Κρυπτογραφία

Εργαστηριακό μάθημα 10
(Επαναληπτικές ασκήσεις)

Εύρεση αντίστροφου αριθμού Mod n

- Έχουμε ήδη δει ότι πολύ συχνά συναντάμε την ανάγκη να βρούμε τον αντίστροφο ενός αριθμού a modulo n, δηλαδή έναν αριθμό a' με την ιδιότητα

$$aa' \equiv 1 \bmod n$$

(*όπου, για να μπορούμε να βρούμε πάντα έναν τέτοιον μοναδικό αριθμό a', πρέπει gcd(a,n)=1*)

- Το πρόβλημα εύρεσης αντιστρόφου το συναντήσαμε:
  - Στον γραμμικό αλγόριθμο αλλά και στον αλγόριθμο Hill για την αποκρυπτογράφηση
  - Στον RSA για τον υπολογισμό του ιδιωτικού κλειδιού d (θυμίζουμε ότι το d είναι τέτοιο ώστε $ed \equiv 1 \bmod \varphi(n)$)
  - Στον El Gamal, για την αποκρυπτογράφηση (όπου χρειάζεται ο υπολογισμός του γ^{-a}, δηλαδή η εύρεση του αντίστροφου του γ^{a}).

Πώς βρίσκουμε τον αντίστροφο???

- Πρώτος τρόπος: αν τα νούμερα είναι σχετικά μικρά, μπορούμε να τον βρούμε με δοκιμές, δοκιμάζοντας όλα τα πιθανά νούμερα.
- Παράδειγμα: έστω ότι θέλουμε τον αντίστροφο του 5 mod 11. Οι πιθανοί αντίστροφοι είναι προφανώς οι 1,2,…,10 (όλοι οι αριθμοί από 1 μέχρι 11-1=10). Δοκιμάζουμε λοιπόν για αυτούς τους 10 αριθμούς ποιος ικανοποιεί τη σχέση $5x \equiv 1 \bmod 11$. Μπορούμε να δούμε λοιπόν ότι $5^{-1} \equiv 9 \bmod 11$.

Υπάρχει πιο συστηματικός τρόπος??

- Ο επεκταμένος αλγόριθμος του Ευκλείδη (τον αναλύσαμε κατά την περιγραφή του RSA).
- Παράδειγμα RSA
  - Ένας χρήστης θέλει να δημιουργήσει ζευγάρι δημόσιου και ιδιωτικού κλειδιού. Κάνει λοιπόν τα εξής:
    - Επιλέγει p=19, q=29. Τότε N=pq=551.
    - φ(N)=18 · 28 = 504
    - Επιλογή e που να μην έχει κοινούς διαιρέτες με το 504. Έστω e=25.
    - Υπολογισμός του ιδιωτικού κλειδιού d. Έχουμε λοιπόν:

$$504 = 20 \cdot 25 + 4$$

$$25 = 6 \cdot 4 + 1$$

$$4 = 4 \cdot 1 + 0$$

Σταματάμε (όπου πράγματι επιβεβαιώσαμε ότι gcd(504,25)=1)

Πώς βρίσκουμε λοιπόν το d???

Αλγόριθμος του Ευκλείδη (συνέχεια)

- Διαβάζουμε τις προηγούμενες σχέσεις ανάποδα ως εξής:

$1 = 25 - 6 \cdot 4 = 25 - 6 \cdot (504 - 20 \cdot 25) =$

$= 25 - 6 \cdot 504 + 120 \cdot 25 \Rightarrow$

$\Rightarrow \quad 1 = -6 \cdot 504 + 121 \cdot 25$

Άρα $25^{-1} \equiv 121 \bmod 504$

(επαλήθευση: $121 \cdot 25 = 3025$, το οποίο αν το διαιρέσουμε με το 504 δίνει υπόλοιπο 1).

Άρα $d=121$.

Κρυπτογράφηση – Αποκρυπτογράφηση RSA

- Αν m το μήνυμα που θέλουμε να στείλουμε, τότε το κρυπτογραφούμε με την πράξη $c = m^e \bmod N$.

- Ο παραλήπτης (κάτοχος του ιδιωτικού κλειδιού d) το αποκρυπτογραφεί με την πράξη $c^d \bmod N$.
- Στη συγκεκριμένη περίπτωση, ισχύει το εξής:

  Αν $m^{25} \bmod 551 = c$, τότε

  $c^{121} \bmod 551 = m$ για όλα τα m

  (η απόδειξη αυτού έγινε στο μάθημα του RSA).

Σύνοψη κρυπτογραφικών μεθόδων:

- Ας κρυπτογραφήσουμε τη λέξη HELLO με όσους αλγορίθμους έχουμε δει μέχρι τώρα:
- Αλγόριθμος του Καίσαρα: KHOOR (κάθε γράμμα μετατοπίζεται κατά 3 θέσεις δεξιά).

Σύνοψη κρυπτογραφικών αλγορίθμων

- Αλγόριθμος του Vigenere: χρειαζόμαστε μια λέξη-κλειδί.
- Έστω σαν κλειδί η λέξη CRYPTOGRAPHY. Τότε το κρυπτόγραμμα για τη λέξη HELLO είναι JVJAH.
- Υλοποίηση στο MATLAB:

http://mathdemos.gcsu.edu/vigenere/vigenere.html

(το αρχείο ventable.zip)

Σύνοψη κρυπτογραφικών αλγορίθμων

- Γραμμικός αλγόριθμος: έστω a=3, b=1
  (θα μπορούσαμε να είχαμε επιλέξει π.χ. a=4?? Όχι, γιατί πρέπει gcd(a,n)=1, όπου n το πλήθος των γραμμάτων του αλφαβήτου – κι αφού είμαστε στο αγγλικό αλφάβητο, n=26).
- Το H είναι το 8ο γράμμα, άρα κρυπτογραφείται σε $3 \cdot 7 + 1 \bmod 26 = 22$. Συνεπώς το H κρυπτογραφείται στο 23ο γράμμα, που είναι το W.
- Αντίστοιχα για το E έχουμε: $(3 \cdot 4 + 1) \bmod 26 = 13$, οπότε το E κρυπτογραφείται στο 14ο γράμμα – δηλαδή στο N.
- Για το L: $(3 \cdot 11 + 1) \bmod 26 = 34 \bmod 26 = 8$, οπότε το L κρυπτογραφείται στο 9ο γράμμα – δηλαδή στο I.
- Τέλος, για το O: $(3 \cdot 14 + 1) \bmod 26 = 43 \bmod 26 = 17$. Άρα το O κρυπτογραφείται στο 18ο γράμμα, που είναι το R.
- Συνεπώς, το HELLO κρυπτογραφείται σε WNIIR.

Σύνοψη κρυπτογραφικών αλγορίθμων

- Γραμμικός αλγόριθμος (αποκρυπτογράφηση):
- Κάθε ένα κρυπτογραφημένο γράμμα c αποκρυπτογραφείται με την πράξη

$$a^{-1}(c-b) \bmod N$$

- Ας δούμε πως θα αποκρυπτογραφούσαμε το WNIIR. Καταρχήν πρέπει να βρούμε το $3^{-1} \bmod 26$. Είτε με αλγόριθμο του Ευκλείδη είτε με δοκιμές μπορούμε να βρούμε ότι ισούται με 9. Συνεπώς:
  - Για το W ($23^{ο}$ γράμμα) έχουμε: $9(22-1) \equiv 189 \bmod 26 \equiv 7$
    Άρα, το W αποκρυπτογραφείται στο $8^{ο}$ γράμμα του αλφαβήτου, δηλαδή το H
  - Για το N ($14^{ο}$ γράμμα) έχουμε $9(13-1) \equiv 108 \bmod 26 \equiv 4$.
    Άρα, το N αποκρυπτογραφείται στο $5^{ο}$ γράμμα του αλφαβήτου, δηλαδή στο E.
  - Ομοίως συνεχίζουμε και για τα υπόλοιπα…..

Σύνοψη κρυπτογραφικών αλγορίθμων

- Αλγόριθμος Hill
- Έστω ότι κάποιοι προτείνουν σαν πίνακα κρυπτογράφησης τον

$$\begin{pmatrix} 2 & 3 \\ 4 & 7 \end{pmatrix}$$

- Μπορούμε να τον χρησιμοποιήσουμε??
- Η ορίζουσα του παραπάνω πίνακα ισούται με $2 \cdot 7 - 3 \cdot 4 = 2$, και $\gcd(2,26) = 2$.

  Συνεπώς, αφού η ορίζουσα δεν είναι πρώτη ως προς το 26, ο πίνακας δεν είναι αντιστρέψιμος mod 26 – άρα δεν μπορεί να χρησιμοποιηθεί για κρυπτογράφηση.

Σύνοψη κρυπτογραφικών αλγορίθμων

- Αλγόριθμος Hill (συνέχεια)
- Έστω ότι εξετάζουμε τον πίνακα $K = \begin{pmatrix} 2 & 3 \\ 1 & 7 \end{pmatrix}$
- Η ορίζουσα αυτού είναι 11 – άρα, πράγματι είναι ένας πίνακας που μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση Hill.
- Το ζευγάρι γραμμάτων HE κρυπτογραφείται με βάση το γινόμενο

$$\begin{pmatrix} 2 & 3 \\ 1 & 7 \end{pmatrix}\begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 26 \\ 35 \end{pmatrix} = \begin{pmatrix} 0 \\ 9 \end{pmatrix} \bmod 26$$

Άρα, το ζευγάρι HE γίνεται AJ

Σύνοψη κρυπτογραφικών αλγορίθμων

- Αλγόριθμος Hill (συνέχεια)
- Το ζευγάρι γραμμάτων LL κρυπτογραφείται με βάση το γινόμενο

$$\begin{pmatrix} 2 & 3 \\ 1 & 7 \end{pmatrix}\begin{pmatrix} 11 \\ 11 \end{pmatrix} = \begin{pmatrix} 55 \\ 88 \end{pmatrix} = \begin{pmatrix} 3 \\ 10 \end{pmatrix} \bmod 26$$

Άρα, το ζευγάρι LL γίνεται DK

Σύνοψη κρυπτογραφικών αλγορίθμων

- Τέλος, το Ο επειδή μένει μόνο του συμπληρώνεται αυθαίρετα με ένα άλλο γράμμα, κατάλληλο ώστε να μην μπερδεύει τον παραλήπτη – να καταλάβει ότι είναι απλά πλεονάζον γράμμα. Συνηθέστερα επιλέγεται το πλεονάζον γράμμα να είναι το Q (χωρίς βέβαια να αποκλείονται και άλλα γράμματα). Έτσι, το ζευγάρι γραμμάτων OQ κρυπτογραφείται με βάση το γινόμενο

$$\begin{pmatrix} 2 & 3 \\ 1 & 7 \end{pmatrix}\begin{pmatrix} 14 \\ 16 \end{pmatrix} = \begin{pmatrix} 76 \\ 126 \end{pmatrix} = \begin{pmatrix} 24 \\ 22 \end{pmatrix} \bmod 26$$

Άρα, το ζευγάρι LQ γίνεται YW

Άρα η λέξη HELLO γίνεται AJDKYW

Σύνοψη κρυπτογραφικών αλγορίθμων

- Αποκρυπτογράφηση Hill
- Χρειάζεται να υπολογιστεί ο αντίστροφος του πίνακα κρυπτογράφησης, ο οποίος αντίστροφος είναι ο:

$$11^{-1}\begin{pmatrix} 7 & -3 \\ -1 & 2 \end{pmatrix} \bmod 26$$

Ο $11^{-1} \bmod 26$ μπορεί να υπολογιστεί με τον αλγόριθμο του Ευκλείδη

Σύνοψη κρυπτογραφικών αλγορίθμων

- Αποκρυπτογράφηση Hill (συνέχεια)

$$26 = 2 \cdot 11 + 4$$

$$11 = 2 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1$$

$$3 = 3 \cdot 1 + 0$$

Συνεπώς:

$$1 = 4 - 1 \cdot 3 = 4 - 1 \cdot (11 - 2 \cdot 4) = -1 \cdot 11 + 3 \cdot 4 =$$

$$= -1 \cdot 11 + 3 \cdot (26 - 2 \cdot 11) = 3 \cdot 26 - 7 \cdot 11$$

Άρα $11^{-1} \bmod 26 = -7 \bmod 26 = 19$

(το 19 προέκυψε από την πράξη -7 + 26)

Σύνοψη κρυπτογραφικών αλγορίθμων

- Αποκρυπτογράφηση Hill (συνέχεια)

Ο πίνακας αποκρυπτογράφησης λοιπόν ισούται με:

$$19\begin{pmatrix} 7 & -3 \\ -1 & 2 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 133 & -57 \\ -19 & 38 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 3 & 21 \\ 7 & 12 \end{pmatrix}$$

Κάθε λοιπόν ζευγάρι από το κρυπτόγραμμα πολλαπλασιάζεται με τον παραπάνω πίνακα K^{-1} – έτσι προκύπτει το αρχικό μήνυμα.

Σύνοψη κρυπτογραφικών αλγορίθμων

- Αποκρυπτογράφηση Hill (συνέχεια)

Έστω ότι λαμβάνουμε το κρυπτογραφημένο μήνυμα ML.

Ποιο είναι το μήνυμα που λάβαμε??

Θα πολλαπλασιάσουμε τον K^{-1} με το διάνυσμα $\begin{pmatrix} 12 \\ 11 \end{pmatrix}$

(αφού το M είναι το 13ο γράμμα και το L το 12ο).

Άρα $$\begin{pmatrix} 3 & 21 \\ 7 & 12 \end{pmatrix}\begin{pmatrix} 12 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} 267 \\ 216 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 8 \end{pmatrix} \bmod 26$$

Συνεπώς, το M αντιστοιχεί στο 8ο γράμμα του αλφαβήτου, δηλαδή το H, και το L αντιστοιχεί στο 9ο γράμμα, δηλαδή το I.

Άρα, η λέξη που εστάλη είναι HI

Σύνοψη κρυπτογραφικών αλγορίθμων

- Αλγόριθμος Playfair με κλειδί τη λέξη CRYPTOGRAPHY.
  - Αρχικά, κατασκευάζουμε τον αντίστοιχο πίνακα: (επιλέξαμε την περίπτωση όπου παραλείπουμε το Q από τον πίνακα, που είναι η συνηθέστερη περίπτωση)

C	R	Y	P	T
O	G	A	H	B
D	E	F	I	J
K	L	M	N	S
U	V	W	X	Z

Σύνοψη κρυπτογραφικών αλγορίθμων

- Playfair (συνέχεια)
  - Στη συνέχεια, «σπάμε» το μήνυμα HELLO σε δυάδες, δηλαδή HE, LX, LO (προσέξτε πως δεν πρέπει ένα ζεύγος να αποτελείται από δύο ίδια γράμματα, συνεπώς επειδή θα σχηματιζόταν το ζεύγος LL παρεμβάλλαμε ένα X ανάμεσα)
- ΠΡΟΣΟΧΗ!! Δεν παρεμβάλλουμε το X ανάμεσα σε οποιοδήποτε ζευγάρι διαδοχικών ίδιων γραμμάτων, παρά μόνο αν το ζευγάρι σχηματίζεται κατά την παραπάνω κατάτμηση της λέξης. Για παράδειγμα, για τη λέξη GOOD, θα είχαμε τα ζευγάρια GO και OD χωρίς κανένα πρόβλημα

C	R	Y	P	T
O	G	A	H	B
D	E	F	I	J
K	L	M	N	S
U	V	W	X	Z

Σύνοψη κρυπτογραφικών αλγορίθμων

- Playfair (συνέχεια)
- Η κρυπτογράφηση γίνεται ως εξής:
- Τα H,E σχηματίζουν ορθογώνιο στον πίνακα, άρα κρυπτογραφούνται στα G,I.
- Τα L,X σχηματίζουν επίσης ορθογώνιο, άρα κρυπτογραφούνται στα N,V.
- Τέλος, τα LO σχηματίζουν ορθογώνιο και αυτά, άρα κρυπτογραφούνται στα K,G
- Συνεπώς, το HELLO γίνεται GINVKG.

C	R	Y	P	T
O	G	A	H	B
D	E	F	I	J
K	L	M	N	S
U	V	W	X	Z

Σύνοψη κρυπτογραφικών αλγορίθμων

- Playfair (Αποκρυπτογράφηση)
- Η αποκρυπτογράφηση γίνεται με ακριβώς την αντίστροφη διαδικασία. Έστω ότι λαμβάνουμε το κρυπτογραφημένο μήνυμα GLGMMRAGDK.
- Τα G,L βρίσκονται στην ίδια στήλη, άρα το καθένα αποκρυπτογραφείται στο γράμμα που βρίσκεται από πάνω του – συνεπώς GL->RE
- Τα G,M σχηματίζουν ορθογώνιο, άρα αποκρυπτογραφούνται σε AL
- Τα M,R σχηματίζουν ορθογώνιο, άρα αποκρυπτογραφούνται σε L,Y.
- Τα A,G είναι στην ίδια γραμμή, άρα το καθένα αποκρυπτογραφείται στο αμέσως προηγούμενό του, συνεπώς AG->GO.
- Τέλος, τα D,K είναι στην ίδια στήλη οπότε το καθένα αποκρυπτογραφείται στο γράμμα που βρίσκεται από πάνω του – με άλλα λόγια, DK -> OD.
- Άρα το αρχικό μήνυμα είναι: REALLY GOOD.

C	R	Y	P	T
O	G	A	H	B
D	E	F	I	J
K	L	M	N	S
U	V	W	X	Z

Σύνοψη

- Οι αλγόριθμοι μετατόπισης (π.χ. του Καίσαρα) και ο γραμμικός αλγόριθμος είναι απλοί αλγόριθμοι αντικατάστασης ή μονοαλφαβητικοί (κι αυτό γιατί ένα γράμμα πάντοτε κρυπτογραφείται στο ίδιο).
- Οι αλγόριθμοι Vigenere, Hill, Playfair είναι πολυαλφαβητικοί αλγόριθμοι αντικατάστασης (ένα γράμμα που εμφανίζεται πολλές φορές στο αρχικό μήνυμα μπορεί να κρυπτογραφείται σε διαφορετικό γράμμα στο παραγόμενο κρυπτόγραμμα)