ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

ΓΙΑΤΙ ΕΙΝΑΙ ΧΡΗΣΙΜΗ Η ΚΡΥΠΤΟΓΡΑΦΙΑ;

Η Αναγκαιότητα της Κρυπτογραφίας

- Η κρυπτογραφία είναι το απαραίτητο εργαλείο για την προστασία ευαίσθητων πληροφοριών σε υπολογιστικά συστήματα.
- Χρησιμοποιείται καθημερινά από πάρα πολλούς χρήστες.
- Υλοποιείται σε πρωτόκολλα όπως το SSL/TLS, το οποίο εξασφαλίζει ασφαλείς ηλεκτρονικές συναλλαγές και κρυπτογραφεί την επικοινωνία (π.χ. στη μηχανή αναζήτησης της Google).
- Εδώ παρουσιάζουμε τη βασική κρυπτογραφία, συμμετρική και δημόσιου κλειδιού.

Εισαγωγή: Τα Πρώτα Συστήματα

- Συμμετρικά Συστήματα: Τα πρώτα συστήματα χρησιμοποιούσαν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση.
- **Παραδείγματα: α. AES** (Advanced Encryption Standard): Σύγχρονο συμμετρικό σύστημα, χρησιμοποιείται στο πρωτόκολλο SSL/TLS.

β. Σύστημα του Καίσαρα: Ένα από τα πιο απλοϊκά, κάθε γράμμα αντικαθίσταται από το τρίτο διαδοχικό γράμμα (σύστημα μετατόπισης).

- Βασική Παραδοχή: Ο εχθρός γνωρίζει πώς δουλεύει το σύστημα, αλλά δεν γνωρίζει το μυστικό κλειδί.

Το Πρόβλημα της Ανταλλαγής Κλειδιών

- Προ-Diffie-Hellman Εποχή (π.D-H): Όλα τα κρυπτοσυστήματα βασίζονταν στην παραδοχή ότι η ανταλλαγή κλειδιών γίνεται με ασφαλή τρόπο.Αυτό δεν ήταν πρακτικό, καθώς απαιτούσε κόστος και καθυστέρηση στον διαμερισμό του κλειδιού.
- Κρυπτοσυστήματα Δημόσιου Κλειδιού (Public Key Cryptography): Ανακαλύφθηκαν από τους Whitfield Diffie και Martin Hellman (1976).
- Λειτουργία: Δημοσιοποιούμε ένα κλειδί σε μη ασφαλή δίαυλο, με τη βοήθεια του οποίου οι οντότητες υπολογίζουν ένα κοινό μυστικό κλειδί.

Οι Στόχοι της Κρυπτογραφίας

- **Εμπιστευτικότητα (Confidentiality):**

Συμμετρική Κρυπτογράφηση (Block Ciphers, Stream Ciphers).

Κρυπτογραφία Δημόσιου Κλειδιού, Υβριδικά Κρυπτοσυστήματα, Ανταλλαγή Κλειδιού.

- **Αυθεντικοποίηση (Authentication):Ψηφιακή Υπογραφή.**

Συστήματα Ταυτοποίησης.

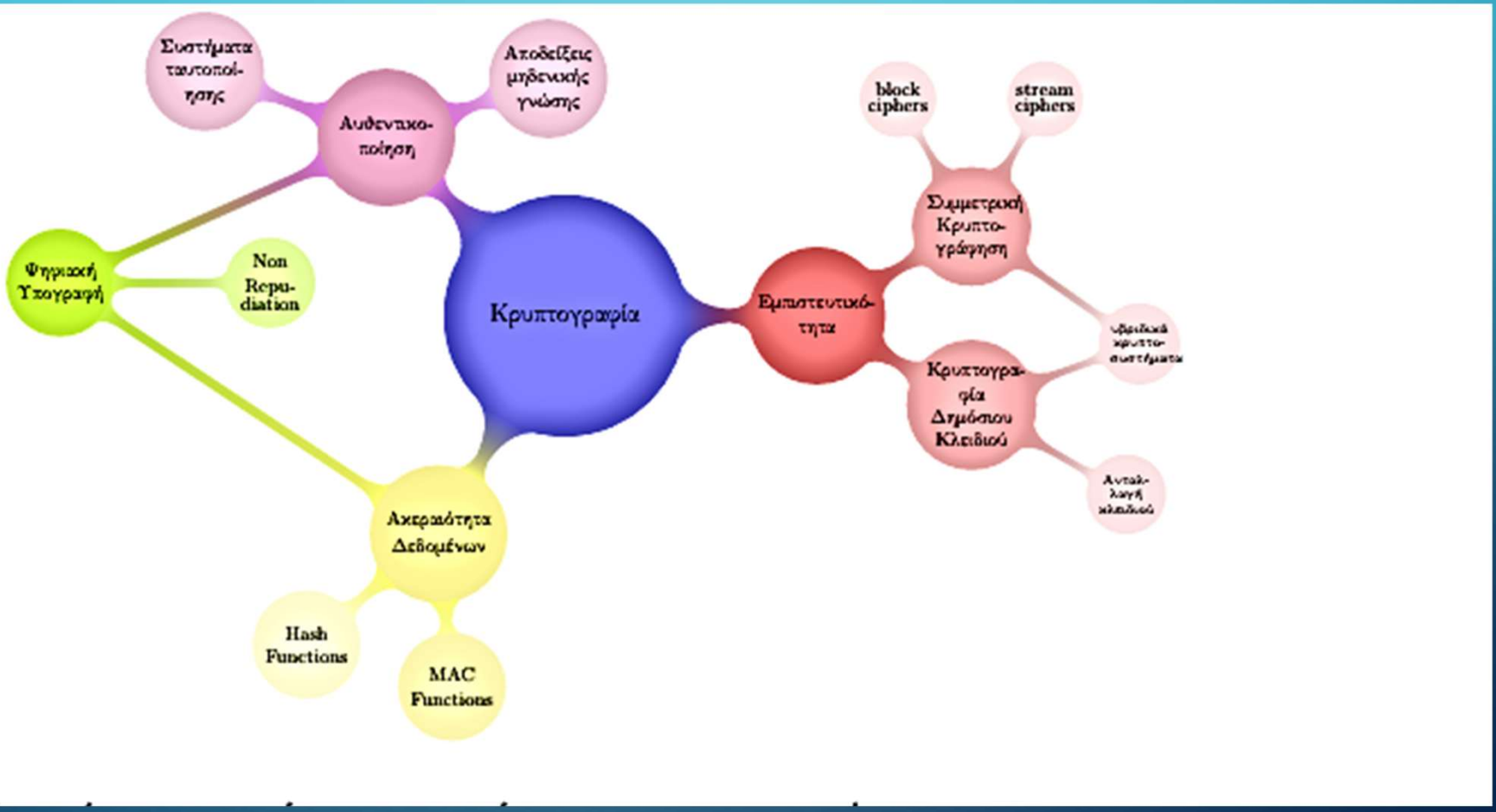
Non-Repudiation (Μη Αποκήρυξη).

- **Ακεραιότητα Δεδομένων (Data Integrity):**

MAC Functions (Κώδικες Αυθεντικοποίησης Μηνύματος).

Hash Functions (Συναρτήσεις Κατακερματισμού).

Οι Στόχοι της Κρυπτογραφίας



Μερικές Πρακτικές Εφαρμογές

Η κρυπτογραφία χρησιμοποιείται για την απόκρυψη ενός μηνύματος, αλλά και για:

- Κατασκευή ψηφιακών νομισμάτων (π.χ. Bitcoin).
- Ψηφιακή υπογραφή αρχείων.
- Εξασφάλιση ανωνυμίας στο διαδίκτυο.
- Ηλεκτρονική ψηφοφορία.

Εφαρμογή: SSL/TLS

- **SSL/TLS (Secure Sockets Layer/Transport Layer Security):** Το βασικό πρωτόκολλο κρυπτογράφησης και αυθεντικοποίησης στο διαδίκτυο.
- **Λειτουργία:** Όταν ενεργοποιείται, οι σελίδες από http γίνονται https (όπου s = secure).
- **Σημασία:** Στηρίζει την ασφάλεια όλων των συναλλαγών (ηλεκτρονικό εμπόριο, τράπεζες, δημόσιο) όπου απαιτείται εισαγωγή μυστικού κωδικού.
- **Εμπιστοσύνη:** Εμπιστευόμαστε το πρωτόκολλο, εφόσον χρησιμοποιούνται κατάλληλες πολιτικές ασφάλειας (σωστοί αλγόριθμοι, τακτικές αναβαθμίσεις, σωστά ψηφιακά πιστοποιητικά).

Εφαρμογές: Tor & PGP

Tor (The Onion Router):

- Αποκεντρωμένο σύστημα ανώνυμης πλοήγησης στο διαδίκτυο.
- Εξασφαλίζει ανωνυμία από παρακολούθηση της κίνησης του δικτύου.

PGP (Pretty Good Privacy):

- Χρησιμοποιείται για την κρυπτογράφηση και την ψηφιακή υπογραφή των email.
- Υλοποιείται στο πρόγραμμα ανοιχτού κώδικα GNU PG (GPG).
- Θεωρείται ασφαλές, εφόσον χρησιμοποιηθεί σωστά.

Εφαρμογή: Ομομορφικά Κρυπτοσυστήματα

- **Ορισμός:** Συστήματα που επιτρέπουν υπολογισμούς πάνω στα κρυπτογραφημένα δεδομένα.
- **Εφαρμογές:** Κυρίως σε υποδομές νέφους (cloud infrastructures).
- **Τεχνολογία:** Το πρώτο ομομορφικό σύστημα (Craig Gentry) κάνει χρήση των πλεγμάτων (lattices).
- **Σκοπός:** Υποψήφια για την κρυπτογραφία μετά τους κβαντικούς υπολογιστές (Post Quantum Cryptography).

Εφαρμογή: Μετα-κβαντική Κρυπτογραφία

- **Ορισμός:** Κρυπτογραφία μετά την εμφάνιση των κβαντικών υπολογιστών, όπου τα RSA και Diffie-Hellman δεν θα είναι πλέον ασφαλή.
- **Νέο Πρότυπο από διαγωνισμό του National Institute of Standards and Technology (NIST):** Το σύστημα Crystals - Kyber έχει επιλεγεί ως το νέο πρότυπο κρυπτογράφησης δημόσιου κλειδιού.
- **Βάση:** Βασίζεται στη θεωρία πλεγμάτων και αντιστέκεται σε γνωστές κβαντικές επιθέσεις (ακόμα!).
- **Σύσταση:** Συνιστάται η μετάβαση σε αυτά τα νέα συστήματα, ως προετοιμασία για την έλευση ισχυρών κβαντικών υπολογιστών.

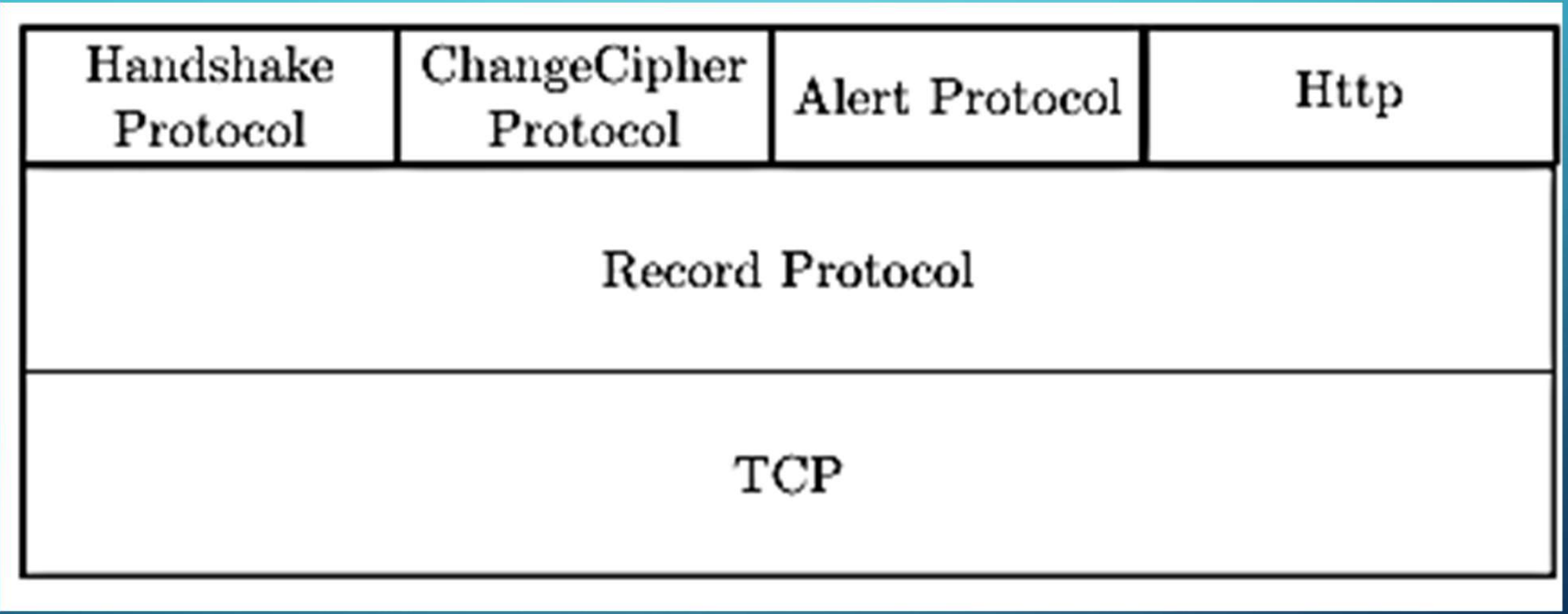
Κλασική Κρυπτογραφία

Μηχανή Enigma (Σύμβολο των κλασικών συστημάτων αντικατάστασης/μετάθεσης)

Πηγή: Δραζιώτης, Κ. (2021). Εισαγωγή στην Κρυπτογραφία [Προπτυχιακό εγχειρίδιο]. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις. http://dx.doi.org/10.57713/kallipos-17

Σύγχρονη Κρυπτογραφία και Εφαρμογές

Δομή πρωτοκόλλου TLS (Το βασικό πρωτόκολλο ασφάλειας στο διαδίκτυο).



Πηγή: Δραζιώτης, Κ. (2021). Εισαγωγή στην Κρυπτογραφία [Προπτυχιακό εγχειρίδιο]. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις. http://dx.doi.org/10.57713/kallipos-17

ΕΡΩΤΗΣΕΙΣ ΓΙΑ ΣΥΖΗΤΗΣΗ

1. Οι Στόχοι της Κρυπτογραφίας: Η θεωρία αναφέρει ότι η κρυπτογραφία, εκτός από την Εμπιστευτικότητα (απόκρυψη του μηνύματος), εξυπηρετεί και τους στόχους της Αυθεντικοποίησης και της Ακεραιότητας Δεδομένων. Ποιος από αυτούς τους τρεις βασικούς στόχους θεωρείτε ότι είναι ο πιο κρίσιμος για την ασφάλεια των καθημερινών σας ηλεκτρονικών συναλλαγών (π.χ. e-banking, αγορές) και γιατί;

2. Ιδιωτικό έναντι Δημόσιου Κλειδιού: Πριν από την ανακάλυψη των κρυπτοσυστημάτων δημόσιου κλειδιού (όπως το Diffie-Hellman), η βασική, μη πρακτική, παραδοχή ήταν ότι η ανταλλαγή του μυστικού κλειδιού έπρεπε να γίνεται με ασφαλή τρόπο. Πώς ακριβώς έλυσε το πρόβλημα αυτό η έννοια του «δημόσιου κλειδιού» και γιατί η λύση αυτή θεωρείται επαναστατική για την εξέλιξη της ασφάλειας στο διαδίκτυο (π.χ. για πρωτόκολλα όπως το SSL/TLS);

ΕΡΩΤΗΣΕΙΣ ΓΙΑ ΣΥΖΗΤΗΣΗ

3. Εφαρμογές και Δεοντολογία: Το πρωτόκολλο SSL/TLS (https) κρυπτογραφεί την επικοινωνία σας με έναν διακομιστή (π.χ. τις αναζητήσεις σας στη Google), ενώ το Tor στοχεύει στην ανωνυμοποίηση των αιτημάτων σας, κρύβοντάς τα ακόμα και από την ίδια την Google. Ποια είναι η βασική διαφορά στη φιλοσοφία ασφάλειας μεταξύ των δύο; Σε ποιες περιπτώσεις η χρήση ενός πρωτοκόλλου ανωνυμοποίησης (όπως το Tor) μπορεί να θεωρηθεί απαραίτητη για τη δημοκρατία και την ελευθερία έκφρασης, και σε ποιες περιπτώσεις μπορεί να εγείρει ηθικά ζητήματα;

4. Το Μέλλον της Κρυπτογραφίας: Η θεωρία παρουσιάζει δύο σύγχρονες/μελλοντικές κατευθύνσεις: τη Μετα-Κβαντική Κρυπτογραφία (PQC) και τα Ομομορφικά Κρυπτοσυστήματα (που επιτρέπουν υπολογισμούς σε κρυπτογραφημένα δεδομένα). Ποιο από τα δύο θεωρείτε ότι θα έχει τον μεγαλύτερο αντίκτυπο στον τομέα της ασφάλειας δεδομένων την επόμενη δεκαετία και γιατί;