Τεχνικὴ περιγραφὴ τῆς κρυπτογράφησης DES

Ν.Γ. Τζανάκης

Τελευταία ἐνημέρωση Μάρτιος 2003

Στὰ παρακάτω, ἕνας ἀριθμὸς n-bit ταυτίζεται μὲ ἕνα διάνυσμα ἀπὸ τὸ $\mathbb{F}_2^n$. Ἔτσι, π.χ. τὸν $x = 1001011$ ταυτίζομε μὲ τὸ διάνυσμα $(1,0,0,1,0,1,1) \in \mathbb{F}_2^7$. Ἐπίσης, λέγοντας π.χ. «ὁ 4-ψήφιος δυαδικὸς ἀριθμὸς 1101», ἢ «ὁ 4-bit ἀριθμὸς 1101», ἐννοοῦμε τὸ ἴδιο πρᾶγμα. Ἂν ὅμως τὸν βλέπαμε σὰν τὸν ἀριθμὸ 001101, εἶναι ἀκριβέστερο νὰ τὸν χαρακτηρίσομε ὡς 6-bit ἀριθμό, παρὰ ὡς 6-ψήφιο δυαδικὸ ἀριθμό, ἀκριβῶς ὅπως δὲν θὰ ἦταν εὔστοχο νὰ χαρακτηρίσομε τὸν ἀριθμὸ 153 ὡς 6-ψήφιο ἐπειδὴ μποροῦμε νὰ τὸν γράψομε καὶ ὡς 000153.

Προσοχή! Ἡ πρόσθεση $\oplus$ δύο δυαδικῶν ἀριθμῶν (πρόσθεση $\bmod 2$ κατὰ συντεταγμένες) διαφέρει ἀπὸ τὴ συνηθισμένη πρόσθεσή τους. Λ.χ. ἂν $x = 1001011$ καὶ $y = 1100011$, τότε $x + y = 10101110$, ἐνῶ $x \oplus y = 0101000$.

Ἂν x, y εἶναι δυαδικοὶ ἀριθμοὶ μὲ m καὶ n ψηφία, ἀντιστοίχως, τότε xy δηλώνει τὸν δυαδικὸ ἀριθμὸ μὲ $m+n$ στοιχεῖα, ποὺ προκύπτει ἀπὸ τὴν ἀλληλουχία τῶν x, y. Ἔτσι, γιὰ παράδειγμα, ἂν $x = 1001011$ καὶ $y = 11001$, τότε $xy = 100101111001$.

ΕΡΓΑΛΕΙΑ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ DES

- Συνάρτηση $f : \mathbb{F}_2^{32} \times \mathbb{F}_2^{48} \longrightarrow \mathbb{F}_2^{32}$, τὴν ὁποία θὰ περιγράψομε παρακάτω.
- Κλειδιὰ $k_0 \in \mathbb{F}_2^{56}$ καὶ $k_1, \ldots, k_{16} \in \mathbb{F}_2^{48}$. Τὰ $k_1, \ldots, k_{16}$ κατασκευάζονται ἀπὸ τὸ k_0 μὲ μία διαδικασία, τὴν ὁποία περιγράφομε παρακάτω.
- Μετάθεση $\mathrm{IP} \in \mathbb{S}_{64}$.

ΔΙΑΔΙΚΑΣΙΑ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ DES

Τὸ πρὸς κρυπτογράφηση μήνυμα M εἶναι ἕνας 64-bit ἀριθμὸς. Ὁ ἀλγόριθμος, ποὺ ὁδηγεῖ στὸ κρυπτογραφημένο μήνυμα KM, περιγράφεται ἀμέσως παρακάτω. Τὰ L_i καὶ R_i συμβολίζουν 32-bit ἀριθμούς.

- Μοίρασε σὲ δεξιὸ καὶ ἀριστερὸ τμῆμα τὸν IP(M): $\mathrm{IP(M)} = L_0 R_0$.
- Γιὰ $i = 0, 1, \ldots, 15$ κάνε

$$\begin{aligned} L_{i+1} &= R_i \\ R_{i+1} &= L_i \oplus f(R_i, k_{i+1}) \end{aligned}$$

- $\mathrm{KM} = \mathrm{IP}^{-1}(R_{16}L_{16})$

ΔΙΑΔΙΚΑΣΙΑ ΤΗΣ ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗΣ DES

Ἔχοντας λάβει τὸ κρυπτογραφημένο μήνυμα KM, ἀκολουθοῦμε τὴν ἑξῆς διαδικασία, ἡ ὁποία εἶναι ἐντελῶς ἀντίστοιχη μὲ αὐτὴν τῆς κρυπτογράφησης:

- Ὑπολογίζουμε τὸ $IP(\mathrm{KM})$ τὸ ὁποῖο γράφουμε ὡς $L'_0R'_0$.
- Θέτουμε $k'_i = k_{17-i}$ γιὰ $i = 1, \ldots, 16$.
- Γιὰ $i = 0, 1, \ldots, 15$ ὑπολογίζουμε ἀναδρομικά

$$L'_{i+1} = R'_i \ , \ R'_{i+1} = L'_i \oplus f(R'_i, k'_{i+1}) \ ,$$

  ὅπου ἡ f εἶναι ἡ ἴδια μὲ αὐτὴ ποὺ χρησιμοποιήθηκε στὴν κρυπτογράφηση.

- $\mathrm{M} = \mathrm{IP}^{-1}(R'_{16}L'_{16})$

Πράγματι, ἂς θεωρήσομε, πρὸς τὸ παρόν, δεδομένο ὅτι ἰσχύει,

$$L'_i = R_{16-i} \quad \text{καὶ} \quad R'_i = L_{16-i} \ \ (i = 0, \ldots 16) \tag{1}$$

Τότε, $R'_{16} = L_0$, $L'_{16} = R_0$, ἄρα,

$$\mathrm{IP}^{-1}(R'_{16}L'_{16}) = \mathrm{IP}^{-1}(L_0R_0) = \mathrm{IP}^{-1}(\mathrm{IP}(\mathrm{M})) = \mathrm{M} \ .$$

Ἀπόδειξη τῆς (1): Γιὰ $i = 0$ εἴδαμε ἤδη ὅτι ἰσχύει. Ἔστω ὅτι ἰσχύει ἡ (1) γιὰ κάποιο $i = 0, \ldots, 15$. Θὰ δείξομε ὅτι ἰσχύει καὶ γιὰ τὸ $i + 1$. Πράγματι,

$$L'_{i+1} = R'_i = L_{16-i} = L_{(15-i)+1} = R_{15-i} = R_{16-(i+1)} \ .$$

Ἐπίσης,

$$R'_{i+1} = L'_i \oplus f(R'_i, k'_{i+1}) = R_{16-i} \oplus f(R_{15-i}, k_{(15-i)+1}) \ .$$

Ὅμως, ἐξ ὁρισμοῦ, $R_{16-i} = L_{15-i} \oplus f(R_{15-i}, k_{(15-i)+1})$, ἄρα, ἐπανερχόμενοι στὴν παραπάνω σχέση,

$$R'_{i+1} = (L_{15-i} \oplus f(R_{15-i}, k_{(15-i)+1})) \oplus f(R_{15-i}, k_{(15-i)+1}) = L_{15-i} = L_{16-(i+1)} \ ,$$

δηλαδή, ἀποδείξαμε τὸν ἰσχυρισμό μας. Σημειῶστε ὅτι, ἀμέσως παραπάνω, κάναμε χρήση τοῦ ὅτι, ἂν b εἶναι k-bit ἀριθμός, τότε $b \oplus b =$ μηδενικὸς k-bit ἀριθμός.

Ἡ συνάρτηση f. Γιὰ τὴν κατασκευὴ της ἀπαιτοῦνται:

- Μία *διασταλτικὴ συνάρτηση* $E : \mathbb{F}_2^{32} \to \mathbb{F}_2^{48}$.
  Σκοπὸς της εἶναι νὰ παίρνει ἕνα 32-bit ἀριθμὸ καὶ νὰ δίνει ἕνα 48-bit ἀριθμό, ὡς ἑξῆς: Ἡ E παριστάνεται ἀπὸ ἕνα πίνακα διαστάσεως 8×6 μὲ ἐγγραφὲς ἀπὸ 1 ἕως 32 (ἄρα, δὲν εἶναι ὅλες οἱ ἐγγραφὲς διαφορετικές). Π.χ. ἔστω

$$E = \begin{pmatrix} 32 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 14 & 15 & 16 & 17 \\ 16 & 17 & 18 & 19 & 20 & 21 \\ 20 & 21 & 22 & 23 & 24 & 25 \\ 24 & 25 & 26 & 27 & 28 & 29 \\ 28 & 29 & 30 & 31 & 32 & 1 \end{pmatrix} \tag{2}$$

  καὶ θέλομε νὰ ὑπολογίσομε τὸν $E(x)$ γιὰ κάποιο συγκεκριμένο 32-bit ἀριθμὸ x. Ὁ $E(x)$ ἔχει 48 bits. Ποιὸ εἶναι π.χ. τὸ δέκατο τέταρτο; Ἀρχίζοντας νὰ μετροῦμε τὶς ἐγγραφὲς τοῦ πίνακα E ἀπὸ ἄνω ἀριστερὰ πρὸς τὰ δεξιὰ καὶ κάτω, βλέπομε ὅτι ἡ δέκατη τέταρτη ἐγγραφὴ εἶναι στὴν τρίτη γραμμὴ καὶ τὴ δεύτερη στήλη, δηλαδή, τὸ 9. Κοιτάζομε τότε ποιὸ εἶναι τὸ ἔννατο bit τοῦ x καὶ βάζομε αὐτὸ ὡς δέκατο τέταρτο bit τοῦ $E(x)$. Γιὰ παράδειγμα, ἐλέγξτε ὅτι, ἂν $x = 01101011101001010100000010001100$, τότε $E(x) = 001101010111110100001010101000000010100011111000$.

- Πίνακες $S_1, \ldots, S_8$ διαστάσεως 4×16 μὲ ἐγγραφὲς μέσα ἀπὸ τὸ σύνολο $\{0, 1, \ldots, 15\}$.
  Αὐτοὶ δημιουργοῦν τὰ λεγόμενα *κουτιὰ* S. Κάθε πίνακας S εἶναι διαστάσεως 4×16 μὲ ἐγγραφὲς μέσα ἀπὸ τὸ σύνολο $\{0, 1, \ldots, 15\}$. Ἡ ἀρίθμηση τῶν γραμμῶν του εἶναι ἀπὸ 0 ἕως 3 (ἀντὶ ἀπὸ 1 ἑως 4) καὶ ἡ ἀρίθμηση τῶν στηλῶν του ἀπὸ 0 ἕως 15 (ἀντὶ ἀπὸ 1 ἕως 16). Ἕνα κουτὶ S εἶναι μία συνάρτηση μὲ πεδίο ὁρισμοῦ τοὺς δυαδικοὺς ἀριθμοὺς 6 bits καὶ πεδίο τιμῶν τοὺς δυαδικοὺς ἀριθμοὺς 4 bits, μέσῳ τῆς ἑξῆς διαδικασίας: Ἂν $x = b_1b_2b_3b_4b_5b_6$ εἶναι ὁ 6-bit ἀριθμός, τότε βλέπομε τὴν ἐγγραφὴ τοῦ πίνακα, ἡ ὁποία ἀντιστοιχεῖ στὴ γραμμὴ ποὺ δηλώνει ὁ δυαδικὸς ἀριθμὸς b_1b_6 (ὁ ὁποῖος, μετατρεπόμενος σὲ δεκαδικό, εἶναι μεταξὺ 0 καὶ 3) καὶ στὴ στήλη ποὺ δηλώνει ὁ δυαδικὸς ἀριθμὸς $b_2b_3b_4b_5$ (ὁ ὁποῖος, μετατρεπόμενος σὲ δεκαδικό, εἶναι μεταξὺ 0 καὶ 15). Γιὰ παράδειγμα, ἂν

$$S = \begin{pmatrix} 12 & 10 & 9 & 4 & 1 & 15 & 14 & 3 & 10 & 4 & 15 & 2 & 15 & 2 & 5 & 12 \\ 9 & 7 & 2 & 9 & 2 & 12 & 8 & 5 & 6 & 9 & 12 & 15 & 8 & 5 & 3 & 10 \\ 0 & 6 & 7 & 11 & 13 & 1 & 0 & 14 & 3 & 13 & 4 & 1 & 4 & 14 & 10 & 7 \\ 14 & 0 & 1 & 6 & 7 & 11 & 13 & 0 & 5 & 3 & 11 & 8 & 11 & 8 & 6 & 13 \end{pmatrix},$$

  καὶ $x = 011011$, τότε $b_1b_6 = 01 =$ δεκαδικὸς 1 καὶ $b_2b_3b_4b_5 = 1101 =$ δεκαδικὸς 13. Ἡ ἐγγραφὴ τοῦ πίνακα, ποὺ βρίσκεται στὴ γραμμὴ ὑπ' ἀριθμὸν

1 καὶ τὴ στήλη ὑπ' ἀριθμὸν 13 (μὴ ξεχνᾶτε ὅτι ἡ ἀρίθμηση ἀρχίζει ἀπὸ τὸ 0!) εἶναι $5 =$ 4-bit ἀριθμὸς 0101. Ἄρα $S(x) = 0101$.

- Μετάθεση $P \in \mathbb{S}_{32}$.

Πῶς βρίσκεται ἡ τιμὴ $f(x, y)$ γιὰ x 32-bit ἀριθμὸ καὶ y 48-bit ἀριθμό:

- Ὑπολογίζεις πρῶτα τὸν $E(x) \oplus y$, ὁ ὁποῖος εἶναι 48-bit ἀριθμὸς.
- Τὸν παραπάνω ἀριθμὸ «σπᾶς» σὲ 8 6-bit ἀριθμούς:

$$E(x) \oplus y = B_1B_2B_3B_4B_5B_6B_7B_8.$$

- Γιὰ $i = 1, \ldots, 8$ ὑπολογίζεις τὰ $S_i(B_i) =$ (ἔστω) C_i. Ὑπενθυμίζεται ὅτι καθένας ἀπὸ τοὺς C_i εἶναι 4-bit ἀριθμός.
- Σχηματίζεις τὸν 32-bit ἀριθμὸ $C = C_1C_2C_3C_4C_5C_6C_7C_8$.
- Μεταθέτεις τὰ ψηφία τοῦ C σύμφωνα μὲ τὴ μετάθεση P παίρνοντας ἕνα νέο 32-bit ἀριθμὸ $P(C)$.

Τελικά, $f(x, y) = P(C)$.

Τὰ κλειδιὰ k. Γιὰ τὴν κατασκευή τους ἀπαιτοῦνται:

- Τὸ κλειδὶ k_0, ποὺ εἶναι ἕνας 56-bit ἀριθμός.
- Μία μετάθεση $PC_1 \in \mathbb{S}_{56}$.
- Μία ἀμφιμονοσήμαντη ἀπεικόνιση $PC_2 : \{1, 2, \ldots, 48\} \longrightarrow \{1, 2, \ldots, 56\}$.

Πρὶν περιγράψομε τὴ διαδικασία κατασκευῆς τῶν 16 κλειδιῶν $k_1, \ldots, k_{16}$, ἂς κάνομε δύο σχόλια στὸ συμβολισμὸ καὶ τὴν ὁρολογία:

(α′) Γενικά, γιὰ $m \geq n$, μία ἀμφιμονοσήμαντη ἀπεικόνιση $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ (ἄρα, εἰδικώτερα, μία μετάθεση $\sigma \in \mathbb{S}_n$) μποροῦμε νὰ τὴν παραστήσομε ὡς διάνυσμα $\sigma = (a_1, a_2, ..., a_n)$ μὲ τὶς συντεταγμένες a_i διαφορετικὲς μεταξύ τους, ἐπιλεγμένες μέσα ἀπὸ τὸ σύνολο $\{1, 2, \ldots, m\}$, ἐννοώντας, προφανῶς, ὅτι ἡ ἀπεικόνιση εἶναι ἡ ἑξῆς: $1 \to a_1$, $2 \to a_2, \ldots, n \to a_n$. Προσοχή! Μὴ γίνει σύγχυση μὲ τὸν συμβολισμὸ τῶν *κύκλων*, ποὺ χρησιμοποιοῦμε στὶς μεταθέσεις. Ὅταν, γιὰ παράδειγμα, γράφομε $\tau = (1\,5\,4\,3\,2) \in \mathbb{S}_5$ (χωρὶς κόμματα ἀνάμεσα στοὺς ἀριθμούς), ἐννοοῦμε τὴ μετάθεση (κύκλο) $1 \to 5\,, 5 \to 4\,, 4 \to 3\,, 3 \to 2\,, 2 \to 1$, ἐνῶ, μὲ συμβολισμὸ διανύσματος, $\tau = (2, 3, 4, 5, 1)$.
Ἂν, τώρα, ὁ $x = b_1b_2 \ldots b_n$ εἶναι ἕνας n-bit ἀριθμός, τότε, $\sigma(x) = b_{a_1}b_{a_2} \ldots b_{a_n}$. Γιὰ παράδειγμα, ἔστω $n = 6, \sigma = (2, 1, 3, 4, 6, 5)$ καὶ $x = 011011$. Τότε $\sigma(x) = b_2b_1b_3b_4b_6b_5 = 101011$.

(β′) Ὅταν λέμε *ἡ μετακίνηση τοῦ δυαδικοῦ* $x = b_1b_2 \ldots b_{n-1}b_n$ μία θέση πρὸς τ' ἀριστερά, ἐννοοῦμε τὸν δυαδικὸ $\mu_1(x) = b_2b_3 \ldots b_nb_1$. Ἀνάλογα, ἡ μετακίνηση τοῦ x δύο θέσεις πρὸς τ' ἀριστερά, εἶναι ὁ $\mu_2(x) = b_3b_2 \ldots b_nb_1b_2$.

Ἀλγόριθμος για τὴν κατασκευὴ τῶν κλειδιῶν k_j:
Θέσε ἀρχικὰ $PC_1(k_0) = c_0 d_0$, ὅπου καθένας ἀπὸ τοὺς c_0, d_0 εἶναι 28-bit ἀριθμός.
Γιὰ $j = 1, \ldots 16$ κάνε:

- $c_j = \mu_1(c_{j-1})$ ἂν $j = 1, 2, 9, 16$ καὶ $c_j = \mu_2(c_{j-1})$ διαφορετικά.
- Ὅρισε ἀναλόγως τὸ d_j.
- Σχημάτισε τὸν $c_j d_j = (\ddot{\varepsilon}\sigma\tau\omega)\, b_1 b_2 \ldots b_{56}$.
- Θέσε $k_j = b_{i_1} b_{i_2} \ldots b_{i_{48}}$, ὅπου $i_m = PC_2(m)$.

Γιὰ παράδειγμα, ἔστω ὅτι

$$
\begin{aligned}
k_0 &= 1100011110000100010111110101011100011010101111110001111 0 \qquad (3)\\
PC_1 &= (50, 43, 36, 29, 22, 15, 8, 1, 51, 44, 37, 30, 23, 16, 9, 2, 52, 45, 38,\\
&\quad 31, 24, 17, 10, 3, 53, 46, 39, 32, 56, 49, 42, 35, 28, 21, 14, 7, 55, 48,\\
&\quad 41, 34, 27, 20, 13, 6, 54, 47, 40, 33, 26, 19, 12, 5, 25, 18, 11, 4)\\
PC_2 &= (14, 17, 11, 24, 1, 5, 3, 28, 15, 6, 21, 10, 23, 19, 12, 4, 26, 8, 16, 7, 27, 20, 13, 2, 41,\\
&\quad 52, 31, 37, 47, 55, 30, 40, 51, 44, 33, 48, 44, 49, 39, 56, 34, 53, 46, 42, 50, 36, 29, 32)
\end{aligned}
$$

Ὁ ὑπολογισμὸς τοῦ k_1 γίνεται ὡς ἑξῆς:

$$
PC_1(k_0) = \underbrace{0110101101111011110110001111}_{c_0}\underbrace{0000111111100101110010000100}_{c_1}
$$

$$
\begin{aligned}
c_1 &= \mu_1(c_0) = 1101011011110111101100011110 = b_1 \ldots b_{28}\\
d_1 &= \mu(d_0) = 0001111111001011100100001000 = b_{29} \ldots b_{56}\\
k_1 &= 111110001101011110111101100100000111100011000101
\end{aligned}
$$

Λ.χ. τὸ πρῶτο bit τοῦ k_1 εἶναι 1 διότι $PC_2(1) = 14$ καὶ $b_{14} = 1$. Τὸ προτελευταῖο bit τοῦ k_1 εἶναι 0 διότι $PC_2(47) = 29$ καὶ $b_{29} = 0$.

Ἕνα συγκεκριμένο παράδειγμα. Ἔστω ὅτι τὰ δεδομένα μας γιὰ μία κρυπτογράφηση DES εἶναι:

$$
\begin{aligned}
IP &= (58, 50, 42, 34, 26, 18, 10, 2, 60, 52, 44, 36, 28, 20, 12, 4,\\
&\quad 62, 54, 46, 38, 30, 22, 14, 6, 64, 56, 48, 40, 32, 24, 16, 8,\\
&\quad 57, 49, 41, 33, 25, 17, 9, 1, 59, 51, 43, 35, 27, 19, 11, 3,\\
&\quad 61, 53, 45, 37, 29, 21, 13, 5, 63, 55, 47, 39, 31, 23, 15, 7)\\
P &= (16, 7, 20, 21, 29, 12, 28, 17, 1, 15, 23, 26, 5, 18, 31, 10,\\
&\quad 2, 8, 24, 14, 32, 27, 3, 9, 19, 13, 30, 6, 22, 11, 4, 25)
\end{aligned}
$$

Ἡ E δίνεται μέσῳ τοῦ πίνακα (2) καὶ τὰ k_0, PC_1, PC_2 δίνονται ἀπὸ τὴν (3).

Πίνακες γιὰ τὰ Κιβώτια S

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
S_1	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
S_2	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
	0	10	0	9	14	6	13	15	5	1	13	12	7	11	4	2	8
S_3	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
S_4	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
S_5	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
S_6	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
S_7	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
S_8	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Ἔχομε ἤδη βρεῖ:

$$\begin{aligned}
c_1 &= \mu_1(c_0) = 11010110111101111101100011110\\
d_1 &= \mu(d_0) = 00011111110010111100100001000\\
\boxed{k_1} &= 11111000110101111011110110010000011111000011000101
\end{aligned}$$

Σύμφωνα μὲ τὸν ἀλγόριθμο, ποὺ περιγράψαμε προηγουμένως, ἔχομε διαδοχικά:

$$\begin{aligned}
c_2 &= \mu_1(c_1) = 10101101111011111011000111101\\
d_2 &= \mu_1(d_1) = 00111111100101111001000010000\\
\boxed{k_2} &= 10111111110111001110001001111001011010001001010 1\\
c_3 &= \mu_2(c_2) = 10110111101111011000111110110\\
d_3 &= \mu_2(d_2) = 11111110010111001000010000000\\
\boxed{k_3} &= 11111010011010111111101010100011001000000100110 11\\
c_4 &= \mu_2(c_3) = 11011110111101100011111011010\\
d_4 &= \mu_2(d_3) = 11111001011100100000100000011\\
\boxed{k_4} &= 10111100111101110001110100100111001100110000011 1\\
c_5 &= \mu_2(c_4) = 01111011110110001111011010 11\\
d_5 &= \mu_2(d_4) = 11100101110010000100000011 11\\
\boxed{k_5} &= 01000111000111110101111110110110000000001111001 10\\
c_6 &= \mu_2(c_5) = 11101111011000111101101011 01\\
d_6 &= \mu_2(d_5) = 10010111001000010000000111111\\
\boxed{k_6} &= 01101111111110001111010101000100110010101111000 111\\
c_7 &= \mu_2(c_6) = 10111101100011111011010110111\\
d_7 &= \mu_2(d_6) = 01011100100001000000111111110\\
\boxed{k_7} &= 10011111111011011110101001010110101001001101100 1\\
c_8 &= \mu_2(c_7) = 11110110001111011010110111 10\\
d_8 &= \mu_2(d_7) = 01110010000100000011111111001\\
\boxed{k_8} &= 11111010011001111011101101101011100101010100100 1\\
c_9 &= \mu_1(c_8) = 11101100011110110101101111 01\\
d_9 &= \mu_1(d_8) = 11100100001000000111111100 10\\
\boxed{k_9} &= 00111111111110101010011101101110100101101010101 0\\
c_{10} &= \mu_2(c_9) = 10110001111011010110111101 11\\
d_{10} &= \mu_2(d_9) = 10010000100000011111111001011\\
\boxed{k_{10}} &= 10111011001111011110101000011100010111010110101 1
\end{aligned}$$

$$
\begin{aligned}
c_{11} &= \mu_2(c_{10}) = 11000111101101011011111011110\\
d_{11} &= \mu_2(d_{10}) = 01000010000001111111100101110\\
\boxed{k_{11}} &= 11111000011001101111110100001110110110000011100000\\
c_{12} &= \mu_2(c_{11}) = 00011110110101101111011111011\\
d_{12} &= \mu_2(d_{11}) = 00001000000111111110010111001\\
\boxed{k_{12}} &= 11010101110111110001110011000001111011010111000 0\\
c_{13} &= \mu_2(c_{12}) = 01111011010110111101111011 00\\
d_{13} &= \mu_2(d_{12}) = 00100000011111110010111001 00\\
\boxed{k_{13}} &= 01000110101110111111011110101001110011100001100 0\\
c_{14} &= \mu_2(c_{13}) = 11101101011011110111101100 01\\
d_{14} &= \mu_2(d_{13}) = 10000001111111001011100100 00\\
\boxed{k_{14}} &= 10111111111111000110011111011001000101100001011 0\\
c_{15} &= \mu_2(c_{14}) = 10110101101111011111011000 111\\
d_{15} &= \mu_2(d_{14}) = 00000111111100101110010000 10\\
\boxed{k_{15}} &= 11101011011001111111010100001110100000010101011 00\\
c_{16} &= \mu_1(c_{15}) = 01101011011110111110110001 111\\
d_{16} &= \mu_1(d_{15}) = 00001111111001011100100001 00\\
\boxed{k_{16}} &= 01100111101100101111111100010000011011101011010 0
\end{aligned}
$$

Ας υποθέσομε τώρα ότι θέλομε να κρυπτογραφήσομε τον 32-bit αριθμό

$\mathrm{KM} = 01101011101001010100000100011100000001100010001101000101100000 00$.

Υπολογίζοντας το $IP(\mathrm{KM}) = L_0R_0$ βρίσκομε

$$
\begin{aligned}
L_0 &= 01000101000010000101101001100111\\
R_0 &= 10000010001000110000100100110001
\end{aligned}
$$

Τώρα πρέπει να υπολογίσομε την τιμή $f(R_0, k_1)$. Σύμφωνα με τη διαδικασία, που έχομε περιγράψει, κάνομε τα εξής διαδοχικά βήματα:

$$
\begin{aligned}
E(R_0) &= 11000000010000010000011010000101001010011010 0011\\
E(R_0)\oplus k_1 &= \underbrace{001110}_{B_1}\underbrace{001001}_{B_2}\underbrace{011010}_{B_3}\underbrace{111011}_{B_4}\underbrace{000101}_{B_5}\underbrace{010101}_{B_6}\underbrace{000101}_{B_7}\underbrace{100110}_{B_8}\\
C &= S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)\\
&= \underbrace{1000}_{C_1}\underbrace{1111}_{C_2}\underbrace{0100}_{C_3}\underbrace{0111}_{C_4}\underbrace{0010}_{C_5}\underbrace{1101}_{C_6}\underbrace{1011}_{C_7}\underbrace{0001}_{C_8}\\
P(C) &= 11010010110010010111110010011001 = \boxed{f(R_0, k_1)}
\end{aligned}
$$

Άρα,

$$
\begin{aligned}
L_1 &= R_0 = 10000010001000110000100100110001\\
R_1 &= L_0 \oplus f(R_0, k_1) = 10010111110000010010011011111110
\end{aligned}
$$

Ἡ διαδικασία ἐπαναλαμβάνεται ἐντελῶς ἀνάλογα, ὁπότε ὑπολογίζονται τὰ ἑξῆς:

$$
\begin{aligned}
f(R_1, k_2) &= 01111010011000011110111011010000 \\
L_2 &= 10010111110000010010011011111110 \\
R_2 &= 11111000010000101110011111100001 \\
f(R_2, k_3) &= 00010001010011000101110001110000 \\
L_3 &= 11111000010000101110011111100001 \\
R_3 &= 10000110100011010111101010001110 \\
f(R_3, k_4) &= 10110001101000011111000010001111 \\
L_4 &= 10000110100011010111101010001110 \\
R_4 &= 01001001111000110001011101101110 \\
f(R_4, k_5) &= 11110110000010111000110100010010 \\
L_5 &= 01001001111000110001011101101110 \\
R_5 &= 01110000100001101111011110011100 \\
f(R_5, k_6) &= 11101100101110111011110100000100 \\
L_6 &= 01110000100001101111011110011100 \\
R_6 &= 10100101010110001010101001101010 \\
f(R_6, k_7) &= 00001010111010100000101011011110 \\
L_7 &= 10100101010110001010101001101010 \\
R_7 &= 01111010011011001111110101000010 \\
f(R_7, k_8) &= 01010010011000101111110110111010 \\
L_8 &= 01111010011011001111110101000010 \\
R_8 &= 11110111001110100101011111010000 \\
f(R_8, k_9) &= 10110010111011110011101000011100 \\
L_9 &= 11110111001110100101011111010000 \\
R_9 &= 11001000100000111100011101011110 \\
f(R_9, k_{10}) &= 11111010100010101001001011111000 \\
L_{10} &= 11001000100000111100011101011110 \\
R_{10} &= 00001101101100001100010100101000 \\
f(R_{10}, k_{11}) &= 01110001100010101101110100101010 \\
L_{11} &= 00001101101100001100010100101000 \\
R_{11} &= 10111001000010010001101001110100 \\
f(R_{11}, k_{12}) &= 01010100010000010000010101000110 \\
L_{12} &= 10111001000010010001101001110100 \\
R_{12} &= 01011001111100011100000001101110 \\
f(R_{12}, k_{13}) &= 00101000100011000010000001011110 \\
L_{13} &= 01011001111100011100000001101110 \\
R_{13} &= 10010001100001010011101000101010
\end{aligned}
$$

$$
\begin{aligned}
f(R_{13}, k_{14}) &= 10101100001001111101101101110001 \\
L_{14} &= 10010001100001010011101000101010 \\
R_{14} &= 11110101110101100001101100011111 \\
f(R_{14}, k_{15}) &= 11000110110011011110100100101010 \\
L_{15} &= 11110101110101100001101100011111 \\
R_{15} &= 01010111010010001101001100000000 \\
f(R_{15}, k_{16}) &= 10111001000000111111011001000101 \\
L_{16} &= 01010111010010001101001100000000 \\
R_{16} &= 01001100110101011110110101011010
\end{aligned}
$$

Τέλος, τὸ **κρυπτογραφημένο μήνυμα** είναι $\mathrm{KM} = IP^{-1}(R_{16}L_{16}) =$
1001110010001001110101000110010110011001000001001111110100011100