Κρυπτογραφία

Εργαστηριακό μάθημα 11
(Επαναληπτικές ασκήσεις)

Σύνοψη κρυπτογραφικών αλγορίθμων – Αλγόριθμος Hill

- Έστω ότι το κλειδί είναι ένας πίνακας 2 x 2. Αυτό σημαίνει ότι:
  - Σπάμε το μήνυμα σε ζευγάρια γραμμάτων
  - Κάθε γράμμα το αντιστοιχούμε σε έναν αριθμό (π.χ. το Α αντιστοιχεί στον αριθμό 0, το Β στον αριθμό 1 κ.ο.κ.)
  - Κάνουμε τους αντίστοιχους πολλαπλασιασμούς. (βλέπε συνέχεια)

Σύνοψη κρυπτογραφικών αλγορίθμων – Αλγόριθμος Hill

- Έστω ότι θέλουμε να κρυπτογραφήσουμε τη λέξη ΓΕΙΑ. Σαν κλειδί έχουμε τον πίνακα

$$K = \begin{pmatrix} 1 & 3 \\ 2 & 13 \end{pmatrix}$$

- Σπάμε το μήνυμα σε ζευγάρια. Το πρώτο ζευγάρι είναι το ΓΕ και το δεύτερο το ΙΑ.
- Το Γ είναι το 3ο γράμμα της αλφαβήτου, άρα αντιστοιχεί στον αριθμό 2. Το Ε είναι το 5 γράμμα, άρα αντιστοιχεί στον αριθμό 4. Συνεπώς, για την κρυπτογράφηση του ΓΕ θα έχουμε τον πολλαπλασιασμό:

Σύνοψη κρυπτογραφικών αλγορίθμων – Αλγόριθμος Hill

$$\begin{pmatrix} 1 & 3 \\ 2 & 13 \end{pmatrix}\begin{pmatrix} 2 \\ 4 \end{pmatrix} \bmod 24 = \begin{pmatrix} 1\cdot 2+3\cdot 4 \\ 2\cdot 2+13\cdot 4 \end{pmatrix} \bmod 24 = \begin{pmatrix} 2+12 \\ 4+52 \end{pmatrix} \bmod 24 =$$

$$= \begin{pmatrix} 14 \\ 56 \end{pmatrix} \bmod 24 = \begin{pmatrix} 14 \\ 8 \end{pmatrix} \longrightarrow \begin{pmatrix} O \\ I \end{pmatrix}$$

- Η τελευταία ανάθεση γίνεται γιατί το Ο είναι το 15ο γράμμα της αλφαβήτου και το Ι το 9ο .
- ΠΡΟΣΟΧΗ! Αν το κείμενο που θέλαμε να κρυπτογραφήσουμε ήταν αγγλικό, στις πράξεις που προηγήθηκαν δεν θα είχαμε mod 24 αλλά mod 26 (επειδή τα γράμματα του αγγλικού αλφάβητου είναι 26)

Σύνοψη κρυπτογραφικών αλγορίθμων – Αλγόριθμος Hill

- Άρα το ζευγάρι ΓΕ κρυπτογραφείται σε ΟΙ.
- Άσκηση: κρυπτογραφείστε το ζευγάρι ΙΑ
- Πώς θα γίνει η αποκρυπτογράφηση?? Ας υποθέσουμε ότι ο παραλήπτης λαμβάνει το ΟΙ και ξέρει και τον πίνακα-κλειδί Κ. Πώς θα αποκρυπτογραφήσει??
- Πρέπει πρώτα να υπολογίσει τον αντίστροφο πίνακα του Κ και μετά να τον πολλαπλασιάσει με το κρυπτόγραμμα που αντιστοιχεί στο ΟΙ.
- Για τον αντίστροφο πίνακα του Κ εργαζόμαστε ως εξής:

Σύνοψη κρυπτογραφικών αλγορίθμων – Αλγόριθμος Hill

- Βρίσκουμε πρώτα την ορίζουσα του K, η οποία συμβολίζεται με det(K).
- Γενικά, για έναν πίνακα $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

η ορίζουσά του det(K) ισούται με ad-bc.

- Άρα, για τον πίνακά μας, έχουμε det(K)=1 · 13 - 3· 2 = 7
- Στη συνέχεια, πρέπει να βρούμε τον αντίστροφο της ορίζουσας, άρα τον αντίστροφο του 7 mod 24.
- Θα εφαρμόσουμε τον αλγόριθμο του Ευκλείδη.

Σύνοψη κρυπτογραφικών αλγορίθμων – Αλγόριθμος Hill

- $24 = 3 \cdot 7 + 3$
- $7 = 2 \cdot 3 + 1$

Σταματάμε. Άρα, η τελευταία σχέση δίνει

1= 7 - 2 · 3 και επειδή η πρώτη σχέση δίνει
3 = 24 - 3 · 7, καταλήγουμε:

$1=7 – 2 \cdot (24 - 3 \cdot 7) = 7 – 2 \cdot 24 + 6 \cdot 7 =$

$7 \cdot 7 - 2 \cdot 24.$

Άρα, ο αντίστροφος του 7 mod 24 είναι ο 7.

Σύνοψη κρυπτογραφικών αλγορίθμων – Αλγόριθμος Hill

Ο αντίστροφος ενός πίνακα $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Είναι ο πίνακας $K^{-1} = \det(K)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Άρα, για μας: $K^{-1} = 7^{-1} \begin{pmatrix} 13 & -3 \\ -2 & 1 \end{pmatrix} \bmod 24$

Είδαμε ήδη όμως παραπάνω ότι $7^{-1} \bmod 24 = 7$ και, επίσης, ισχύει, $-3 \bmod 24 = (-3+24) \bmod 24 = 21$ και $-2 \bmod 24 = (-2+24) \bmod 24 = 22$. Άρα, έχουμε:

Σύνοψη κρυπτογραφικών αλγορίθμων – Αλγόριθμος Hill

$$K^{-1} = 7 \begin{pmatrix} 13 & 21 \\ 22 & 1 \end{pmatrix} \bmod 24 = \begin{pmatrix} 91 & 147 \\ 154 & 7 \end{pmatrix} \bmod 24 = \begin{pmatrix} 19 & 3 \\ 10 & 7 \end{pmatrix}$$

Τώρα πια είμαστε έτοιμοι να κάνουμε αποκρυπτογράφηση. Για την αποκρυπτογράφηση του ΟΙ, κάνουμε τον πολλαπλασιασμό

$$\begin{pmatrix} 19 & 3 \\ 10 & 7 \end{pmatrix} \begin{pmatrix} 14 \\ 8 \end{pmatrix} \bmod 24 = \begin{pmatrix} 19 \cdot 14 + 3 \cdot 8 \\ 10 \cdot 14 + 7 \cdot 8 \end{pmatrix} \bmod 24 = \begin{pmatrix} 266 + 24 \\ 140 + 56 \end{pmatrix} \bmod 24 =$$

$$\begin{pmatrix} 290 \\ 196 \end{pmatrix} \bmod 24 = \begin{pmatrix} 2 \\ 4 \end{pmatrix} \longrightarrow \begin{pmatrix} \Gamma \\ \text{E} \end{pmatrix}$$

Σύνοψη κρυπτογραφικών αλγορίθμων – Αλγόριθμος Hill

Προσοχή! Δεν έχουν όλοι οι πίνακες αντίστροφο, οπότε ο πίνακας κλειδί δεν μπορεί να είναι ο οποιοσδήποτε – πρέπει να είναι τέτοιος ώστε να έχει αντίστροφο.

Πότε ο K είναι αντιστρέψιμος?? Πρέπει **gcd(det(K),N)=1**

Ποιοι λοιπόν από τους παρακάτω πίνακες μπορούν να είναι κλειδιά σε κρυπτογράφηση Hill ελληνικού κειμένου???

$$\begin{pmatrix} 3 & 8 \\ 1 & 6 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 4 & 9 \end{pmatrix}, \begin{pmatrix} 5 & 2 \\ 10 & 4 \end{pmatrix}$$

Σύνοψη κρυπτογραφικών αλγορίθμων - RSA

- Δημιουργία δημόσιου-ιδιωτικού κλειδιού από έναν χρήστη:
  - Επιλογή δύο πρώτων αριθμών p,q. Έστω p=11, q=19.
  - Υπολογισμός N=pq=209
  - Υπολογισμός φ(N)=(p-1)(q-1)=180
  - Επιλογή e τέτοιου ώστε gcd(e,φ(N))=1.

    π.χ. μεταξύ των 39,56,29, μόνο το 29 μπορεί να επιλεγεί ως e.
  - Εύρεση του αντίστροφου του e mod φ(N).

Σύνοψη κρυπτογραφικών αλγορίθμων - RSA

- Αλγόριθμος του Ευκλείδη:

$180 = 6 \cdot 29 + 6$

$29 = 4 \cdot 6 + 5$

$6 = 1 \cdot 5 + 1$

Άρα, θα έχουμε $1 = 6 - 1 \cdot 5 =$

$= 6 - 1 \cdot (29 - 4 \cdot 6) = 6 - 1 \cdot 29 + 4 \cdot 6 =$

$= 5 \cdot 6 - 1 \cdot 29 = 5 \cdot (180 - 6 \cdot 29) - 1 \cdot 29 =$

$= 5 \cdot 180 - 31 \cdot 29$

Σύνοψη κρυπτογραφικών αλγορίθμων - RSA

- Άρα ο αντίστροφος του 29 είναι ο -31 mod 180 = (-31+180) mod 180 = 149.
- Άρα d=149
- Δημόσιο κλειδί: e,N
- Ιδιωτικό κλειδί: d
- Για την κρυπτογράφηση λοιπόν του αριθμού m έχουμε $c=m^e \bmod N$
- Και την αποκρυπτογράφηση: $m=c^d \bmod N$

Σύνοψη κρυπτογραφικών αλγορίθμων – El Gamal

- Παραγωγή Δημόσιου-Ιδιωτικού κλειδιού
  - Ο χρήστης επιλέγει πρώτο αριθμό p. Έστω p=7.
  - Επιλέγει γεννήτορα g mod 7. Προσέξτε: οι αριθμοί g=2,4,6 δεν είναι γεννήτορας mod 7, αλλά οι g=3,5, είναι.
  - Έστω λοιπόν g=3
  - Επιλογή a τυχαίου. Έστω a=4
  - Υπολογισμός $y = g^a \bmod p = 81 \bmod 7 = 4$
  - Δημόσιο Κλειδί: (p, g, y). Ιδιωτικό κλειδί: a.

Σύνοψη κρυπτογραφικών αλγορίθμων – El Gamal

- Κρυπτογράφηση του αριθμού m=2
  - Επιλογή τυχαίου k. Έστω k=5.
  - (προσοχή! Ανάλογα με την επιλογή του k, θα προκύψει και άλλο κρυπτόγραμμα!! Πάντα όμως η αποκρυπτογράφηση εν τέλει θα είναι σωστή!!)
  - Υπολογισμός του $\gamma=g^k \bmod p =5$ και του $\delta=my^k \bmod p = 2\cdot 4^5 \bmod 7 = 4$
  - Άρα, το κρυπτόγραμμα είναι: (γ,δ)=(5,4)

Σύνοψη κρυπτογραφικών αλγορίθμων – El Gamal

- Αποκρυπτογράφηση του (γ,δ)=(5,4)
  - Υπολογισμός του $\delta/\gamma^{\alpha} \bmod p$.
  - $\gamma^{\alpha}=5^4 \bmod 7 = 625 \bmod 7 = 2$
  - Θέλουμε λοιπόν τον αντίστροφο του 2 mod 7. Προφανώς είναι 4. Άρα, η αποκρυπτογράφηση δίνει

    $4 \cdot 4 \bmod 7 = 16 \bmod 7 = 2$

Πράγματι λοιπόν αποκρυπτογραφήσαμε το m=2