Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Σημειώσεις Διαλέξεων

UP class

&

DES και AES

Επιμέλεια σημειώσεων:
Ιωάννης Νέμπαρης
Μάριος Κουβαράς

Διδάσκοντες:
Στάθης Ζάχος
Άρης Παγουρτζής

11 Φεβρουαρίου 2013

1 UP *class*

Θα αποδείξουμε ότι η κλάση UP ισούται με την P, αν και μόνο αν υπάρχουν συναρτήσεις μονής κατεύθυνσης. Λέμε ότι μια γλώσσα ανήκει στο UP αν μια MT την αποφασίζει και έχει την εξής ιδιότητα: Αν το x ανήκει στη γλώσσα υπάρχει ακριβώς ένα κλαδί υπολογισμού απ όλο το full complete binary tree του υπολογισμού που επιστρέφει yes. Αλλιώς κάθε κλαδί του υπολογισμού επιστρέφει no. Προφανώς η κλάση είναι υποσύνολο της NP (όπου τα yes μονοπάτια είναι τουλάχιστον 1).

Η κλάση UP είναι σημαντική για την κρυπτογραφία. Ακολουθεί η απόδειξη του θεωρήματος.

" $\Leftarrow$ ": Έστω f συνάρτηση μονής κατεύθυνσης. Ορίζω $L_f = \{(x, y) : \exists z : f(z) = y, z \leq x\}$ Το $z \leq x$ είναι καταχρηστικός συμβολισμός και ορίζει την σχέση των μηκών τους. Οπότε $z \leq x$ σημαίνει είτε ότι το z έχει μικρότερο μήκος ή ότι προηγείται λεξικογραφικά.

Λήμμα 1.1. $L_f \in UP - P$.
Απόδειξη: Κατασκευάζω μια MT που δέχεται την γλώσσα L_f. Μη ντετερμινιστικά μαντεύω ένα z τέτοιο ώστε $f(z) = y$ και με μήκος του $z \leq |y|^k$ ώστε να μην ξεφεύγω από την πολυωνυμικότητα της μηχανής. Αν $|z| \leq |x|$ τότε η μηχανή αποδέχεται. Ακόμα από ορισμό, η συνάρτηση μονής κατεύθυνσης είναι και 1-1, άρα η MT είναι μονοσήμαντη, άρα υπάρχει όντως ακριβώς ένα κλαδί υπολογισμού που η μηχανή αποδέχεται και αντιστοιχεί σε αυτή τη μοναδική τιμή που μαντέψαμε μη ντετερμινιστικά.

Λήμμα 1.2. $L_f \notin P$.
Απόδειξη: Έστω η L_f αποφασίζεται από πολυωνυμικό αλγόριθμο, από μηχανή M'. Θα καταλήξω ότι μπορώ να αντιστρέψω την f γρήγορα με μια τεχνική σαν δυαδική αναζήτηση. Αυτό όμως θα αντίκειται στην υπόθεση μας ότι η f είναι μονής κατεύθυνσης και έτσι θα προκύψει το άτοπο. Ρωτάμε την M' αν $(1^{|y|^k}, y) \in L_f$. Αν δεν υπάρχει τέτοιο z, τότε σημαίνει ότι ισχύει η ισότητα και $|z| = |x|$ ώστε $f(z) = y$. Άρα το μήκος του z είναι γνωστό και μένει να βρούμε τα ψηφία του, με τρόπο που ακολουθεί παρακάτω. Αν υπάρχει τέτοιο z, θα ρωτήσω την M' για ένα τέτοιο z μισού μήκους, δηλαδή μήκους $1^{|y|^{k-1}}$. Κάποια στιγμή, όταν μου επιστραφεί αρνητική απάντηση, θα ξέρω ότι έχω προσδιορίσει το μήκος του z, (γιατί θα έχω καταλήξει στην πάνω περίπτωση) και $|z| = |x|$. Πως θα προσδιορίσω τώρα τα ψηφία του z; Θα εκμεταλλευτώ τη λεξικογραφικότητα. Γνωρίζοντας πλέον το μήκος του z, ρωτώ την M' αν $(1^{|y|^l}, y) \in L_f$. Αυτό επιστρέφει σίγουρα yes γιατί αυτό το z είναι σίγουρα μικρότερο ή ίσο του x. Αν όμως ρωτήσω αν $(01^{|y|^{l-1}}, y) \in L_f$ και πάρω απάντηση no, τότε σίγουρα το z αυτό είναι το $1^{|y|^k}$. Λογικά θα έχω αρκετά yes στην αρχή, οπότε θα συνεχίσω να ρωτάω αν πχ $(001^{|y|^{l-1}}, y) \in L_f (101^{|y|^{l-1}}, y) \in L_f$ και σε χρόνο ανάλογο του μήκους της συμβολοσειράς, θα έχω τελικά προσδιορίσει όλα τα ψηφία.
" $\Rightarrow$ ": Έστω ότι $\exists L \in UP - P$, θα δημιουργήσουμε μια συνάρτηση μονής κατεύθυνσης.

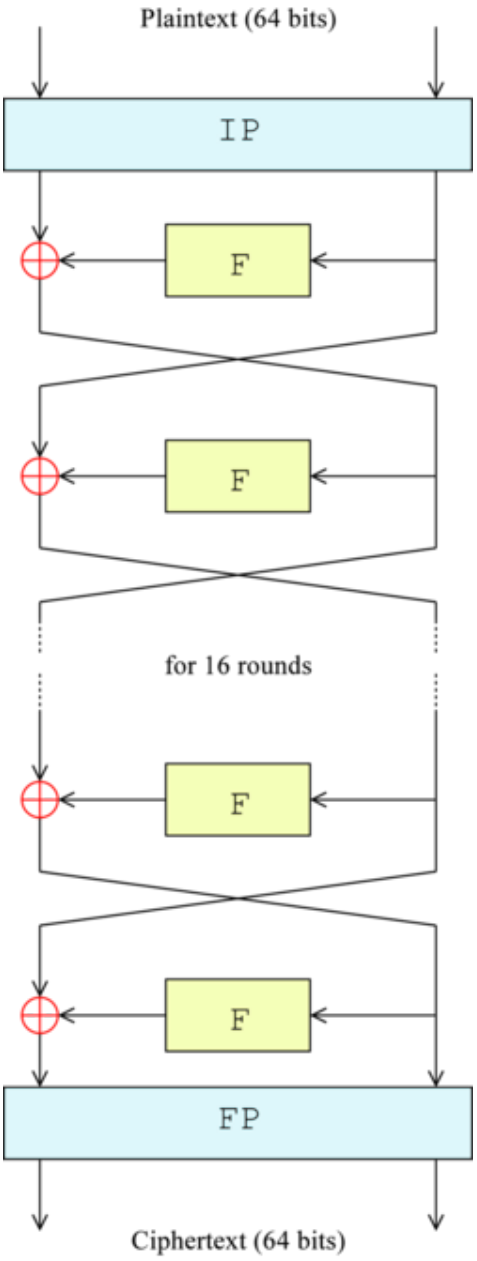
Έστω M η μηχανή που αποφασίζει αυτή τη γλώσσα.Και έστω p ο κωδικός ενός μονοπατιού της M που αποδέχεται με είσοδο y (υπενθυμίζεται ότι ως κωδικός μονοπατιού, μπορεί να θεωρηθεί η 'διαδρομή' απ' την κορυφή ως το κλαδι, με κάθε 0 να σημαίνει ότι συνεχίζω πχ στο αριστερό υποδένδρο, ενώ 1 σημαίνει στο δεξί). Ορίζουμε $f(x) = 1y$ αν $x = p$ αλλιώς $f(x) = 0x$, άρα γνωρίζω αν ένα $x \in L$ διαβάζοντας μόνο ένα bit, το πρώτο.

Λήμμα 1.3. *Η f είναι μονής κατεύθυνσης.*
Η f περιέχει το x αν $p = x$ $(f(p) = 1p)$. Άρα ο υπολογισμός της $f(x)$ διαρκεί όσο σχεδόν και αυτός της x (+ 1 bit). Επίσης το x υπολογίζεται σε πολυωνυμικό χρόνο (η M είναι πολυωνυμική μηχανή). Άρα παραμένουμε σε πολυωνυμικό χρόνο. Ακόμα, η f είναι 1-1 επειδή η M έχει μόνο ένα υπολογιστικό μονοπάτι, για το οποίο η μηχανή αποδέχεται για κάθε $x \neq x'$ και έτσι $f(x) \neq f(x')$. Τέλος η f δεν αντιστρέφεται, γιατί αν αντιστρεφόταν η $f^{-1}(1y)$ θα μας έδειχνε αν η M αποφασίζει ή όχι και άρα η M θα ήταν μια P μηχανή, όχι μια $UP - P$.

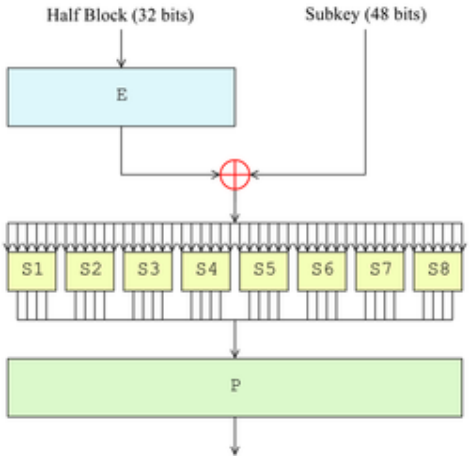
2 DES

Θα αναφερθούμε τώρα στο κρυπτοσύστημα DES. Ο αλγόριθμος DES είναι ένας block cipher αλγόριθμος. Ο αλγόριθμος παίρνει ένα αρχικό κείμενο δεδομένου μήκους και παράγει ένα κρυπτοκείμενο ιδίου μήκους. Η διαδικασία της κρυπτογράφησης γίνεται μέσω ενός δικτύου Feistel, στο οποίο και θα αναφερθούμε στη συνέχεια. Το DES χρησιμοποιεί και ένα κλειδί για να μπορούν να αποκρυπτογραφούν μηνύματα, μόνο όσοι το γνωρίζουν. Αρχικά η είσοδος χωρίζεται σε blocks των 64 bits. Αν τα bits της εισόδου δεν είναι πολλαπλάσια του 64, απλά συμπληρώνω με κάποια dummy bits το τελευταίο block. Αρχικά σε κάθε τέτοιο block κάνω μια permutation (χωρίς αυτό να χει κάποια ιδιαίτερη σημασία). Στην συνέχεια έχω ένα δίκτυο Feistel. Αυτό αποτελείται από 16 γύρους. Χωρίζω το 64-sized block σε δεξί και αριστερό τμήμα. Το δεξί 32-bit τμήμα γίνεται αριστερό τμήμα για το επόμενο στάδιο του δικτύου και το δεξί τμήμα του επόμενου επιπέδου ισούται με το αριστερό τμήμα του προηγούμενου XOR το δεξί τμήμα αφού περάσει πρώτα από μια F (Feistel function). Κάθε F τέτοια Feistel "συνάρτηση" δέχεται ως είσοδο ένα υποblock 32 bits. Αφού κάνει XOR με ένα υποκλειδί του αρχικού κλειδιού μήκους 48 bits και δημιουργημένο από κάποια swifts στο αρχικό κλειδί τα 48 bits, εισέρχονται σε S-boxes τα οποία είναι μη γραμμικά "look-up tables" τα οποία επιστρέφουν έξοδο μήκους 32. Γίνεται εμφανές λοιπόν ότι τα S-boxes είναι η καρδια του DES. Αν ήταν γραμμικές συναρτήσεις το σύστημα θα μπορούσε πολύ εύκολα να σπάσει, εφόσον απλά θα αρκούσε να ακολουθήσω την αντίστροφη διαδικασία.Όπως είναι φυσικό και έγινε και εμφανές από όσα προαναφέρθηκαν, δεν υπάρχει σαφής απόδειξη για την ασφάλεια του συστήματος. Δεν ξέρουμε αν ο δημιουργός του συστήματος δεν κράτησε κάποια trapdoor συνάρτηση, που να αντιστρέφει το μετασχηματισμό. Αυτός είναι και ο λόγος που το σύστημα κατακρίθηκε πολύ. Ωστόσο το σύστημα μέχρι να ξεπεραστεί, δεν υπέκυψε σε καμία επίθεση που να διέφερε

ουσιαστικά από την ωμή βία. Η μοναδική τέτοια επίθεση είναι η επίθεση γνωστού κρυπτοκειμένου. Υπό την προϋπόθεση ότι ο επιτιθέμενος είχε στην διάθεση του έναν αριθμό (μη ρεαλιστικό) κειμένων και των κρυπτοκειμένων που τους αντιστοιχούσαν, μπορούσε να σπάσει το σύστημα. Βέβαια γίνεται λόγος για 2^{50} τέτοια κείμενα. Τέλος, το DES είχε μια 'αδύναμη' ιδιότητα. Είναι συμμετρικό, δηλαδή με συμμετρικά κλειδιά συμμετρικά αρχικά κείμενα οδηγούν σε συμμετρικά κρυπτοκείμενα. Βέβαια αυτό απλά μειώνει κατά στο μισό τον ήδη τεράστιο αριθμό περιπτώσεων που εμφανίζονται στην ωμή βία.



Σχήμα 1: Το DES κύκλωμα με το Feistel δίκτυο



Σχήμα 2: Η Feistel Function

3 AES

Τέσσερις τρόπους λειτουργίας (modes of operation) αναπτύχθηκαν για το DES και αυτοί, με μικρές αλλαγές, μπορούν να χρησιμοποιηθούν για κάθε block cipher. Αυτοί, που χρησιμοποιούνται και στο AES, είναι:

1. electronic codebook mode(ECB mode)
2. cipher feedback mode(CFB mode)
3. cipher block chaining mode(CBC mode)
4. output feedback mode(OFB mode).

ECB Πλεονεκτήματα:

- Η κρυπτογράφηση e_i γίνεται για κάθε x_i ξεχωριστά οπότε υπάρχει δυνατότητα παράλληλιας.
- Λογω ξεχωριστής κρυπτογράφησης για κάθε x_i έχουμε μη διάδοση λαθών(τοπικότητα λαθών).

Μειονεκτήματα:

- Όμοια plaintext μπλοκς δημιούργουν όμοια μπλοκς κρυπτοκειμένου ($x_i = x_j \Rightarrow c_i = c_j$).

CBC $c_i = e_K * (c_{i-1} \oplus x_i)$

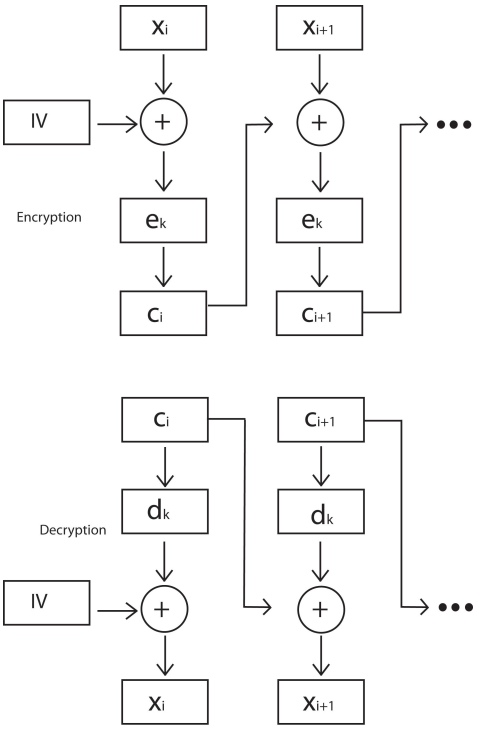
Πλεονετήματα:

- Όμοια plaintext μπλοκς δεν συνεπάγονται όμοια μπλοκς κρυπτοκειμένου ($x = x_j \Rightarrow c_i \; neq c_j$).
- Αν ένα x_i αλλάξει τότε αλλαζουν όλα τα c_j (για $j \geq i$).Αυτό είναι χρήσιμο σε keyed hash function(MAC) και μπορεί να χρησιμοποιηθεί για να message authetication αλλά και να εξασφαλίσει την ακεραιότητα.
- Αν υπάρχει λάθος στο plaintext υπάρχει αντίστοιχο λάθος στην αποκρυπτογράφηση.
- Αν υπάρχει λάθος στο cyphertext επηρεάζονται δύο μόνο blocks, το δεύτερο κιόλας κατά τον ίδιο αριθμό bit (self recovering property).

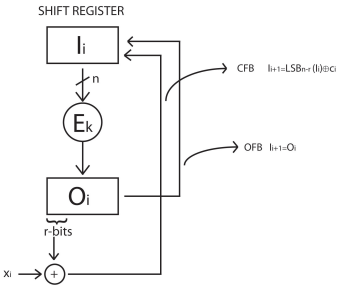
Μειονεκτήματα:

- Σε προσθήκη ή απώλεια bits έχουμε διάδοση των λαθών παντού.
- Ο malicious adversary μπορεί να αλλάξει κατά βούληση το plaintext αν ξέρει το plaintext. Έτσι θα έχουμε ένα χαλασμένο μπλοκ (θα νομίζουμε ότι ειναι error) και αυτά που θα προκύπτουν θα'ναι αλλαγμένες πληροφορίες.

CFB-OFB Παράγουν keystream σε πακέτα των r-bits($r < n$) $I_1 =$ IV(initializing vector).



Σχήμα 3: Αρχιτεκτονική AES



Σχήμα 4: CFB-OFB καταχωρητής