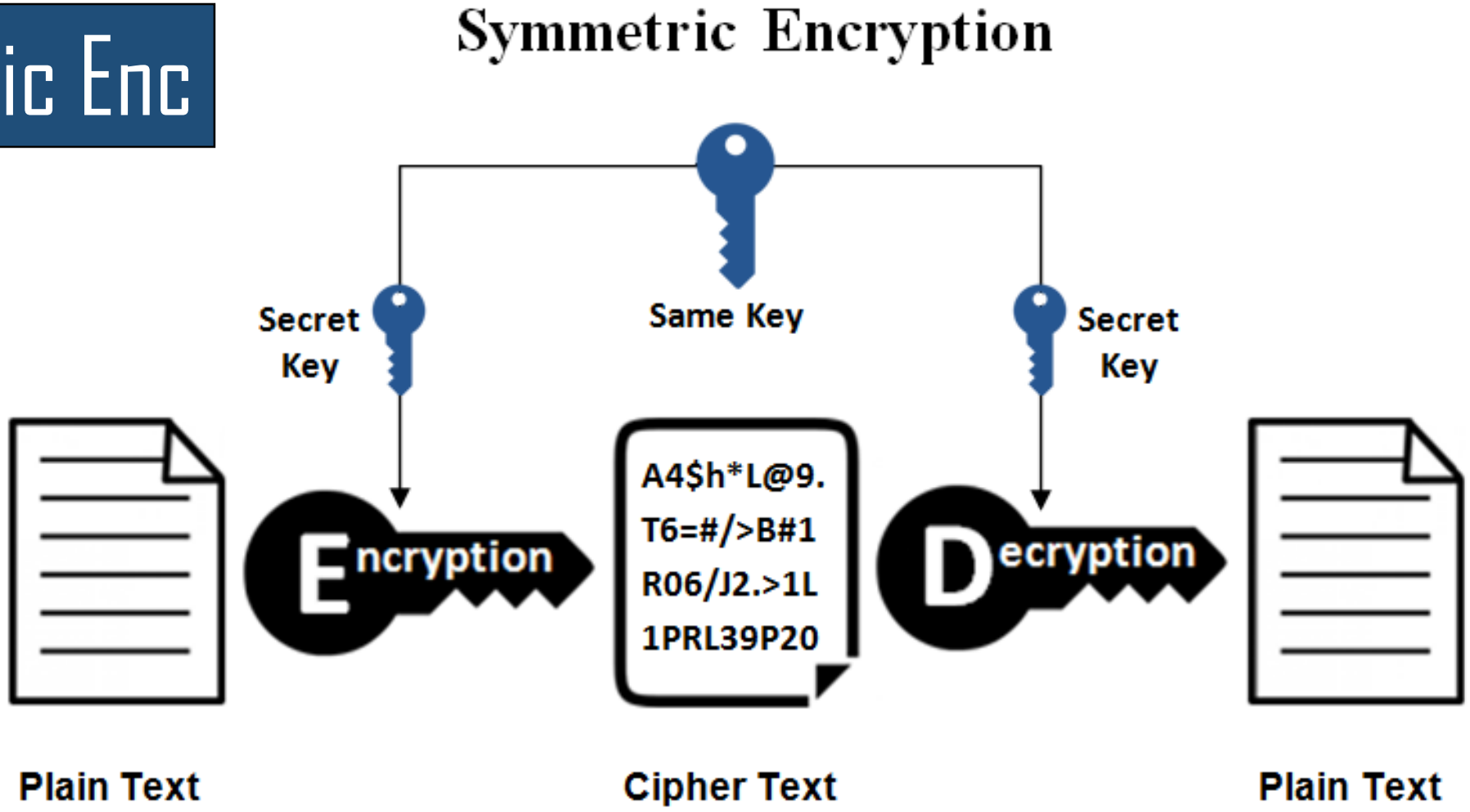
Cryptography - PGP

BY STYLIANOS KARAGIANNIS

PhD Candidate | Ionian University

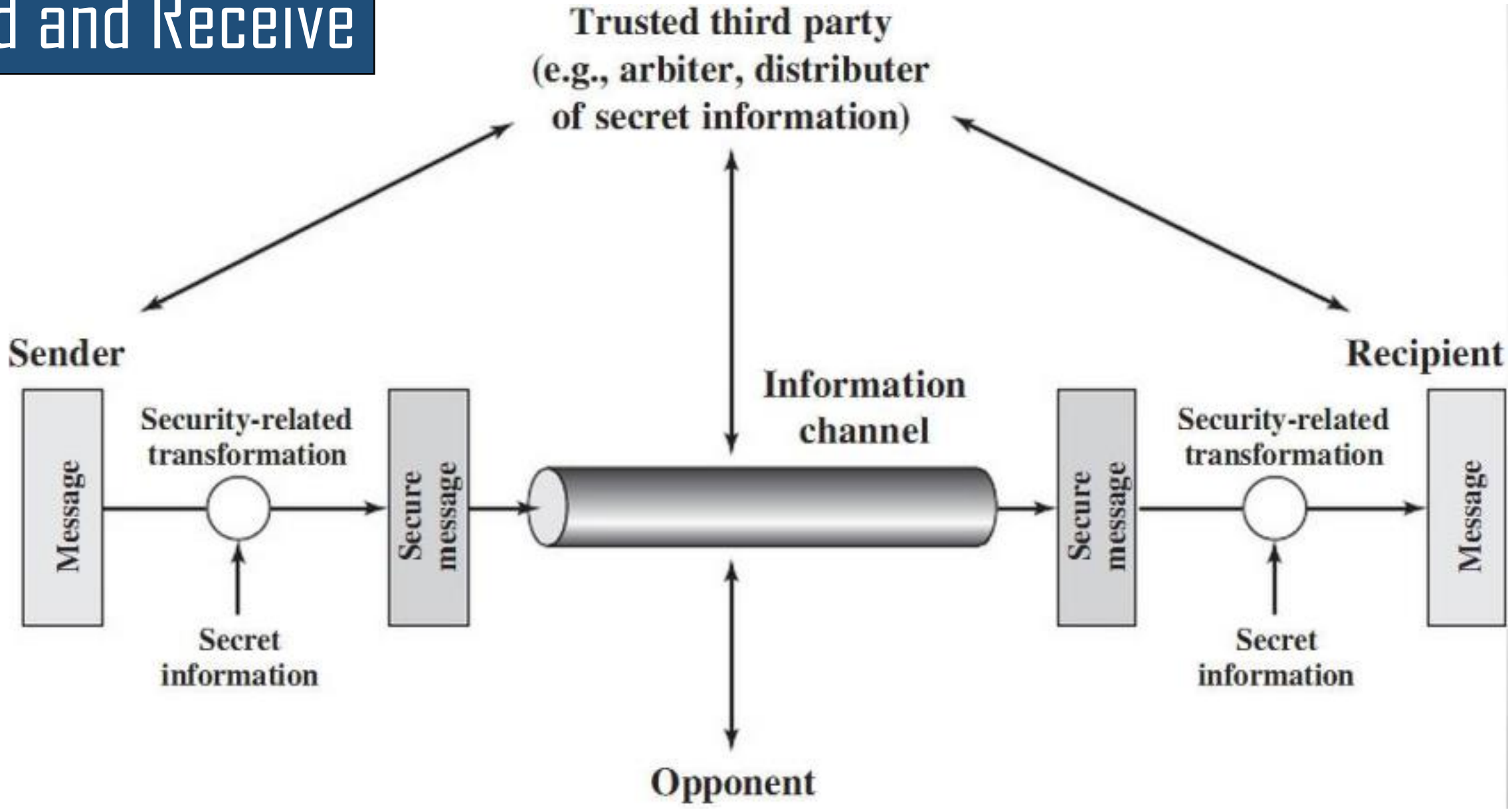
Symmetric Enc



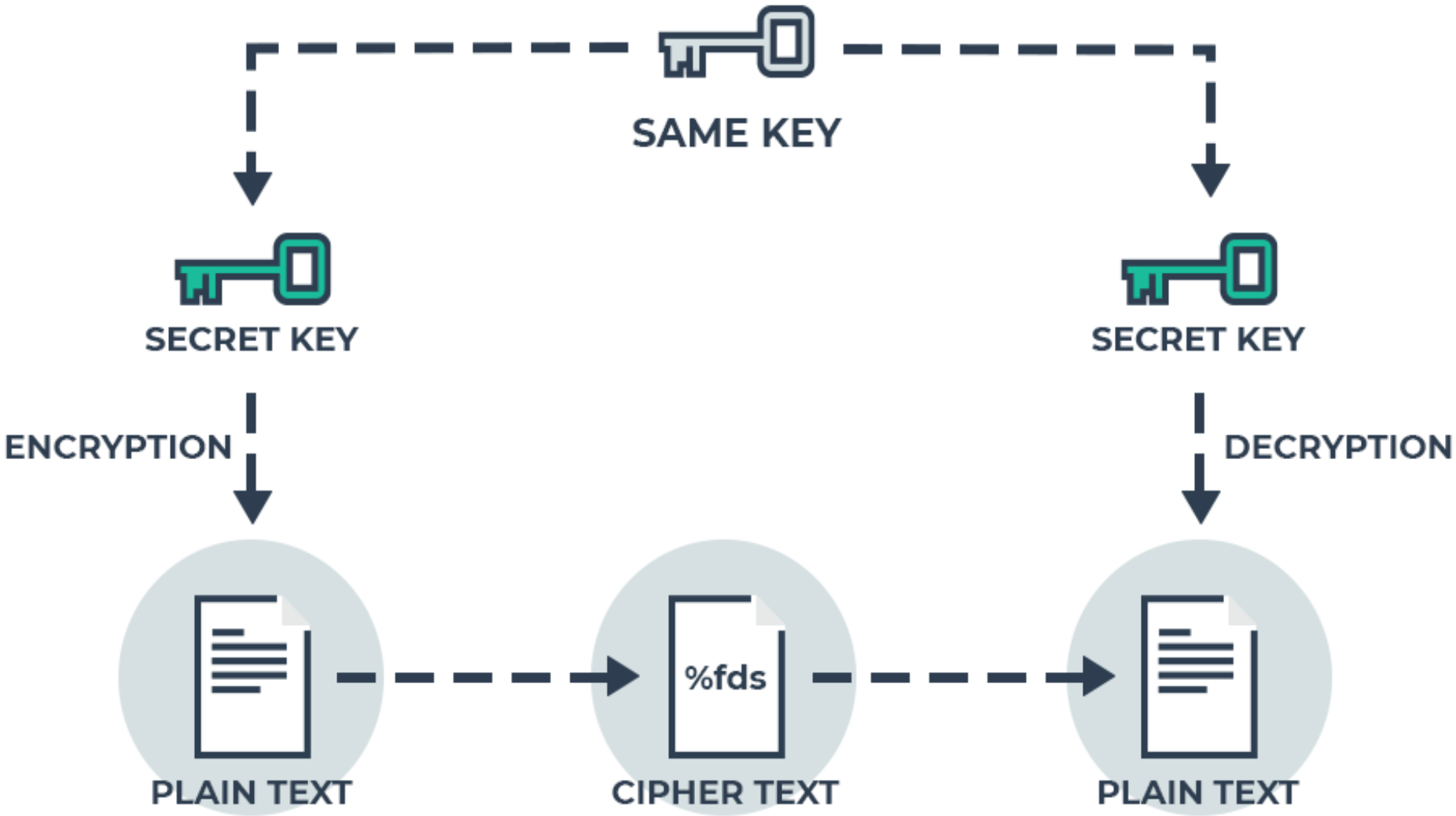
ABCDEFGHIJKLMNOPQRSTUVWXYZ Plain
FGHIJKLMNOPQRSTUVWXYZABCDE Encrypted

COMPUTER SCIENCE Plain
HTRUZYJWXHNJSHJ Encrypted

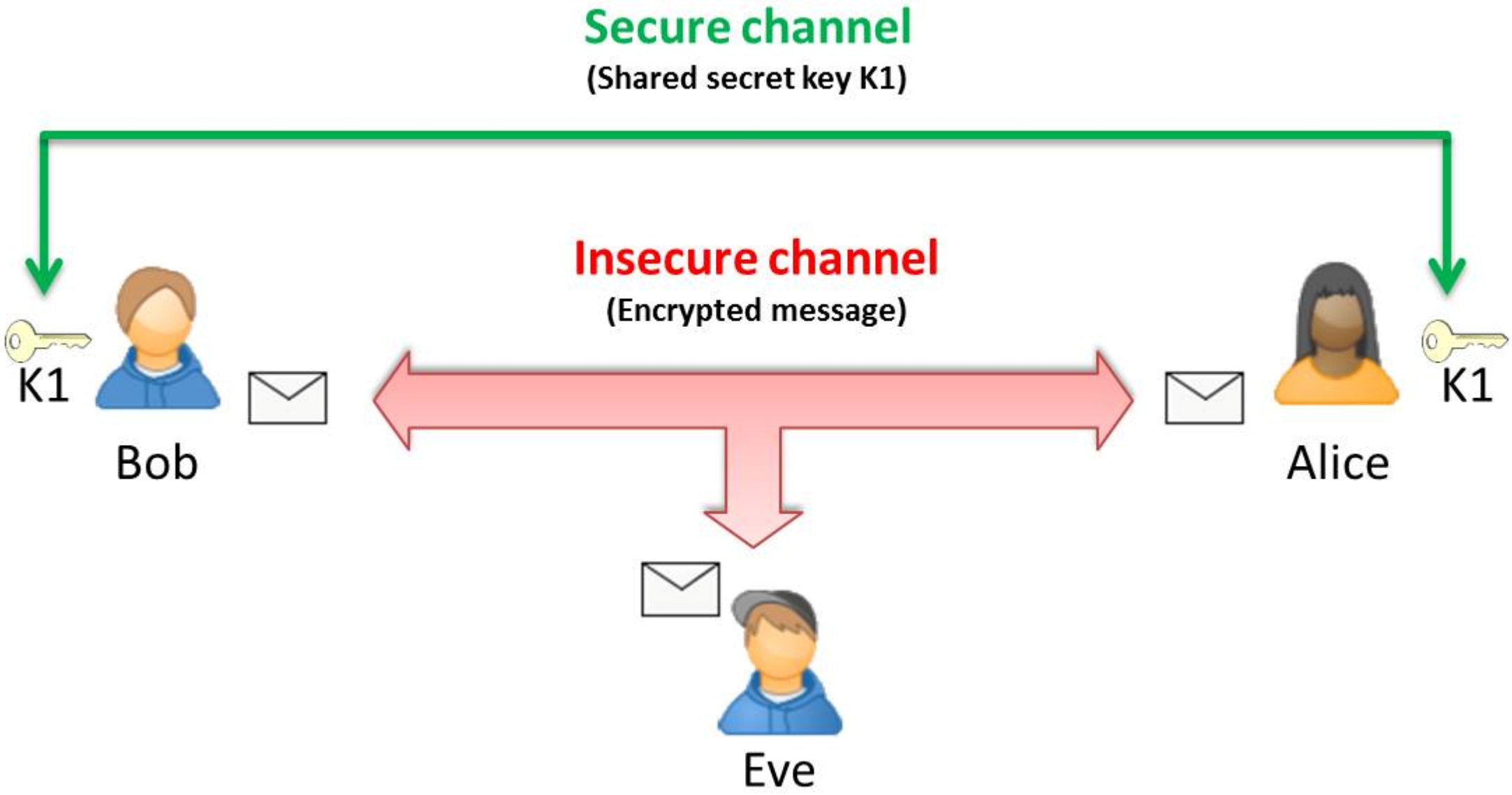
Send and Receive



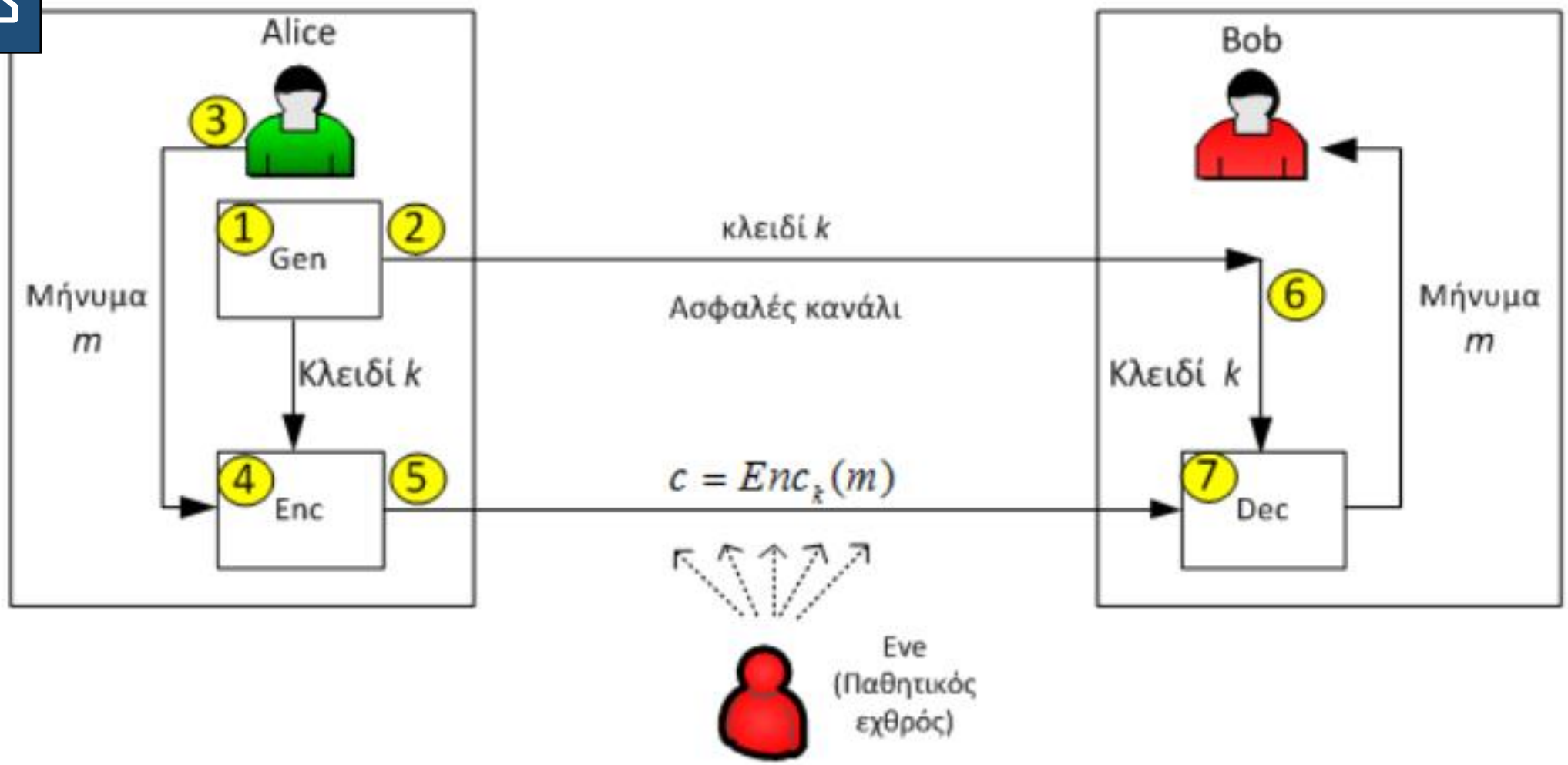
Secret - Symmetric



Channels of Communication

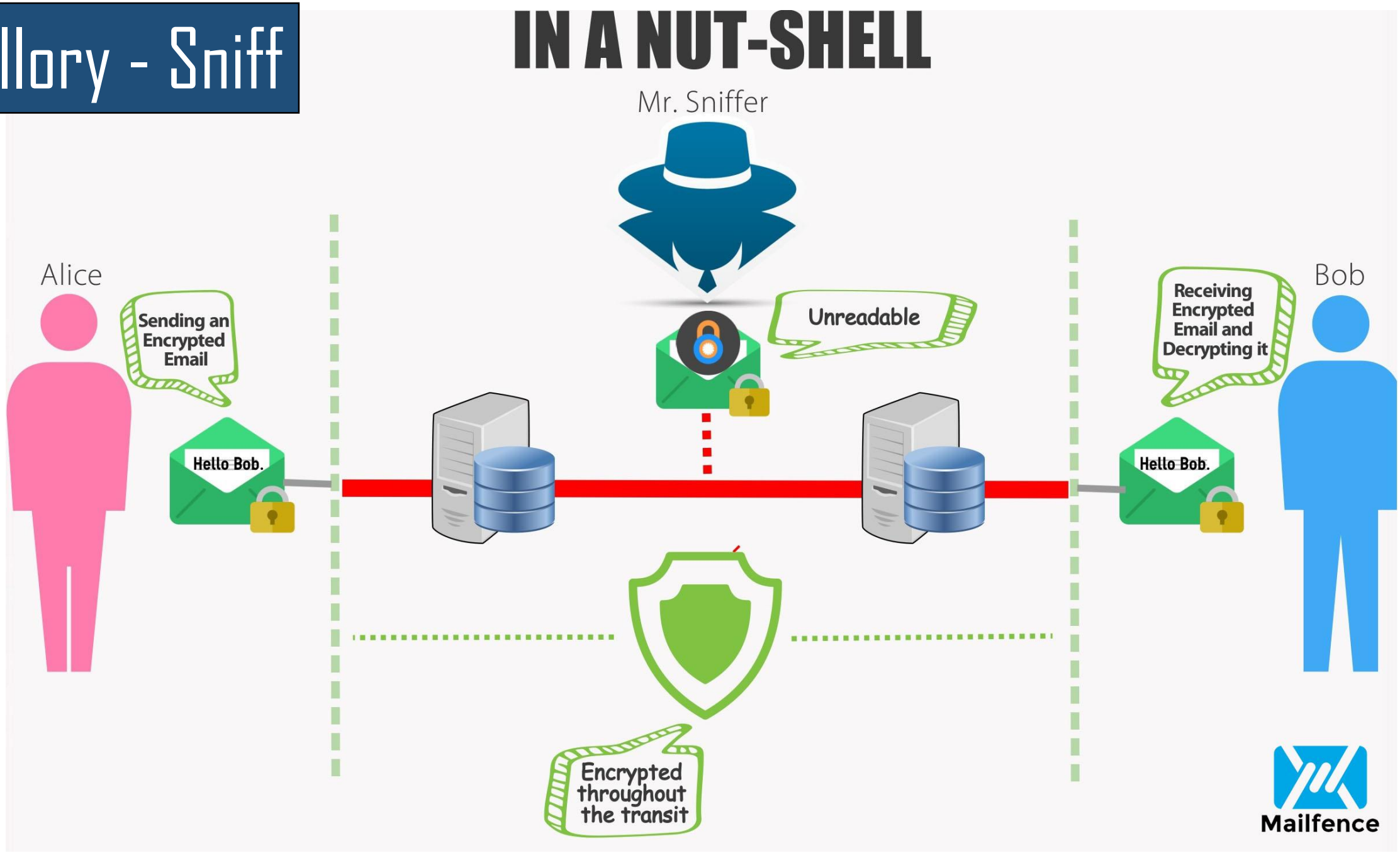


Models

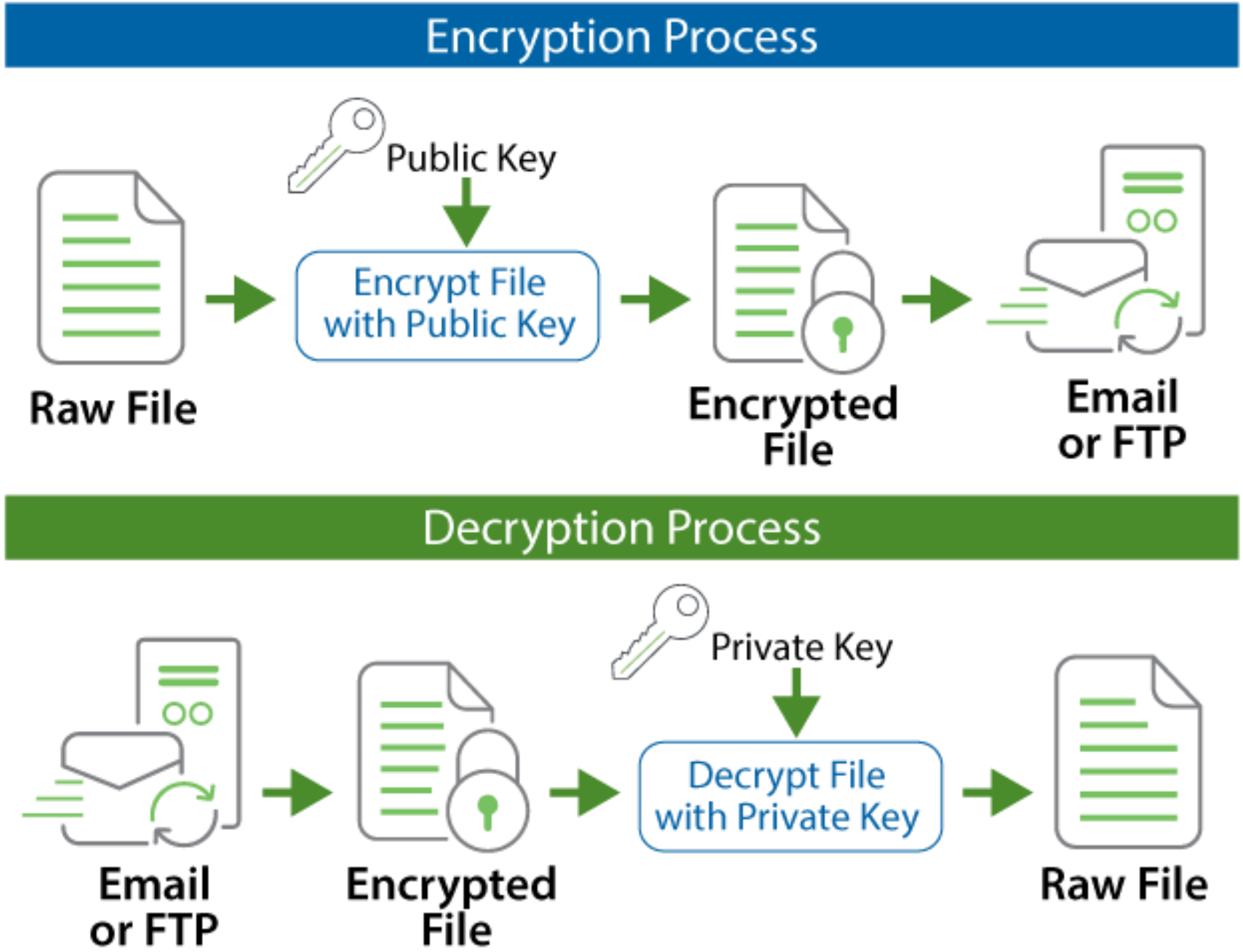


Σχήμα 4.2. Συμμετρικό μοντέλο κρυπτογραφικής επικοινωνίας

Mallory - Sniff



P.K.I.


Encryption Process
Public Key
Encrypt File with Public Key
Raw File
Encrypted File
Email or FTP
Decryption Process
Private Key
Decrypt File with Private Key
Email or FTP
Encrypted File
Raw File

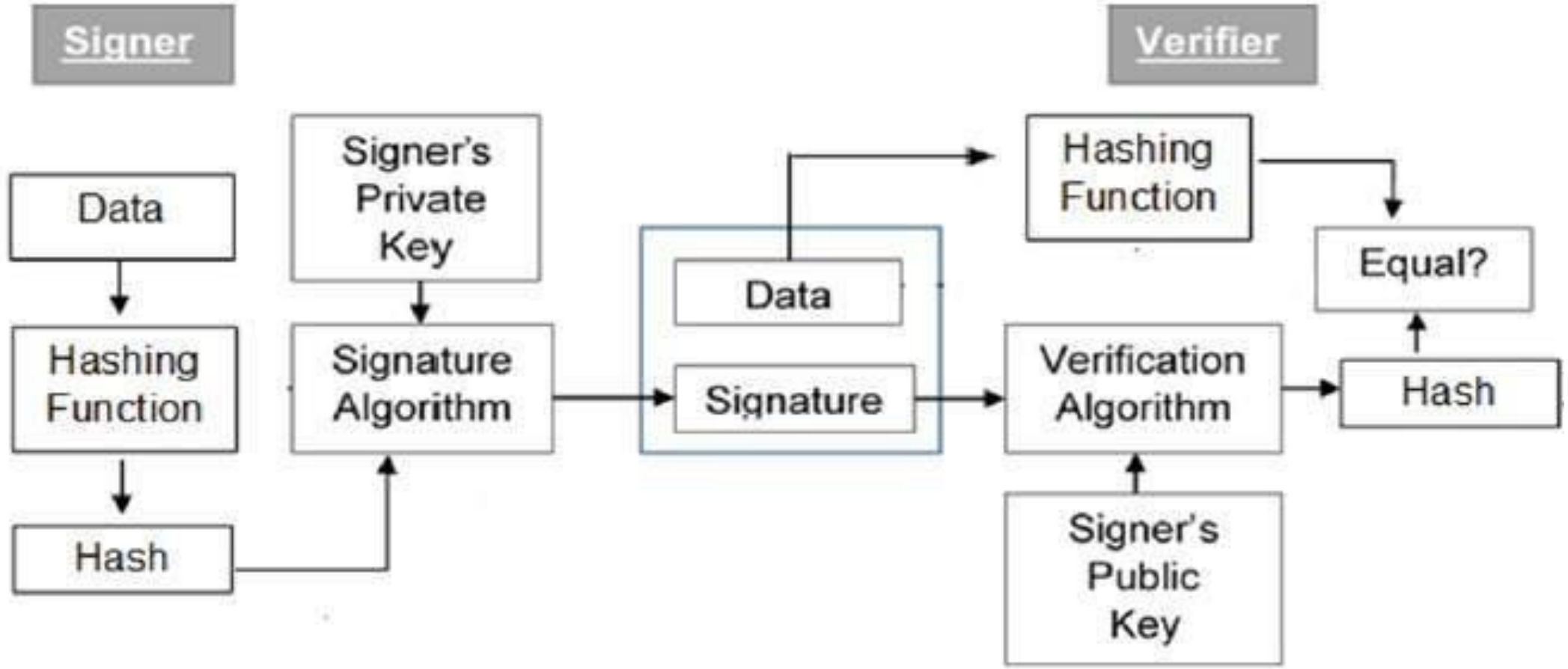
Hash - Fingerprint

```
lucidbeta@lucidbeta-desktop:~$ cd Desktop
lucidbeta@lucidbeta-desktop:~/Desktop$ ls
Imager Lite 2.9.0.zip
lucidbeta@lucidbeta-desktop:~/Desktop$ md5sum "Imager Lite 2.9.0.zip"
b1ace199216000f350ad46de02965230  Imager Lite 2.9.0.zip
lucidbeta@lucidbeta-desktop:~/Desktop$
```

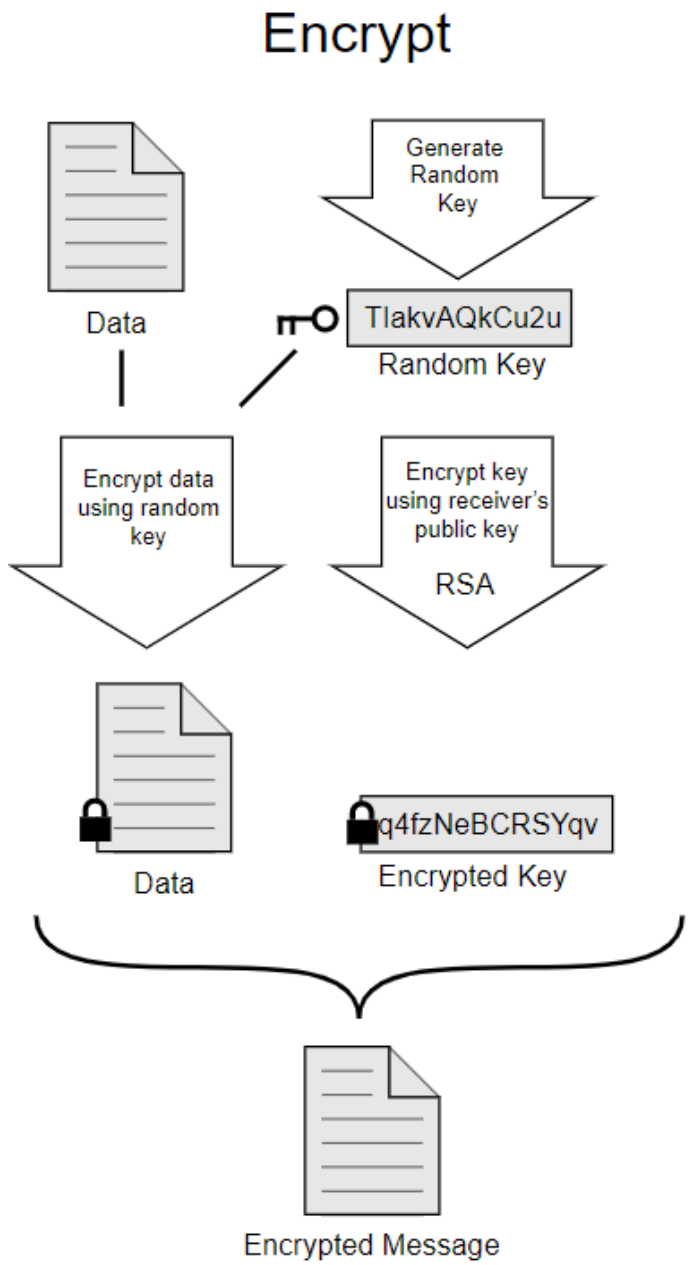
=

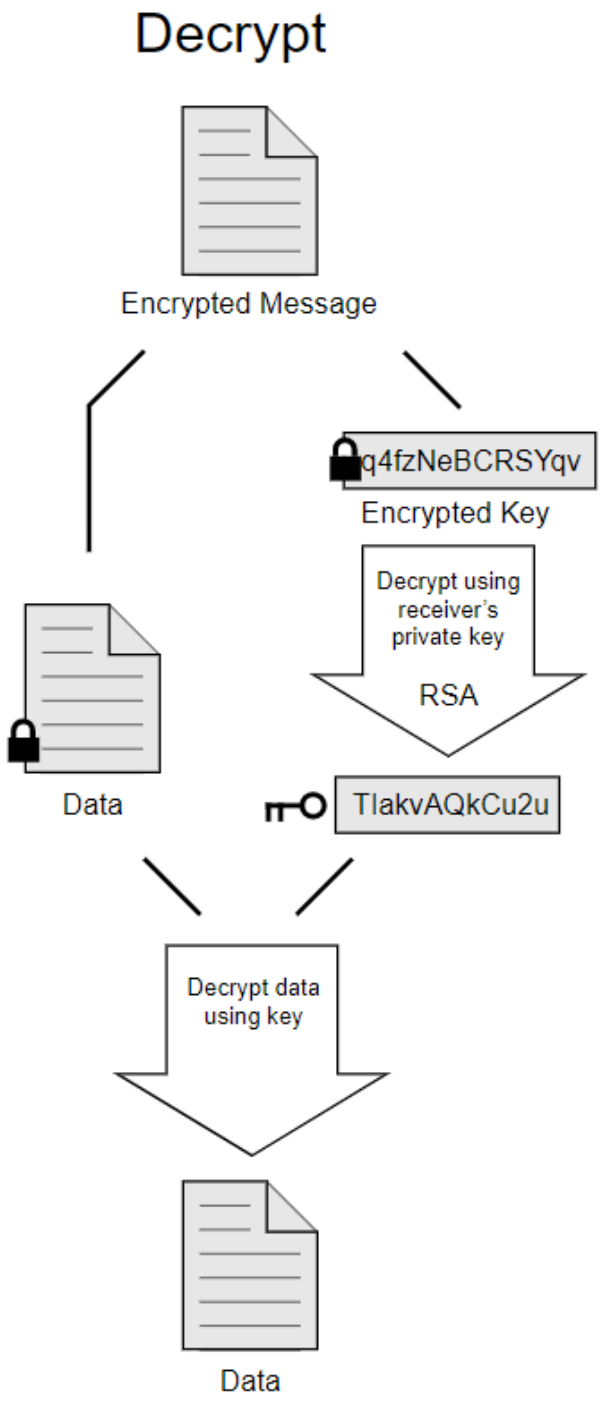
79054025
255fb1a2
6e4bc422
aef54eb4

Data + Signature



Enc - Dec

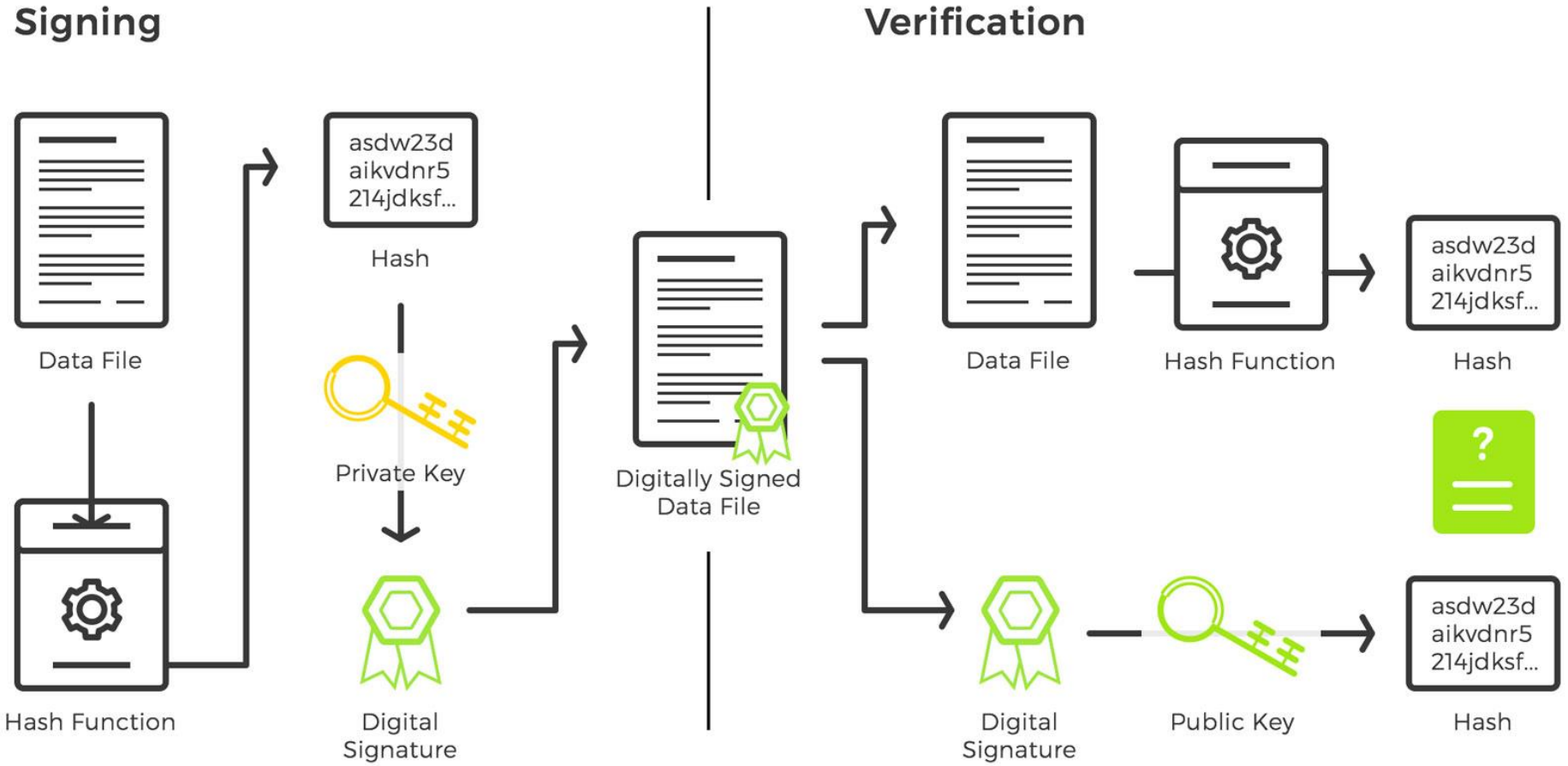

Encrypt
Data
Generate Random Key
TlakvAQkCu2u
Random Key
Encrypt data using random key
Encrypt key using receiver's public key
RSA
Data
q4fzNeBCRSYqv
Encrypted Key
Encrypted Message


Decrypt
Encrypted Message
q4fzNeBCRSYqv
Encrypted Key
Decrypt using receiver's private key
RSA
Data
TlakvAQkCu2u
Decrypt data using key
Data

Digital Sign

mmon Public Key

Digital Signature



PGP

- Το λογισμικό **Pretty Good Privacy (PGP),** το οποίο σχεδιάστηκε από τον Phill Zimmerman, είναι ένα *λογισμικό κρυπτογράφησης υψηλής ασφάλειας* για λειτουργικά συστήματα όπως τα MS DOS, Unix, VAX/VMS και για άλλες πλατφόρμες.

- Το PGP επιτρέπει την ανταλλαγή αρχείων και μηνυμάτων διασφαλίζοντας το απόρρητο και την ταυτότητα σε συνδυασμό με την ευκολία λειτουργίας.

- *Διασφάλιση του απορρήτου* σημαίνει ότι μόνο αυτός για τον οποίο προορίζεται ένα μήνυμα είναι ικανός και να το διαβάσει.

- *Πιστοποίηση της ταυτότητας* σημαίνει ότι μηνύματα που φαίνεται πως έχουν προέλθει από κάποιο άτομο μπορούν να έχουν προέλθει μόνο από αυτό το άτομο.

Key Id.

GPG key ID: 4AEE18F83AFDEB23

- Το key id χρησιμοποιείται από τον παραλήπτη για την ανεύρεση του δημόσιου κλειδιού του αποστολέα έτσι ώστε να ελέγξει την ψηφιακή υπογραφή.
- Ο παραλήπτης αναζητεί αυτόματα το δημόσιο κλειδί του αποστολέα και το user id του στο μπρελόκ δημοσίων κλειδιών που έχει στην κατοχή του.
- Ο παραλήπτης χρησιμοποιεί αυτό το key id για την ανεύρεση του μυστικού κλειδιού που απαιτείται για την αποκρυπτογράφηση του μηνύματος.
- Και στη συνεχεια αναζητεί αυτόματα το απαραίτητο μυστικό κλειδί αποκρυπτογράφησης στο μπρελόκ μυστικών κλειδιών του.

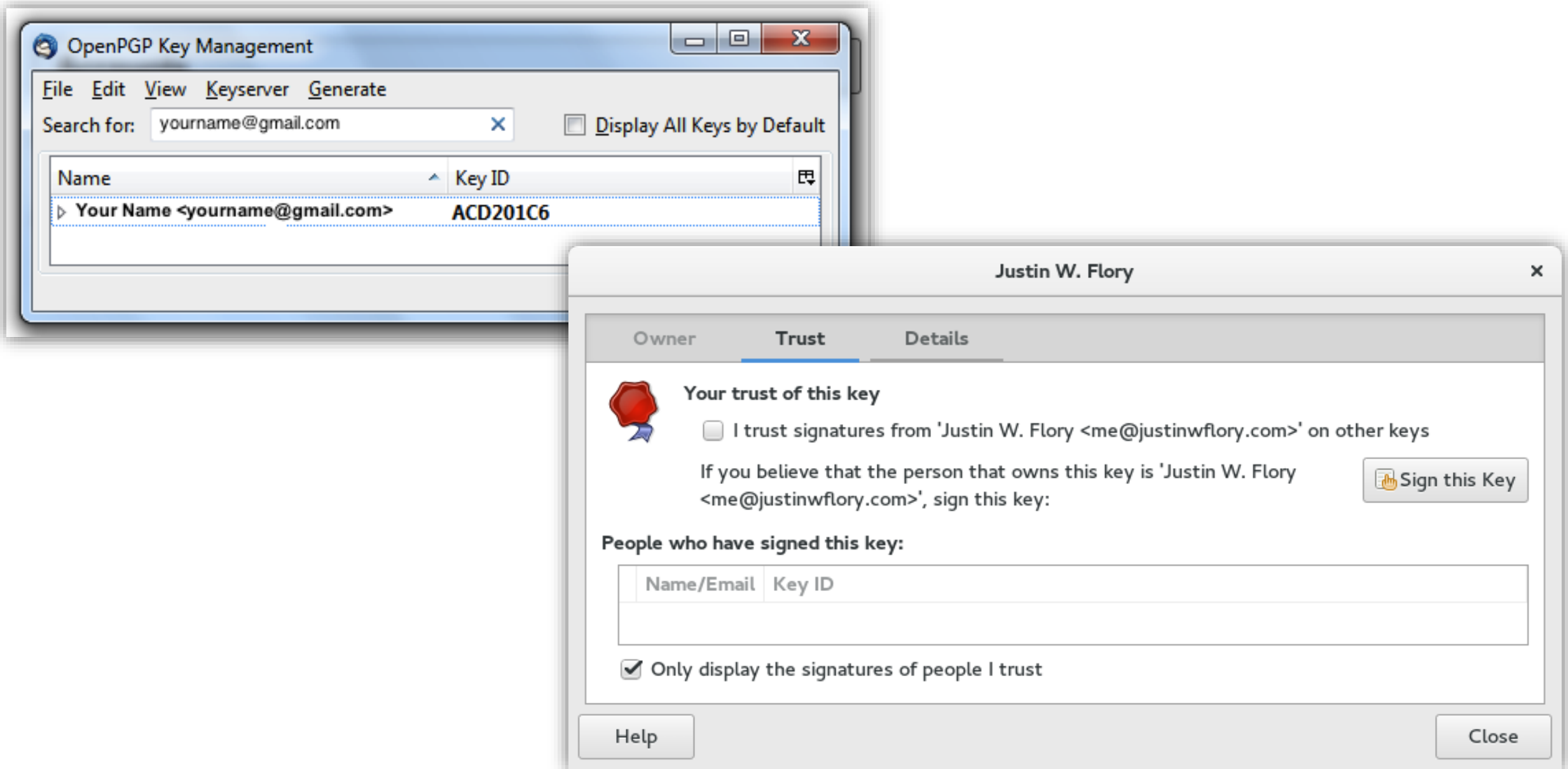
Trust

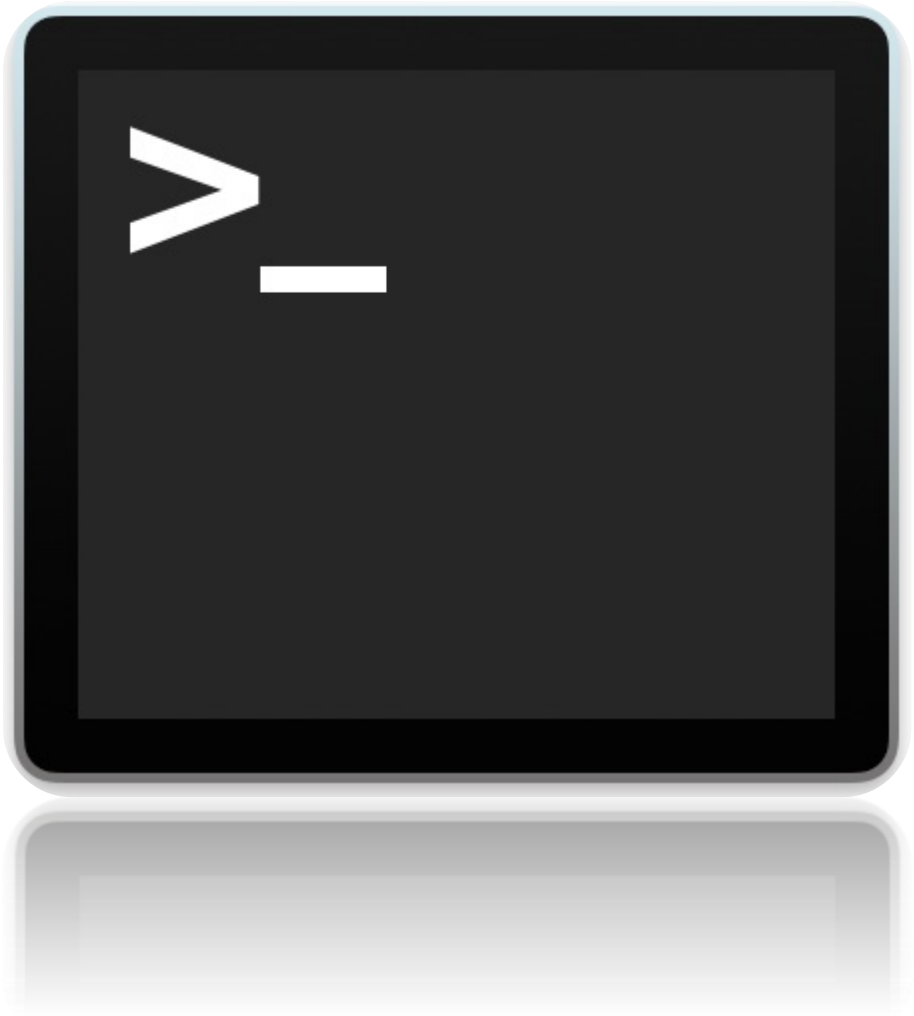
- Σε ένα κρυπτοσύστημα δημοσίων κλειδιών δεν υπάρχει ανάγκη προστασίας των δημοσίων κλειδιών Το σημαντικό και αυτό που θα πρέπει να διασφαλίζεται είναι το να είμαστε σίγουροι ότι κάποιο δημόσιο κλειδί που φαίνεται ότι ανήκει σε κάποιον, όντως να ανήκει σε αυτόν.
- Αυτό μπορεί να είναι και το πιο σημαντικό μειονέκτημα του κρυπτοσυστήματος δημόσιων κλειδιών.
- Μία διέξοδος σε αυτό το πρόβλημα είναι η χρήση κάποιου τρίτου κοινά αποδεκτού «φίλου» ο οποίος έχει στη κατοχή του ένα καλό αντίγραφο του δημόσιου κλειδιού του παραλήπτη. Αυτό το κοινά αποδεκτό άτομο θα μπορούσε να είναι κάποιος "key server".

Private Keys – Alert!

- Η προστασία του μυστικού κλειδιού είναι κάτι το αυτονόητο στο οποίο πρέπει να δοθεί μεγάλη προσοχή.
- Εάν ποτέ το μυστικό κλειδί πέσει σε λάθος χέρια τα οποία είναι οποιαδήποτε άλλα εκτός των δικών μας τότε θα πρέπει άμεσα, τόσο για τη δική μας ασφάλεια όσο και των άλλων, να ειδοποιήσουμε τους πάντες για το γεγονός προτού κάποιος αρχίσει να υπογράφει με το "όνομά" μας.
- Θα πρέπει να γίνεται χρήση του μυστικού κλειδιού μόνο σε συστήματα στα οποία έχουμε φυσικό έλεγχο. Επιπρόσθετα, πρέπει να προσέξουμε πού αποθηκεύουμε τη μυστική φράση-κλειδί.
- Δεν πρέπει ποτέ αυτή να βρίσκεται στον ίδιο υπολογιστή με αυτόν που έχει το αρχείο του μυστικού κλειδιού μας.

Software Tools





Terminal
Command Line Interface (CLI)
Cmd (Windows-Ms Dos)