**Χρήσιμα Βήματα**

Διαβάζω τα εξής links:

SeedLink:

* http://ds.iris.edu/ds/nodes/dmc/services/seedlink/ (initial release by IRIS)
* https://www.seiscomp.de/doc/apps/seedlink.html (supported by GFZ)

Seiscomp:

* https://www.seiscomp.de/doc/

Python library:

* https://docs.obspy.org/packages/obspy.clients.seedlink.html?highlight=seedlink#module-obspy.clients.seedlink
* https://docs.obspy.org/tutorial/code\_snippets/easyseedlink.html

Gisola:

* https://eida.gein.noa.gr/ (real-time)
* https://github.com/nikosT/Gisola (code)

EIDA federation:

* http://www.orfeus-eu.org/data/eida/
* https://eida.gein.noa.gr/ (EAA -NOA- κόμβος)

Σελίδα του Γεωδυναμικού Ινστιτούτου του Ε.Α.Α. να πάρεις μια ιδέα:

* https://bbnet.gein.noa.gr/HL/
* https://bbnet2.gein.noa.gr/husn\_network/index\_en.html (map)

**Ασκήσεις/Βήματα:**

1. Κατεβάζεις σεισμολογικά δεδομένα σε mseed format

(http://ds.iris.edu/ds/nodes/dmc/data/formats/miniseed/) π.χ. μιας

ημέρας από το ΕΑΑ μέσω του webservice, και χρησιμοποιώντας το builder

<https://eida.gein.noa.gr/fdsnws/dataselect/1/builder.>

Διάλεξε net:HL, sta:ATH, loc:κενό, cha:HH?

2. Τσεκάρεις ότι είναι αυτό που κατέβηκε με Python read('filepath'),

plot():

https://docs.obspy.org/packages/autogen/obspy.core.stream.read.html

3. Σηκώνεις Seedlink Server

4. Με τη λειτουργία "playback" ανατροφοδοτείς το seedlink με το mseed

και φαίνεται πως ο server δίνει realtime αυτά τα παλιά δεδομένα.

5. Διαπιστώνεις ότι ισχύει, τρέχοντας Seedlink Client (π.χ. slinktool

ή python seedlink lib -δες πιο πάνω-)

Τα δύσκολα είναι τα 3 και 4. Μπορείς να κατεβάσεις τον κώδικα του

seiscomp για κάποια διανομή Linux, δεν προτείνω compile από την αρχή),

από εδώ: https://www.seiscomp.de/downloader/

Μπορείς να δοκιμάσεις και έτοιμες υλοποιήσεις dockerized (googlare το). Είχα φτιάξει κι εγώ μία που επικεντρώνεται στο να σηκώνει archival

modules (FDSN station και dataselect). Εσένα σε ενδιαφέρει μόνο το Seedlink module, αλλά μπορείς να πάρεις μια ιδέα, βλ.

<https://github.com/nikosT/Gisola/tree/main/tools/seiscomp>

**Περιγραφή Διπλωματικής**

**Τίτλος:** Ενσωμάτωση μηχανισμού κρυπτογράφησης στο πρωτόκολλο επικοινωνίας SeedLink

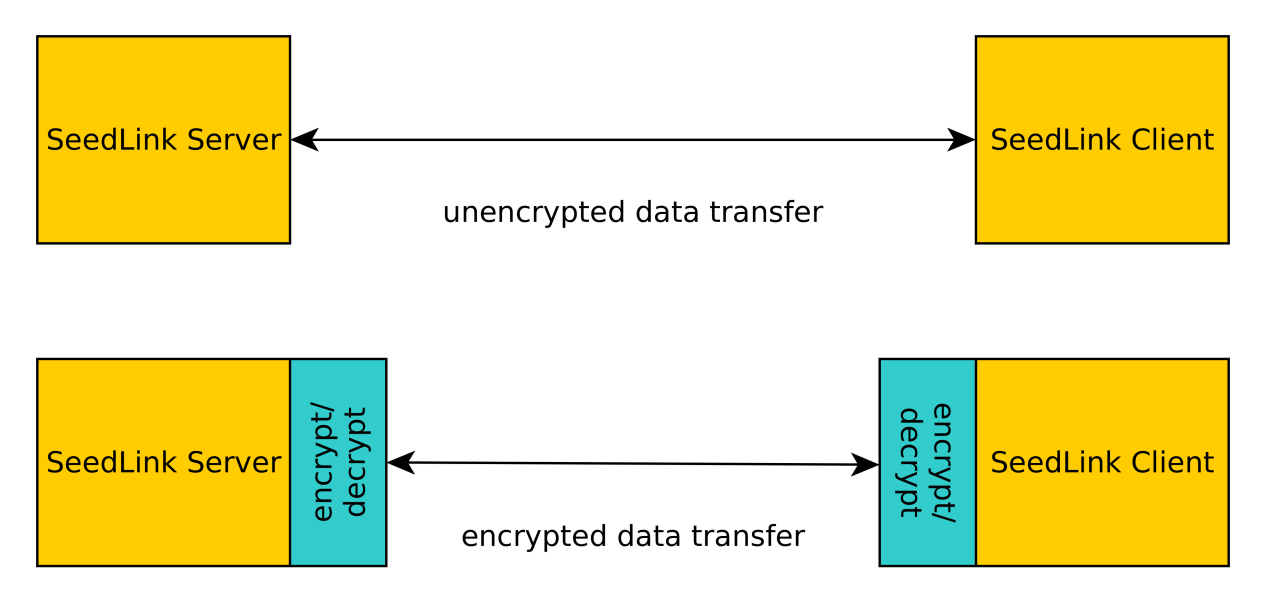
To SeedLink [1][2] αποτελεί ένα καθολικό πρωτόκολλο επικοινωνίας μεταξύ σεισμολογικών σταθμών και συστημάτων αποθήκευσης/επεξεργασίας σεισμικών δεδομένων σε πραγματικό χρόνο. Χρησιμοποιείται από όλα τα σεισμολογικά ινστιτούτα/εργαστήρια παγκοσμίως για τη συλλογή των σεισμολογικών δεδομένων από τους διάφορους σεισμολογικούς σταθμούς και δίκτυα σε πραγματικό χρόνο. Ωστόσο, αυτή τη στιγμή η μεταφορά των δεδομένων πραγματοποιείται χωρίς κρυπτογράφηση με κίνδυνο να εφαρμόσει κάποιος τεχνικές κυβερνοεπίθεσης (π.χ. man-in-the-middle [3]) και να υποκλέψει σεισμολογικά δεδομένα ή ακόμα χειρότερα να αλλοιώσει το περιεχόμενό τους δημιουργώντας ψεύτικες/λανθασμένες ειδοποιήσεις της αντίστοιχης Γενικής Γραμματείας Πολιτικής Προστασίας εκάστου κράτους. Σκοπός της διπλωματικής είναι η ενσωμάτωση κατάλληλου κρυπτογραφικού μηχανισμού στο πρωτόκολλο επικοινωνίας SeedLink έτσι ώστε η μετάδοση των δεδομένων να είναι κρυπτογραφημένη και ασφαλής

(βλ. επισύναψη -η τρέχουσα κατάσταση και η προτεινόμενη-).

[1] https://www.seiscomp.de/doc/apps/seedlink.html?highlight=seedlink

[2] https://ds.iris.edu/ds/nodes/dmc/services/seedlink/

[3] https://en.wikipedia.org/wiki/Man-in-the-middle\_attack



Σπάσιμο διπλωματικής σε βήματα:

1. Στήσιμο και απλά connect/read των ΜΠΛΕ μεταξύ τους (το SeedLink Client δεν είναι τίποτα άλλο παρά connect και read σε ένα υπάρχον SeedLink Server).

Προτείνω, χρήση ObsPy (links στο προηγούμενο email).

2. Το ΠΟΡΤΟΚΑΛΙ είναι το ίδιο με το ΜΠΛΕ σε θέμα στησίματος.

3. Στήσιμο και εφαρμογή των ΠΡΑΣΙΝΩΝ. Αυτό το βήμα είναι εντελώς αυτοτελές. Δεν χρειάζεται καν σεισμολογικά δεδομένα. Φτιάξε server/client (e.g. Python)

και στείλε/λάβε enc/decrypted data.

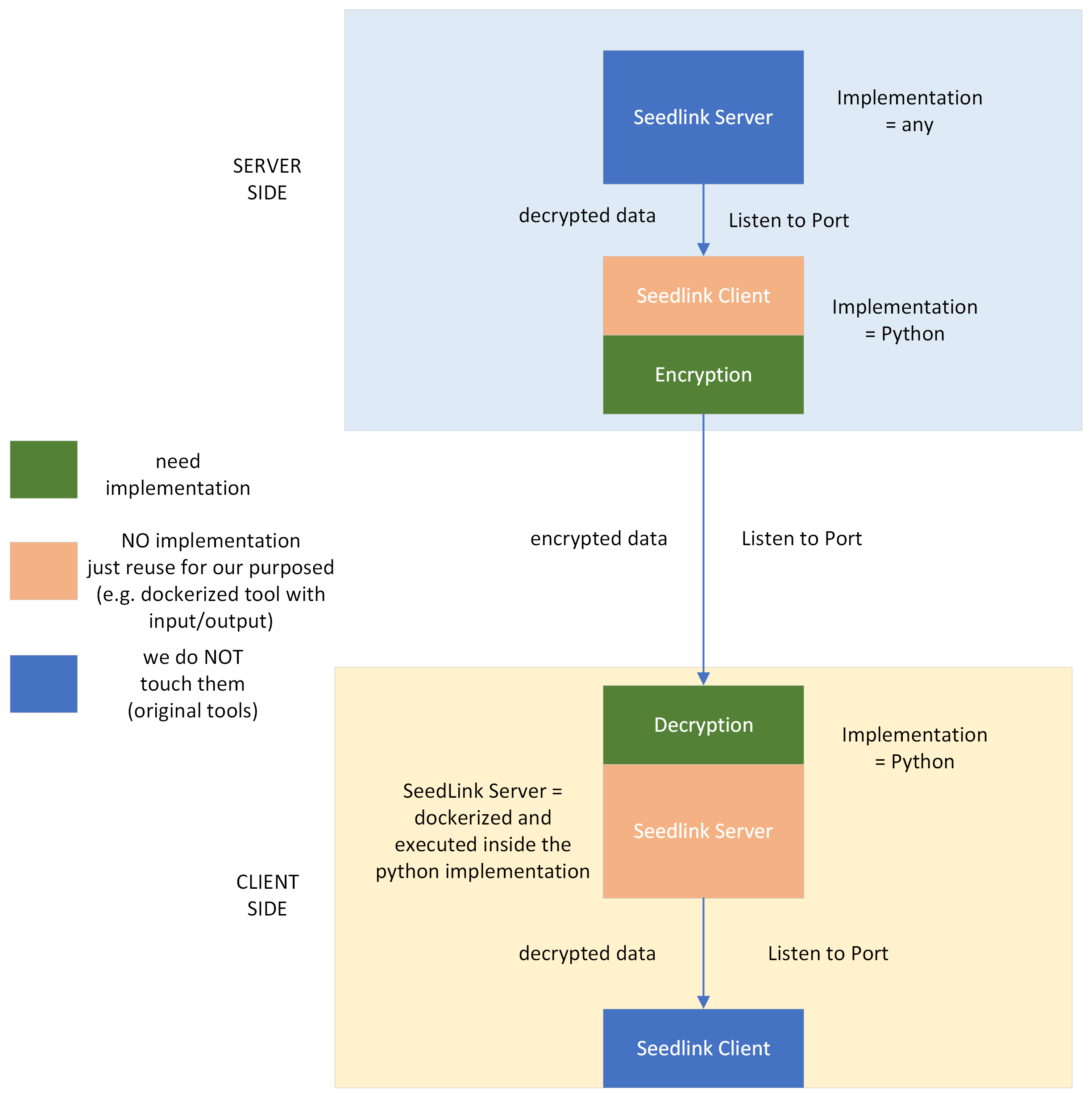
4. Κουμπώνεις τα ΠΟΡΤΟΚΑΛΙ στα ΠΡΑΣΙΝΑ (μπορείς τα πορτοκαλί να τα έχεις και dockerized - μπορεί να έχει και το github dockerized seedlink server).

5. Το ενώνεις σε πραγματικό σύστημα (ΜΠΛΕ). Το πραγματικό για σένα σε αυτή τη φάση είναι και πάλι εικονικό (άρα μοιάζει με το ΠΟΡΤΟΚΑΛΙ). Θεωρητικά όμως,

θα μπορεί να στηθεί σε πραγματικό σύστημα σε ινστιτούτο.

ΥΓ: Το SeedLink Client δεν είναι τίποτα άλλο παρά έτοιμες Python κλήσεις μέσω τις ObsPy.

ΥΓ: Για μένα τα δύσκολα που θα συναντήσεις είναι το setup SeedLink Server (και ενσωμάτωση σε docker) και μετά τα ΠΡΑΣΙΝΑ



**Seedlink Server Deployment**

Github Repository: <https://github.com/nikosT/seedlink-with-slarchive-docker/blob/main/README.md>

**Slarchive**

* *slarchive\seiscomp\var\lib\slarchive\****purge\_datafiles****:* Ουσιαστικά, είναι ένα script συντήρησης των σεισμικών δεδομένων που αποθηκεύονται στον τοπικό server. Κάνει iterate στα αρχεία που εντοπίζονται στο path CFGDIR (που ορίζεται μέσα στο script), εξάγει πληροφορίες - όπως είναι ο σταθμός - κλπ και στη συνέχεια προχωρά στη διαγραφή παλαιών αρχείων από το φάκελο archive (σύμφωνα με τις παραμέτρους NET, STATION …)
* *slarchive\seiscomp3\****slarchive.cfg****:* Είναι ένα configuration file που χρησιμοποιείται για να ορίσει πως θα συμπεριφέρεται ο server, ποια δεδομένα πρέπει να συλλέγει, που πρέπει αυτά να αποθηκεύονται και άλλες ρυθμίσεις που σχετίζονται με τη λειτουργία του
* *slarchive\****wait-for-it.sh****:* ελέγχει αν η σύνδεση TCP host/port είναι διαθέσιμη

**Seedlink**

* *seedlink\****ring.conf****:* Ορίζει το φάκελο που το πρωτόκολλο seedlink θα αποθηκεύσει τα δεδομένα του ring buffer

**Ring buffer**: είναι μια προσωρινή τοποθεσία αποθήκευσης των σεισμικών δεδομένων (γράφεται και αντικαθίσταται συνεχώς με κυκλικό τρόπο)

* seedlink\Makefile: Αυτοματοποιεί τις διαδικασίες compilation και build. Περιέχει ένα σύνολο κανόνων και εξαρτήσεων που καθορίζουν τον τρόπο με τον οποίο θα πρέπει να μεταγλωττίζονται και να συνδέονται τα αρχεία πηγαίου κώδικα για τη δημιουργία εκτελέσιμων προγραμμάτων ή άλλων αρχείων προορισμού

**Technologies used:**

* Docker
* Seiscomp
* Obspy
* Python
* Seedlink protocol (miniseed - .mseed files)
* Slarchive (google search: slarchive seedlink github)

link: <https://www.seiscomp.de/doc/apps/slarchive.html>

**Cubersecurity attacks**

* Man-in-the-middle attack (MiTM)
* Denial-of-Service attack (DoS attack)

**Bibliography**

* **[D](https://nemertes.library.upatras.gr/server/api/core/bitstreams/8d6d2f3a-d9b8-46e6-afa3-ccf4b67fb463/content?fbclid=IwAR3hRcGQ44EO4M6mmAfEfX6qfbuXAWAImAcYHRlezCamkkGaGiTW1eYiYz4)oS attack ταξινόμηση**

(

https://nemertes.library.upatras.gr/server/api/core/bitstreams/8d6d2f3a-d9b8-46e6-afa3-ccf4b67fb463/content?fbclid=IwAR3hRcGQ44EO4M6mmAfEfX6qfbuXAWAImAcYHRlezCamkkGaGiTW1eYiYz4,

-----------------------------------------------------------------------------------------------------------------

https://nemertes.library.upatras.gr/server/api/core/bitstreams/19e9e666-4e4d-4750-927f-1ca5a2e31f31/content?fbclid=IwAR1IsQRC8ckoxG7EfEZroYd8lQUg\_kcvHTB4NNGd8DxkhfqXQ239Oi0C1Nw,

-----------------------------------------------------------------------------------------------------------------

https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection/understanding-denial-of-service-attacks?fbclid=IwAR0sn10K9tTcV2y6T5qTSRNgta\_t644F6mHyDKElsFzV5r7aOWnTqOtSL0A

)

* **MiTM attack**

(

https://nemertes.library.upatras.gr/server/api/core/bitstreams/4d0b0ef2-25d2-4f33-83ad-b0bed7d13514/content?fbclid=IwAR11J9mjoBdMM-uIo\_15OlrVKCrRO6fGfcMLHjZi4L\_QHCExG0pPJnO4B1M

)

* https://nemertes.library.upatras.gr/server/api/core/bitstreams/19e9e666-4e4d-4750-927f-1ca5a2e31f31/content?fbclid=IwAR27MAXTAtP\_OIC66u-tfXMSvdJIdHrpH1ce8JVUaHPC5fyBlgFh9iIdEZs
* **Cryptography**

(

https://nemertes.library.upatras.gr/server/api/core/bitstreams/b8e193f7-0ca3-4432-a858-734b9555d877/content?fbclid=IwAR0ulEojGOQWHn37sT\_3gl1m8lPVBa9A75shyiHOM\_AxrZ1y0g1PYI4ADN0,

-----------------------------------------------------------------------------------------------------------------

https://www.fortinet.com/resources/cyberglossary/what-is-cryptography?fbclid=IwAR0lzeOofbKI0yxG8tUJrzB86KYjmYe2VEPLQOMqRwjiV91Af5PkhvNU6x4

)

* **AES Algorithm**

(

https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption?fbclid=IwAR2JMaP8DIchZI7zFTTPX7-FgvZp5kDerFfQGprSgFXPSdZDIyhR05uHEvU

)