ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Οικονομικό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής
ΠΜΣ στα Πληροφοριακά Συστήματα

Κρυπτογραφία και Εφαρμογές
Διαλέξεις Ακ. Έτους 2015-2016

Μαρκάκης Ευάγγελος
markakis@aueb.gr

Ντούσκας Θεόδωρος
tntouskas@aueb.gr

Άσκηση (Caesar)

- Κρυπτογραφήστε το παρακάτω κείμενο με τον αλγόριθμο Caesar
  - ✓ This is a secret
- Στη συνέχεια προσπαθήστε να βρείτε το αρχικό κείμενο χρησιμοποιώντας τη συχνότητα εμφάνισης των γραμμάτων
- Στη συνέχεια προσπαθήστε να βρείτε το αρχικό κείμενο χρησιμοποιώντας τη συχνότητα εμφάνισης των γραμμάτων
  - ✓ WREHRUQRWWREH
  - ✓ WHVW IRU GHFUBSW
- Επαληθεύστε το αποτέλεσμα από το Cryptool
- Είδος άσκησης: Ατομική
- Χρόνος προετοιμασίας: 15 λεπτά

Άσκηση (affine cipher)

Plaintext Alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- $e_k(x) = (ax + b) \bmod n$
- *Κρυπτογραφήστε το ακόλουθο μήνυμα χρησιμοποιώντας τα κλειδιά:*
  - ✓ *a=3*
  - ✓ *b=5*
- *Είδος άσκησης: Ατομική*
- *Χρόνος προετοιμασίας: 10 λεπτά*

Άσκηση

- Βρείτε τα x και y

- $15x = 12 \bmod 26$
- $20x = 12 \bmod 26$

- $13x + y = 12 \bmod 37$
- $2x + y = 7 \bmod 37$

Άσκηση (affine cipher)

- Έστω το ακόλουθο ciphertext
  - ✓ FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDK APRKDLYEVLRHHRH
- Βρείτε τα σωστά κλειδιά και αποκρυπτογραφήστε το μήνυμα
- Είδος άσκησης: Ατομική
- Χρόνος προετοιμασίας: 15 λεπτά

Γράμμα	Συχνότητα εμφάνισης (%)	Γράμμα	Συχνότητα εμφάνισης (%)
a	8.167	**n**	6.749
b	1.492	**o**	7.507
c	2.782	**p**	1.929
d	4.253	**q**	0.095
e	12.702	**r**	5.987
f	2.228	**s**	6.327
g	2.015	**t**	9.056
h	6.094	**u**	2.758
i	6.966	**v**	0.978
j	0.153	**w**	2.360
k	0.772	**x**	0.150
l	4.025	**y**	1.974
m	2.406	**z**	0.074

Πίνακας 3.3 Συχνότητα εμφάνισης των γραμμάτων της αγγλικής γλώσσας (Πηγή: Lewand, 2000)

Πιο συχνά γράμματα:
E
T
A
O
i

Άσκηση (Vigenere cipher)

- Έστω το ακόλουθο μήνυμα:
  - ✓ THI SCI PHE RIS CER TAI NLY NOT SEC URE
- Κρυπτογραφήστε το με κλειδί k=DHK
- Επαναλάβετε το ίδιο με τη βοήθεια του Cryptool
- Προσπαθήστε να το μαντέψετε τ κλειδί με τη μέθοδο Kasiski
- Είδος άσκησης: Ατομική
- Χρόνος προετοιμασίας: 15 λεπτά

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

Κρυπτανάλυση του Vigenère Cipher - Μέθοδος Kasiski (1863)

- Στηρίζεται στο γεγονός ότι επαναλαμβανόμενα μοτίβα θα τύχουν κρυπτογράφησης με το ίδιο τμήμα του κλειδιού πάνω από 1 φορά
- Στην ελληνική γλώσσα μοτίβα όπως «στο», «από», «ένα», «του» εμφανίζονται αρκετά συχνά
- Χρησιμοποιούμε συνήθως μοτίβα με τουλάχιστον 3 ή 4 χαρακτήρες που επαναλαμβάνονται τουλάχιστον 3 φορές
- Ο Oscar παρατηρεί κάθε μοτίβο και σημειώνει τις αποστάσεις από την 1η εμφάνιση
- Αν έχουν κρυπτογραφηθεί με το ίδιο τμήμα του κλειδιού, οι αποστασεις πρέπει να είναι 0 (mod m).
- Άρα το μήκος του κλειδιού είναι διαιρέτης των αποστάσεων

```
CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBW
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK
LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX
VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR
ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBI
PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP
WQAIIWXNRMGWOIIFKEE
```

- Το μοτίβο CHR εμφανίζεται 5 φορές στις θέσεις 1, 166, 236, 276, 286
- Αποστάσεις από την 1η εμφάνιση: 165, 235, 275, 285
- gcd = 5
- Υποψήφιο μήκος κλειδιού m = 5
- Κάνουμε 5 μονοαλφαβητικές αποκρυπτογραφήσεις για να ελέγξουμε αν
- όντως m = 5

Κρυπτανάλυση του Vigenère Cipher - Index of Coincidence

- Για ένα string $x = x_1x_2\ldots x_n$ μίας γλώσσας έστω f_i ο αριθμός εμφανισεων του i-οστού γράμματος, i=0,…,25.
- Ορισμός: Ο δείκτης σύμπτωσης (index of coincidence) *Ic(x)* του *x* είναι η πιθανότητα 2 τυχαία γράμματα του *x* να συμπίπτουν

$$I_c(x) = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n-1)}$$

- Έστω pi οι συχνότητες εμφάνισης κάθε γράμματος στην αγγλική γλώσσα. Τότε για ένα σχετικά «τυχαίο» string x της αγγλικής γλώσσας περιμένουμε ότι

Παραδείγματα I

1. Δημιουργία ενός τυχαίου κειμένου.
2. Κρυπτογράφηση του κειμένου που δημιουργήθηκε με την χρήση του κλασσικού αλγόριθμου Caeser. Αποκρυπτογράφηση του κρυπτογραφήματος που προέκυψε.
    1. *Crypt/Decrypt → Symmetric (Classic) → Caesar/Rot-13*
3. Κρυπτογράφηση του αρχικού κειμένου την χρήση του κλασσικού αλγόριθμου XOR. Αποκρυπτογράφηση του κρυπτογραφήματος που προέκυψε.
    1. *Crypt/Decrypt → Symmetric (Classic) → XOR*
4. Κρυπτογράφηση του αρχικού κειμένου την χρήση του συμμετρικού αλγόριθμου RC2. Αποκρυπτογράφηση του κρυπτογραφήματος που προέκυψε.
    1. *Crypt/Decrypt → Symmetric (Modern) → RC2*
5. Κρυπτογράφηση του αρχικού κειμένου με την χρήση του συμμετρικού αλγόριθμου DES (ECB). Αποκρυπτογράφηση του κρυπτογραφήματος που προέκυψε.
    1. *Crypt/Decrypt → Symmetric (Modern) → DES (ECB)*
6. Κρυπτογράφηση του αρχικού κειμένου με την χρήση του συμμετρικού αλγόριθμου DES (CCB). Αποκρυπτογράφηση του κρυπτογραφήματος που προέκυψε.
    1. Crypt/Decrypt → Symmetric (Modern) → DES (CBC)
7. Κρυπτογράφηση του αρχικού κειμένου με την χρήση του συμμετρικού αλγόριθμου AES (self extracting). Αποκρυπτογράφηση του κρυπτογραφήματος που προέκυψε.
    1. Crypt/Decrypt→ Symmetric (Modern) → AES (self extracting)
8. Δημιουργία ενός ασύμμετρου ζεύγους κλειδιών.
    1. *Digital Signatures / PKI → Generate / Import keys*
9. Εμφάνιση των πληροφοριών που σχετίζονται με το ζεύγος που δημιουργήθηκε.
    1. Digital Signatures / PKI → Display / Export keys ..
10. Κρυπτογράφηση του αρχικού κειμένου με την χρήση του ασύμμετρου αλγόριθμου RSA. Αποκρυπτογράφηση του κρυπτογραφήματος που προέκυψε.
    1. *Crypt/Decrypt → Asymmetric → RSA Encryption*
11. Κρυπτογράφηση του αρχικού κειμένου με την χρήση υβριδικής κρυπτογραφίας.
    1. *Crypt/Decrypt → Hybrid → RSA – AES Encryption*
12. Δημιουργία σύνοψης του αρχικού κειμένου (χρήση Συνάρτησης Κατακερματισμού).
    1. *Indiv. Procedures → Hash → Επιλογή Αλγορίθμου – Συνάρτησης κατακερματισμού.*

Παραδείγματα ΙΙ

1. Ψηφιακή υπογραφή του αρχικού κειμένου. Επικύρωση της ψηφιακής υπογραφής.
   1. *Digital Signatures / PKI → Sign Document → ...*
2. Δημιουργία κλειδιού με την χρήση ενός κωδικού.
   1. *Indiv. Procedures → Hash → Key generation from paswd*
3. Συμπίεση του αρχικού κειμένου.
4. Στα πλαίσια του RSA να πραγματοποιηθούν ενέργειες
   - Δημιουργία πρώτων αριθμών.
   - Κρυπτογράφηση και αποκρυπτογράφηση κειμένου.
   - Παραγοντοποίηση ενός αριθμού.
   - Ψηφιακή υπογραφή με χρήση RSA.
5. Δημιουργία ψευδοτυχαίων αριθμών.
6. Πραγματοποίηση ασφαλούς ανταλλαγής κλειδιών με την χρήση του πρωτοκόλλου Diffie-Hellman.
7. Εφαρμογή επίθεσης στις ψηφιακές υπογραφές.
8. Εφαρμογή Brute-Force Ανάλυσης του DES. Πια συμπεράσματα εξάγονται;
9. Πραγματοποιήστε επίθεση παραγοντοποίησης για το modulo 1074775746359965154248021947268736508 01

Άσκηση

- Κρυπτογραφήστε το παρακάτω κείμενο
  - Weak DES Key
- Χρησιμοποιώντας τον αλγόριθμο DES και με κλειδί:
  - ✓ 01 01 01 01 01 01 01 01
  - ✓ Επαναλάβετε τη διαδικασία. Τι παρατηρείτε?

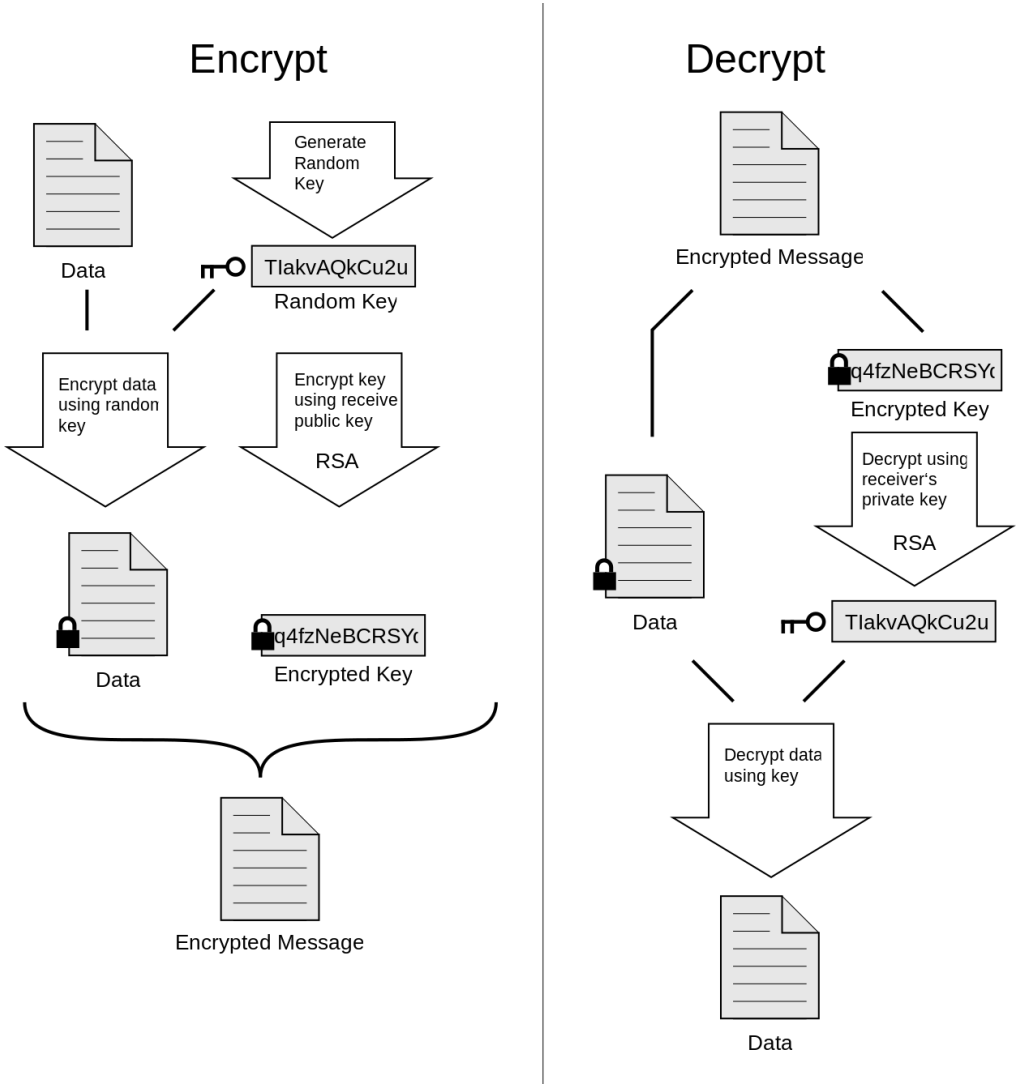
Pretty Good Privacy - PGP

Pretty Good Privacy - PGP

- Μέθοδος κρυπογράφησης και ψηφιακής υπογραφής
- Το PGP είναι ένα υβριδικό πρωτόκολλο κρυπτογράφηση Δημόσιου Κλειδιού.
- Κάνει χρήση και συμμετρικής και ασύμετρης κρυπρογραφίας.
- Δημιουργήθηκε από τον Zimmerman το 1991
- Χρησιμοποιείται για την διακίνηση email και αρχείων στο διαδίκτυο
- Κρυπτογραφικό σύστημα το οποίο επιτρέπει την ανταλλαγή αρχείων με χρήση δημόσιων κλειδιών

Διαφορά PGP – X509 πιστοποιητικών

- Το X509 χρειάζεται αίτηση και έκδοση από μια αρχή πιστοποίησης
- Το PGP μπορεί να δημιουργηθεί άμεσα. Κάθε υποκείμενο μπορεί να γίνει Αρχή Πιστοποίησης για κάποιο άλλο ή για τον ίδιο
- Τα πιστοποιητικά PGP περιέχουν ένα τμήμα δεδομένων και ένα τμήμα υπογραφών


Encrypt
Data
Generate Random Key
TIakvAQkCu2u
Random Key
Encrypt data using randon key
Encrypt key using receive public key
RSA
Data
q4fzNeBCRSY(
Encrypted Key
Encrypted Message
Decrypt
Encrypted Message
q4fzNeBCRSY(
Encrypted Key
Decrypt using receiver's private key
RSA
Data
TIakvAQkCu2u
Decrypt data using key
Data

Πώς λειτουργεί το PGP (Κρυπτογράφηση)

1. Το μήνυμα αρχικά συμπιέζεται->μειώνονται τα patterns
2. Δημιουργείται ένα **session key**
3. Το **Session key** κρυπτογραφεί το μήνυμα χρησιμοποιώντας κάποιον αλγόριθμο (συνήθως 128bits-IDEA)
4. Το κρυπτομήνυμα (ciphertext) δημιουργείται
5. Κρυπτογραφείται το Session key με το δημόσιο κλειδί του παραλήπτη
6. Στέλνεται στον παραλήπτη το κρυπτογραφημένο μήνυμα μαζί με το κρυπτογραφημένο Session key

Πώς λειτουργεί το PGP (Απο-κρυπτογράφηση)

- Αποκρυπτογράφηση του Session Key με το ιδιωτικό κλειδή του παραλήπτη
- Αποκρυπτογράφηση του μηνύματος με το Session Key

Άσκηση

- Δημιουργήστε ένα ζεύγος κλειδιών με τη χρήση του GPG με ημερομηνία λήξης του κλειδιού σας 1 έτος.
- Ανεβάστε το κλειδί (πιστοποιητικό) σας σε κάποιον key server.
- Αναζητήστε και εγκαταστήστε τα κλειδιά των άλλων μελών της ομάδας σας στον υπολογιστή σας (μέσω του GPG). Υπογράψτε τα κλειδιά των άλλων μελών της ομάδας σας με το δικό σας κλειδί. Αλλάξτε το επίπεδο εμπιστοσύνης των κλειδιών αυτών σε έμπιστα.
- Εγκαταστήστε σε έναν mail client της επιλογής σας το δικό σας πιστοποιητικό καθώς και τα πιστοποιητικά των άλλων χρηστών. Ανταλλάξτε μέσω email ένα κρυπτογραφημένο και υπογεγραμμένο μήνυμα.(Υπόδειξη: εγκαταστήστε κάποιο κατάλληλο plugin για τον mail client. Πχ. στον thunderbird μπορείτε να εγκαταστήσετε το πρόσθετο enigmail για τη διαχείριση κλειδιών του openPGP).

Εργαλεία PGP

- Portable PGP
  - ✓ http://ppgp.sourceforge.net/
- GPG4win
  - ✓ http://www.gpg4win.org/
- OpenPGP
  - ✓ http://www.openpgp.org/resources/downloads.shtml
- GO ANYWHERE PGP
  - ✓ http://www.goanywheremft.com/products/openpgp-studio/download

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Οικονομικό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής
ΠΜΣ στα Πληροφοριακά Συστήματα

Κρυπτογραφία και Εφαρμογές
Διαλέξεις Ακ. Έτους 2015-2016

Μαρκάκης Ευάγγελος
markakis@aueb.gr

Ντούσκας Θεόδωρος
tntouskas@aueb.gr