ΣΥΜΜΕΤΡΙΚΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ

ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΤΜΗΜΑΤΟΣ (BLOCK CIPHERS)

ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΡΟΗΣ (STREAM CIPHERS)

ΣΥΜΜΕΤΡΙΚΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ

- Στην παρουσίαση αυτή θα εξεταστούν οι βασικές αρχές και η αρχιτεκτονική των Συμμετρικών Κρυπτοσυστημάτων, εστιάζοντας στους αλγόριθμους Block Ciphers (DES, AES) και Stream Ciphers (LFSR, Κλειδοροές).
- Στόχος είναι η κατανόηση των μηχανισμών που διασφαλίζουν την υπολογιστική ασφάλεια και την αποδοτικότητα αυτών των συστημάτων.

ΣΥΜΜΕΤΡΙΚΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ: ΚΟΙΝΟ ΜΥΣΤΙΚΟ ΚΛΕΙΔΙ

Τα Συμμετρικά Κρυπτοσυστήματα (Symmetric Ciphers) είναι γνωστά και ως κρυπτοσυστήματα **μυστικού** ή **κοινού κλειδιού** (Secret/Shared Key Cryptography). Χρησιμοποιούν το **ίδιο μοναδικό κλειδί (K)** για την κρυπτογράφηση ($C = E_K(M)$) και για την αποκρυπτογράφηση ($M = D_K(C)$). Το κύριο Πλεονέκτημά τους είναι ότι είναι εξαιρετικά **γρήγορα** και **αποδοτικά** για τη μαζική κρυπτογράφηση μεγάλων όγκων δεδομένων (π.χ., κρυπτογράφηση αρχείων, VPN). Η θεμελιώδης πρόκληση παραμένει η ασφαλής **διανομή** του κοινού μυστικού κλειδιού μεταξύ των χρηστών.

ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΤΜΗΜΑΤΟΣ (BLOCK CIPHERS)- ΟΜΑΔΕΣ ΔΕΔΟΜΕΝΩΝ ΣΤΑΘΕΡΟΥ ΜΗΚΟΥΣ (BLOCKS)

Τα Block Ciphers κρυπτογραφούν το μήνυμα χωρισμένο σε **σταθερά, ανεξάρτητα τμήματα (blocks)** δεδομένων, συνήθως 64 bits (DES) ή 128 bits (AES). Ένα block απλού κειμένου (M_i) κρυπτογραφείται σε ένα block κρυπτοκειμένου (C_i) με χρήση του κλειδιού K. Ο σχεδιασμός τους βασίζεται σε ένα **επαναληπτικό δίκτυο** (με πολλούς γύρους) που συνδυάζει δύο θεμελιώδεις κρυπτογραφικές ιδιότητες, τη **Σύγχυση** και τη **Διάχυση**, για να διασφαλίσει την ασφάλεια έναντι κρυπτανάλυσης.

ΒΑΣΙΚΕΣ ΚΡΥΠΤΟΓΡΑΦΙΚΕΣ ΙΔΙΟΤΗΤΕΣ – ΣΥΓΧΥΣΗ (CONFUSION) ΚΑΙ ΔΙΑΧΥΣΗ (DIFFUSION)

1. Σύγχυση (Confusion): Στόχος είναι η σχέση μεταξύ του **κλειδιού** και του τελικού **κρυπτοκειμένου** να γίνει **όσο το δυνατόν πιο πολύπλοκη και μη γραμμική**. Αυτό αποτρέπει την εύκολη εξαγωγή του κλειδιού. Επιτυγχάνεται κυρίως μέσω **αντικαταστάσεων (Substitutions)**, όπως οι S-Boxes. **2. Διάχυση (Diffusion):** Στόχος είναι η επίδραση ενός μεμονωμένου bit του **απλού κειμένου** να διασκορπίζεται σε **όσο το δυνατόν περισσότερα bits** του κρυπτοκειμένου (φαινόμενο χιονοστιβάδας). Επιτυγχάνεται μέσω **μεταθέσεων (Permutations)** και πράξεων ανάμειξης, όπως το MixColumns στον AES.

ΔΙΚΤΥΑ FEISTEL (FEISTEL NETWORKS) - Η ΚΛΑΣΣΙΚΗ ΑΝΑΣΤΡΕΨΙΜΗ ΔΟΜΗ

Η δομή Feistel (που χρησιμοποιήθηκε στον **DES**) είναι ένας επαναληπτικός μηχανισμός που επιτρέπει την κατασκευή ενός **αναστρέψιμου** Block Cipher, ακόμα και αν η βασική συνάρτηση του γύρου (f) είναι μη αναστρέψιμη. Το block εισόδου χωρίζεται σε αριστερό (L) και δεξιό (R) μισό. Σε κάθε γύρο, L και R εναλλάσσονται, ενώ το R τροποποιείται με μια συνάρτηση f και XOR με το L. Η **αποκρυπτογράφηση** γίνεται χρησιμοποιώντας την **αντίστροφη σειρά των υποκλειδιών** στον ίδιο μηχανισμό.

DATA ENCRYPTION STANDARD (DES) – ΤΟ ΙΣΤΟΡΙΚΟ ΠΡΟΤΥΠΟ ΤΩΝ 56-BIT

Ο **DES** υπήρξε το ομοσπονδιακό πρότυπο κρυπτογράφησης των ΗΠΑ (1977-2001). Είναι ένα **Block Cipher 64-bit** που χρησιμοποιεί τη δομή **Feistel με 16 γύρους**. Το πραγματικό μήκος του κλειδιού είναι **56 bits**, γεγονός που αποτέλεσε την κύρια αδυναμία του. Λόγω του περιορισμένου μήκους κλειδιού, ο DES κατέστη ευάλωτος σε επιθέσεις **brute-force** με τη χρήση σύγχρονων υπολογιστικών πόρων, οδηγώντας στην αντικατάστασή του.

ΔΟΜΗ DES: ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΑΙ ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ - Η ΑΡΧΗ ΤΗΣ ΑΝΑΣΤΡΕΨΙΜΟΤΗΤΑΣ FEISTEL

Η κρυπτογράφηση DES περιλαμβάνει μια Αρχική Μετάθεση (IP), 16 γύρους Feistel και μια Τελική Αντίστροφη Μετάθεση (IP^{-1}). Το βασικό χαρακτηριστικό της δομής Feistel είναι ότι η **αποκρυπτογράφηση** είναι δομικά **πανομοιότυπη** με την κρυπτογράφηση. Δεν απαιτείται ξεχωριστή συνάρτηση. Αρκεί να εφαρμοστεί ακριβώς η ίδια διαδικασία, αλλά τα 16 **υποκλειδιά (K_i)** να χρησιμοποιηθούν με **αντίστροφη σειρά** (από K_{16} έως K_1).

Η ΚΡΙΣΙΜΗ ΣΥΝΑΡΤΗΣΗ F ΤΟΥ DES – Ο ΜΗΧΑΝΙΣΜΟΣ ΣΥΓΧΥΣΗΣ ΚΑΙ ΔΙΑΧΥΣΗΣ

Η συνάρτηση f είναι ο πυρήνας της κρυπτογραφικής ασφάλειας του DES. Λειτουργεί σε 32 bits δεδομένων (R_i) και 48 bits υποκλειδιού (K_i). Τα βασικά βήματα είναι:

1. **Επέκταση (E-Box):** Επέκταση 32 bits σε 48 bits.
2. **XOR:** Το αποτέλεσμα XORίζεται με το υποκλειδί K_i.
3. **S-Boxes (Substitution Boxes):** Ο μηχανισμός **σύγχυσης**. Μη γραμμική αντικατάσταση 6 bits σε 4 bits. Η **μη γραμμική** φύση των S-Boxes είναι κρίσιμη για την αντοχή του DES σε επιθέσεις διαφορικής και γραμμικής κρυπτανάλυσης.
4. **P-Box:** Μετάθεση 32-bit για **διάχυση**.

ΠΑΡΑΓΩΓΗ ΥΠΟΚΛΕΙΔΙΩΝ (KEY SCHEDULE) ΣΤΟ DES - ΔΗΜΙΟΥΡΓΙΑ ΤΩΝ 16 ΥΠΟΚΛΕΙΔΙΩΝ

Η διαδικασία Key Schedule παράγει τα 16 υποκλειδιά (K_1 έως K_{16}) από το αρχικό 56-bit κλειδί. Το κλειδί υφίσταται μια αρχική μετάθεση (PC-1) και χωρίζεται σε δύο μισά (C και D). Σε κάθε γύρο:

1. Τα C και D **ολισθαίνουν** κυκλικά (Circular Left Shift) κατά 1 ή 2 θέσεις, ανάλογα με τον γύρο.
2. Μια δεύτερη επιλογή μετάθεσης (PC-2) επιλέγει **48 bits** από τα ολισθημένα C και D για να σχηματίσει το υποκλειδί του γύρου K_i.

ΠΑΡΑΔΕΙΓΜΑ 1: ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ECB - ELECTRONIC CODE BOOK (ECB) ΚΑΙ Η ΑΔΥΝΑΜΙΑ ΕΠΑΝΑΛΗΨΗΣ

Electronic Code Book (ECB): Ο πιο απλός τρόπος λειτουργίας. Κάθε block απλού κειμένου (M_i) κρυπτογραφείται **ανεξάρτητα** από τα άλλα, χρησιμοποιώντας το **ίδιο** κλειδί: $C_i = E_K(M_i)$. **Αδυναμία (Παράδειγμα):** Εάν το απλό κείμενο περιέχει **πανομοιότυπα blocks**, τα αντίστοιχα blocks κρυπτοκειμένου θα είναι επίσης πανομοιότυπα. Αυτό **αποκαλύπτει μοτίβα** (patterns) του απλού κειμένου, καθιστώντας το ανασφαλές για οποιαδήποτε μορφή δεδομένων όπου αναμένονται επαναλαμβανόμενες ακολουθίες (π.χ., κρυπτογραφώντας μια εικόνα, διατηρείται η γενική της δομή).

ΤΡΟΠΟΙ ΛΕΙΤΟΥΡΓΙΑΣ: CBC ΚΑΙ CTR - ΕΞΑΡΤΗΣΗ ΚΑΙ ΠΑΡΑΛΛΗΛΙΣΜΟΣ BLOCKS

Οι **Τρόποι Λειτουργίας (Modes of Operation)** επιλύουν τα προβλήματα του ECB εισάγοντας εξάρτηση.

- **CBC (Cipher Block Chaining):** Κάθε block εξαρτάται από το προηγούμενο, αποτρέποντας την επανάληψη μοτίβων. Χρειάζεται ένα τυχαίο **IV (Initialization Vector)** για το πρώτο block: $C_i = E_K(M_i \oplus C_{i-1})$.
- **CTR (Counter Mode):** Μετατρέπει το Block Cipher σε Stream Cipher. Κρυπτογραφεί έναν **μετρητή** (Counter) και το αποτέλεσμα XORίζεται με το απλό κείμενο. **Πλεονέκτημα:** Επιτρέπει τον **παραλληλισμό** στην κρυπτογράφηση και αποκρυπτογράφηση, καθώς κάθε block μπορεί να υπολογιστεί ανεξάρτητα.

Η ΕΞΕΛΙΞΗ ΠΡΟΣ ΤΟ TRIPLE DES (3DES) - ΑΥΞΗΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΚΛΕΙΔΙΟΥ

Με την αύξηση της υπολογιστικής ισχύος, το κλειδί 56-bit του DES κρίθηκε ανασφαλές. Η προσωρινή λύση ήταν ο **Triple DES (3DES)**. Εφαρμόζει τον DES **τρεις φορές** διαδοχικά, συνήθως με δύο διαφορετικά κλειδιά (K_1 και K_2). **Λειτουργία (E-D-E):** $C = E_{K1}(D_{K2}(E_{K1}(M)))$. Αυτό παρέχει ένα αποτελεσματικό μήκος κλειδιού **112 bits**, αυξάνοντας δραματικά την αντοχή σε brute-force. Ο 3DES είναι ασφαλής, αλλά πολύ **πιο αργός** από τον DES και τον AES.

ADVANCED ENCRYPTION STANDARD (AES) - ΤΟ ΤΡΕΧΟΝ ΠΑΓΚΟΣΜΙΟ ΠΡΟΤΥΠΟ

Ο **AES** (Advanced Encryption Standard) επιλέχθηκε το 2001 ως ο διάδοχος του 3DES, βασισμένος στον αλγόριθμο **Rijndael**. Είναι ένα **Block Cipher** σταθερού μήκους **128-bit**.

- **Μήκη Κλειδιού & Γύροι:** Υποστηρίζει κλειδιά **128, 192 ή 256 bits**, με 10, 12 ή 14 γύρους αντίστοιχα. Ο AES είναι σήμερα το πιο διαδεδομένο συμμετρικό κρυπτοσύστημα, λόγω της ισχυρής του ασφάλειας και της εξαιρετικής του ταχύτητας.

ΔΟΜΗ AES: STATE ARRAY ΚΑΙ SPN - ΔΙΚΤΥΟ ΑΝΤΙΚΑΤΑΣΤΑΣΗΣ-ΜΕΤΑΘΕΣΗΣ (SPN)

Ο AES **δεν** χρησιμοποιεί τη δομή Feistel, αλλά ένα **Substitution-Permutation Network (SPN)**. Η είσοδος (128 bits) οργανώνεται σε έναν πίνακα 4x4 από bytes, ο οποίος ονομάζεται **State** (Κατάσταση). Κάθε γύρος (εκτός του τελευταίου) αποτελείται από τέσσερις διαδοχικούς, αναστρέψιμους μετασχηματισμούς που εξασφαλίζουν την πλήρη ανάμειξη των bits.

AES: ΒΑΣΙΚΟΙ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΙ - SUBBYTES (ΣΥΓΧΥΣΗ) ΚΑΙ SHIFTROWS (ΔΙΑΧΥΣΗ)

Οι πρώτες δύο πράξεις κάθε γύρου:

1. **SubBytes (Αντικατάσταση Bytes):** Μη γραμμική αντικατάσταση κάθε byte του State, χρησιμοποιώντας έναν πίνακα αντικατάστασης (**S-Box**). Αυτή η πράξη παρέχει την απαραίτητη **σύγχυση** και μη γραμμικότητα.
2. **ShiftRows (Ολίσθηση Γραμμών):** Κυκλική ολίσθηση των γραμμών του State κατά διαφορετικό αριθμό θέσεων (0, 1, 2, 3). Αυτό επιτυγχάνει **οριζόντια διάχυση**, διασκορπίζοντας τα bytes σε όλο το State.

AES: ΒΑΣΙΚΟΙ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΙ - MIXCOLUMNS (ΙΣΧΥΡΗ ΔΙΑΧΥΣΗ) ΚΑΙ ADDROUNDKEY

Οι επόμενες δύο πράξεις ολοκληρώνουν το κρυπτογραφικό αποτέλεσμα: 3. **MixColumns (Ανάμειξη Στηλών):** Πολλαπλασιασμός κάθε στήλης του State με έναν σταθερό πολυωνυμικό πίνακα, πάνω από το πεπερασμένο σώμα $GF(2^8)$. Αυτή η πράξη παρέχει **ισχυρή διάχυση**, εξασφαλίζοντας ότι κάθε byte εξόδου εξαρτάται από όλα τα bytes της στήλης εισόδου. 4. **AddRoundKey (Προσθήκη Κλειδιού Γύρου):** Το τρέχον State **XORίζεται** με το υποκλειδί (K_i) του γύρου. Αυτή η πράξη εισάγει την **εξάρτηση από το κλειδί**.

ΠΑΡΑΔΕΙΓΜΑ 2: Η ΛΕΙΤΟΥΡΓΙΑ MIXCOLUMNS- ΜΑΘΗΜΑΤΙΚΗ ΒΑΣΗ ΤΗΣ ΔΙΑΧΥΣΗΣ

Η MixColumns είναι το κρίσιμο βήμα που επιτυγχάνει **γρήγορη και ισχυρή διάχυση**. Η πράξη είναι ένας **πολλαπλασιασμός πολυωνύμων** πάνω από το πεπερασμένο σώμα $GF(2^8)$. Η δομή του σταθερού πίνακα εξασφαλίζει ότι οποιαδήποτε αλλαγή σε ένα bit του State διασκορπίζεται σε πολλά άλλα bits μετά από έναν μόνο γύρο, καθιστώντας τον αλγόριθμο εξαιρετικά ανθεκτικό σε επιθέσεις διαφορικής φύσης.

AES: Η ΕΠΕΚΤΑΣΗ ΚΛΕΙΔΙΟΥ (KEY EXPANSION) - ΔΗΜΙΟΥΡΓΙΑ ΤΩΝ ΥΠΟΚΛΕΙΔΙΩΝ

Η διαδικασία Key Expansion παράγει τα υποκλειδιά (Round Keys) για όλους τους γύρους από το αρχικό κλειδί. Ο μηχανισμός είναι **πολύπλοκος** και **μη γραμμικός** για να διασφαλίσει ότι τα υποκλειδιά είναι ανεξάρτητα μεταξύ τους και ότι το αρχικό κλειδί διαχέεται πλήρως. Τα βασικά βήματα περιλαμβάνουν: **RotWord** (κυκλική ολίσθηση), **SubWord** (εφαρμογή S-Box) και **XOR** με μια μοναδική **σταθερά γύρου (Rcon)**.

ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΡΟΗΣ (STREAM CIPHERS) - ΚΡΥΠΤΟΓΡΑΦΗΣΗ BIT ΠΡΟΣ BIT ΣΕ ΠΡΑΓΜΑΤΙΚΟ ΧΡΟΝΟ

Τα Stream Ciphers κρυπτογραφούν το μήνυμα **bit προς bit** (ή byte προς byte) καθώς αυτό παράγεται. Η βασική αρχή είναι η παραγωγή μιας **ψευδοτυχαίας ακολουθίας bits** (την **κλειδοροή,** Z). Η κρυπτογράφηση είναι απλώς η πράξη **XOR** του απλού κειμένου (M) με την κλειδοροή: $C = M \oplus Z$. Είναι ιδανικά για εφαρμογές σε **πραγματικό χρόνο** (π.χ., φωνή, video) λόγω της υψηλής ταχύτητας και της χαμηλής καθυστέρησης.

ΚΑΤΑΧΩΡΗΤΕΣ ΟΛΙΣΘΗΣΗΣ ΜΕ ΑΝΑΔΡΑΣΗ (FSR) - Η ΔΟΜΙΚΗ ΜΟΝΑΔΑ ΤΗΣ ΚΛΕΙΔΟΡΟΗΣ

Οι Καταχωρητές Ολίσθησης με Ανάδραση (Feedback Shift Registers - FSRs) αποτελούν τη βασική αρχιτεκτονική για την παραγωγή κλειδοροών. Αποτελούνται από L **καταχωρητές** (μνήμη) και μια **συνάρτηση ανάδρασης (f)**. Σε κάθε βήμα, τα bits ολισθαίνουν κατά μία θέση και το νέο bit εισόδου υπολογίζεται από την f επί των προηγούμενων L bits. Η πολυπλοκότητα της f καθορίζει την ασφάλεια του Stream Cipher.

ΓΡΑΜΜΙΚΟΙ FSR (LFSR)/ΜΑΘΗΜΑΤΙΚΗ ΒΑΣΗ - Η ΕΝΝΟΙΑ ΤΟΥ ΧΑΡΑΚΤΗΡΙΣΤΙΚΟΥ ΠΟΛΥΩΝΥΜΟΥ

Στους **Γραμμικούς** FSR (LFSRs), η συνάρτηση ανάδρασης είναι **γραμμική** (δηλαδή, ένα άθροισμα XOR των καταχωρητών). Η λειτουργία τους περιγράφεται πλήρως από το **Χαρακτηριστικό Πολυώνυμο** ($P(x)$). Ενώ είναι εύκολοι στην υλοποίηση και αποδοτικοί, η **γραμμικότητά** τους αποτελεί κρυπτογραφική αδυναμία, καθώς μπορούν να αναλυθούν και να σπάσουν με αλγόριθμους γραμμικής ανακατασκευής.

ΠΑΡΑΔΕΙΓΜΑ 3: ΑΚΟΛΟΥΘΙΕΣ ΜΕΓΙΣΤΟΥ ΜΗΚΟΥΣ (M-SEQUENCES) - ΨΕΥΔΟΤΥΧΑΙΟΤΗΤΑ ΚΑΙ ΠΕΡΙΟΔΟΣ

Μια ακολουθία που παράγεται από έναν LFSR μήκους L ονομάζεται **Ακολουθία Μεγίστου Μήκους (M-Sequence)** εάν έχει την **μέγιστη δυνατή περίοδο**: $N = 2^L - 1$. Αυτό επιτυγχάνεται μόνο όταν το χαρακτηριστικό πολυώνυμο ($P(x)$) είναι **Πρωταρχικό (Primitive)**. Οι M-Sequences έχουν καλές ιδιότητες **ψευδοτυχαιότητας** (π.χ. ισορροπημένη κατανομή 0 και 1) και χρησιμοποιούνται ευρέως σε συστήματα επικοινωνιών, αλλά δεν είναι ασφαλείς για κρυπτογραφική χρήση.

ΠΑΡΑΔΕΙΓΜΑ 4: Η ΓΡΑΜΜΙΚΗ ΠΟΛΥΠΛΟΚΟΤΗΤΑ - Η ΚΡΥΠΤΟΓΡΑΦΙΚΗ ΑΔΥΝΑΜΙΑ ΤΩΝ LFSR

Η **Γραμμική Πολυπλοκότητα ($lc(y)$)** μιας ακολουθίας y είναι το μήκος (L) του **μικρότερου** LFSR που μπορεί να παράγει αυτή την ακολουθία. Αυτός είναι ο βασικός δείκτης ασφάλειας: όσο μεγαλύτερη η $lc(y)$, τόσο πιο ασφαλές το Stream Cipher. **Αδυναμία:** Οι M-Sequences μήκους L έχουν $lc(y) = L$. Αυτή η χαμηλή τιμή επιτρέπει την πλήρη ανακατασκευή του LFSR με την παρατήρηση ενός πολύ μικρού τμήματος της ακολουθίας ($2 \times L$ bits) χρησιμοποιώντας τον **Αλγόριθμο Berlekamp-Massey**.

ΠΑΡΑΓΩΓΗ ΑΚΟΛΟΥΘΙΩΝ ΥΨΗΛΗΣ ΠΟΛΥΠΛΟΚΟΤΗΤΑΣ - ΕΙΣΑΓΩΓΗ ΤΗΣ ΜΗ ΓΡΑΜΜΙΚΟΤΗΤΑΣ

Για να είναι ένα Stream Cipher κρυπτογραφικά ασφαλές, η κλειδοροή πρέπει να έχει **πολύ υψηλή Γραμμική Πολυπλοκότητα** (π.χ., $lc(y) \geq 128$). Αυτό επιτυγχάνεται με την εισαγωγή **μη γραμμικών** στοιχείων στη δομή των LFSR:

1. **Μη Γραμμικά Φίλτρα:** Εφαρμογή μιας μη γραμμικής συνάρτησης στην **εσωτερική κατάσταση** ενός LFSR.
2. **Μη Γραμμικοί Συνδυαστές:** Συνδυασμός των **εξόδων** πολλών, ανεξάρτητων LFSRs με μια **μη γραμμική συνάρτηση**.

ΠΑΡΑΔΕΙΓΜΑ 5: ΣΥΝΟΨΗ ΣΥΜΜΕΤΡΙΚΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ - BLOCK CIPHERS VS. STREAM CIPHERS

Η επιλογή του κρυπτοσυστήματος εξαρτάται από την εφαρμογή. **Block Ciphers (AES):** Ιδανικά για κρυπτογράφηση **μεγάλων αρχείων** και **πρωτοκόλλων ασφαλείας** (π.χ., IPsec, TLS), ειδικά όταν απαιτείται ταυτόχρονη εξασφάλιση **ακεραιότητας** (μέσω Modes όπως GCM). **Stream Ciphers (π.χ., ChaCha20):** Ιδανικά για **κρυπτογράφηση δεδομένων σε ροή** και εφαρμογές **χαμηλής καθυστέρησης** (π.χ., 4G/5G, VoIP) λόγω της υψηλής τους ταχύτητας και του χαμηλού overhead.

ΣΥΝΟΨΗ- ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα Συμμετρικά Συστήματα (κοινό κλειδί) είναι γρήγορα και διακρίνονται σε:

1. **Block Ciphers:** (π.χ., **AES**) Κρυπτογραφούν blocks σταθερού μήκους. Η ασφάλεια εξασφαλίζεται μέσω ισχυρής **σύγχυσης** και **διάχυσης** σε πολλούς γύρους.
2. **Stream Ciphers:** Κρυπτογραφούν bit προς bit. Η ασφάλεια τους εξαρτάται από την **υψηλή Γραμμική Πολυπλοκότητα** και την **ψευδοτυχαιότητα** της κλειδοροής, που επιτυγχάνεται μέσω μη γραμμικών μηχανισμών.

ΣΥΝΟΨΗ- ΣΥΜΠΕΡΑΣΜΑΤΑ

Η Σημασία της Σύγχρονης Κρυπτογραφίας

Η μετάβαση από τον DES (56-bit κλειδί) στον **AES** (έως 256-bit κλειδί) ήταν απαραίτητη για την αντιμετώπιση της αυξημένης υπολογιστικής ισχύος. Η ασφάλεια των Block Ciphers προκύπτει από την **πολυπλοκότητα** και το **μη-γραμμικό** αποτέλεσμα των επαναληπτικών γύρων. Τέλος, η επιλογή του **Τρόπου Λειτουργίας** (π.χ. CBC αντί ECB) είναι κρίσιμη για την αποφυγή πρακτικών επιθέσεων στο κρυπτοσύστημα.

ΕΡΩΤΗΣΕΙΣ ΓΙΑ ΣΥΖΗΤΗΣΗ

1. **Σύγκριση Αρχών Ασφάλειας:** Ποια είναι η θεμελιώδης διαφορά στη μηχανική ασφάλειας μεταξύ των **Κρυπτοσυστημάτων Τμήματος (AES)** και των **Κρυπτοσυστημάτων Ροής**; Πώς η έννοια της **πολυπλοκότητας** συνδέεται με την ασφάλεια των Stream Ciphers έναντι της δομικής πολυπλοκότητας των Block Ciphers;
2. **Πρακτικές Αδυναμίες:** Εξηγήστε, δίνοντας ένα πρακτικό παράδειγμα (π.χ., κρυπτογράφηση εικόνας), γιατί ο τρόπος λειτουργίας **Electronic Code Book (ECB)** θεωρείται θεμελιωδώς ανασφαλής. Ποιος από τους τρόπους λειτουργίας (CBC, CTR) προτιμάται για τη μαζική κρυπτογράφηση δεδομένων και γιατί;
3. **Εξέλιξη Προτύπων:** Για ποιους λόγους ο **DES** κρίθηκε ανεπαρκής, παρά τη χρήση του ισχυρού δικτύου Feistel; Πώς ο **AES** αντιμετώπισε αυτές τις αδυναμίες μέσω αλλαγών στη δομή του (SPN αντί Feistel) και, κυρίως, στο μήκος του κλειδιού;

ΠΡΟΒΛΗΜΑΤΑ ΕΞΑΣΚΗΣΗΣ

Πρόβλημα 1: Υπολογισμός Δύναμης (Βασική Πράξη)

Ερώτηση: Υπολογίστε το αποτέλεσμα της έκφρασης $3^{23} \pmod{13}$ χρησιμοποιώντας τον **αλγόριθμο επαναλαμβανόμενου τετραγωνισμού**.

Πρόβλημα 2: Γραμμική Πολυπλοκότητα (Εννοιολογικό)

Ερώτηση: Μία κλειδοροή y παράγεται από έναν **Γραμμικό Καταχωρητή Ολίσθησης με Ανάδραση (LFSR)** μήκους $L = 5$, με πρωταρχικό χαρακτηριστικό πολυώνυμο.

1. Ποια είναι η **μέγιστη περίοδος** που μπορεί να έχει αυτή η ακολουθία y;
2. Ποια είναι η **Γραμμική Πολυπλοκότητα** ($lc(y)$) της ακολουθίας;
3. Τι σημαίνει η τιμή της $lc(y)$ για την **κρυπτογραφική ασφάλεια** της ακολουθίας και πόσα bits κλειδοροής αρκούν για να "σπάσει" (ανακατασκευαστεί) ο LFSR;