ΤΕΙ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΙΚΑ ΜΑΘΗΜΑΤΑ

ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ(Θ)

Ενότητα 2: ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

ΔΙΔΑΣΚΩΝ: ΚΩΝΣΤΑΝΤΙΝΟΣ ΧΕΙΛΑΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΕ

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

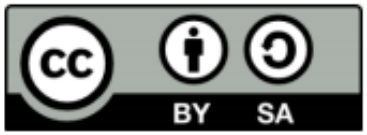
ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.

- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.



Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο ΤΕΙ Κεντρικής Μακεδονίας» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Ενότητα 2

ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

Χειλάς Κωνσταντίνος
Διδάκτορας Φυσικής

Περιεχόμενα ενότητας

1. Ασφάλεια και Δίκτυα
2. Κρυπτολογία (cryptology)
3. Απαιτήσεις κωδίκων
4. Μοντέλο κρυπτογράφησης
5. Η αρχή του Kerckhoff
6. Μια περίληψη της σύγχρονης επιστήμης της κρυπτογραφίας
7. Το πρόβλημα της κρυπτανάλυσης
8. Κώδικες αντικατάστασης
9. Βελτίωση του κώδικα του Καίσαρα
10. Το εύκολο σπάσιμο ενός κώδικα
11. Κώδικες αντιμετάθεσης (transposition ciphers)
12. One-time pads «ένας άσπαστος κώδικας»
13. Μειονεκτήματα
14. Κβαντική κρυπτογραφία

Σκοποί ενότητας

Εισαγωγή στην Κρυπτογραφία

Ασφάλεια και Δίκτυα

- Σε ποιο σημείο της στοίβας πρωτοκόλλων ανήκει η ασφάλεια; Απάντηση: Σε όλα!
  - Φυσικό: κλείδωμα κατανεμητών, σωλήνες αερίου,…
  - Ζεύξης: κρυπτογράφηση: εφαρμόζεται εύκολα
    - Πρόβλημα κατά τη διέλευση από δρομολογητές
  - Δικτύου: έλεγχος πρόσβασης με firewalls
  - Μεταφοράς: κρυπτογράφηση από άκρο σε άκρο
  - Εφαρμογής: ο κύριος χώρος εφαρμογής της αυθεντικοποίησης και της μη-απάρνησης

- Σημαντική μέθοδος για τη βελτίωση της ασφάλειας στα δίκτυα: ΚΡΥΠΤΟΓΡΑΦΗΣΗ

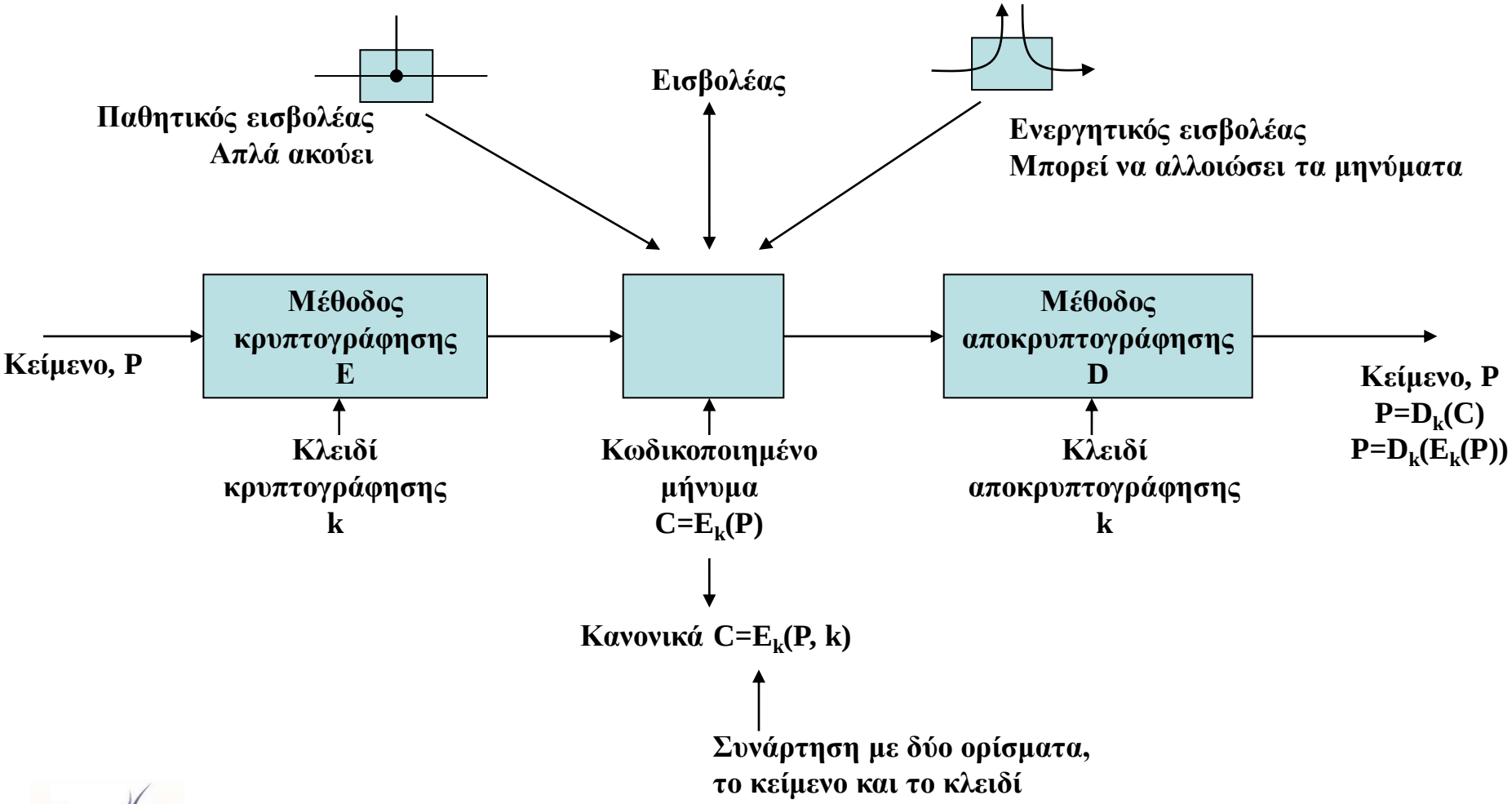
Κρυπτολογία (cryptology)

- Κρυπτογραφία (cryptography) : η τέχνη να κατασκευάζεις κώδικες
- Κρυπτανάλυση (cryptanalysis): η τέχνη να σπας κώδικες
- Κρυπτογραφικοί κώδικες (ciphers): byte προς byte ή bit προς bit μετασχηματισμός ενός μηνύματος ανεξάρτητα από το νόημά του.
- Κώδικες (codes): αντικατάσταση μιας λέξης με κάποια άλλη ή με κάποιο σύμβολο
  - δεν βρίσκονται πλέον σε χρήση
  - WWII: Κώδικας Navajo
- Παραδοσιακοί χρήστες της κρυπτογραφίας
  - Οι στρατιωτικοί
  - Οι διπλωμάτες
  - Οι συγγραφείς ημερολογίων, και
  - Οι εραστές …

Απαιτήσεις κωδίκων

- Να εφαρμόζονται εύκολα
- Τα κλειδιά τους να αλλάζουν εύκολα
- Να είναι απόρθητοι από τους μη-γνώστες
- Να είναι εύκολα αναγνωρίσιμοι από τους χρήστες

Μοντέλο κρυπτογράφησης



Η αρχή του Kerckhoff

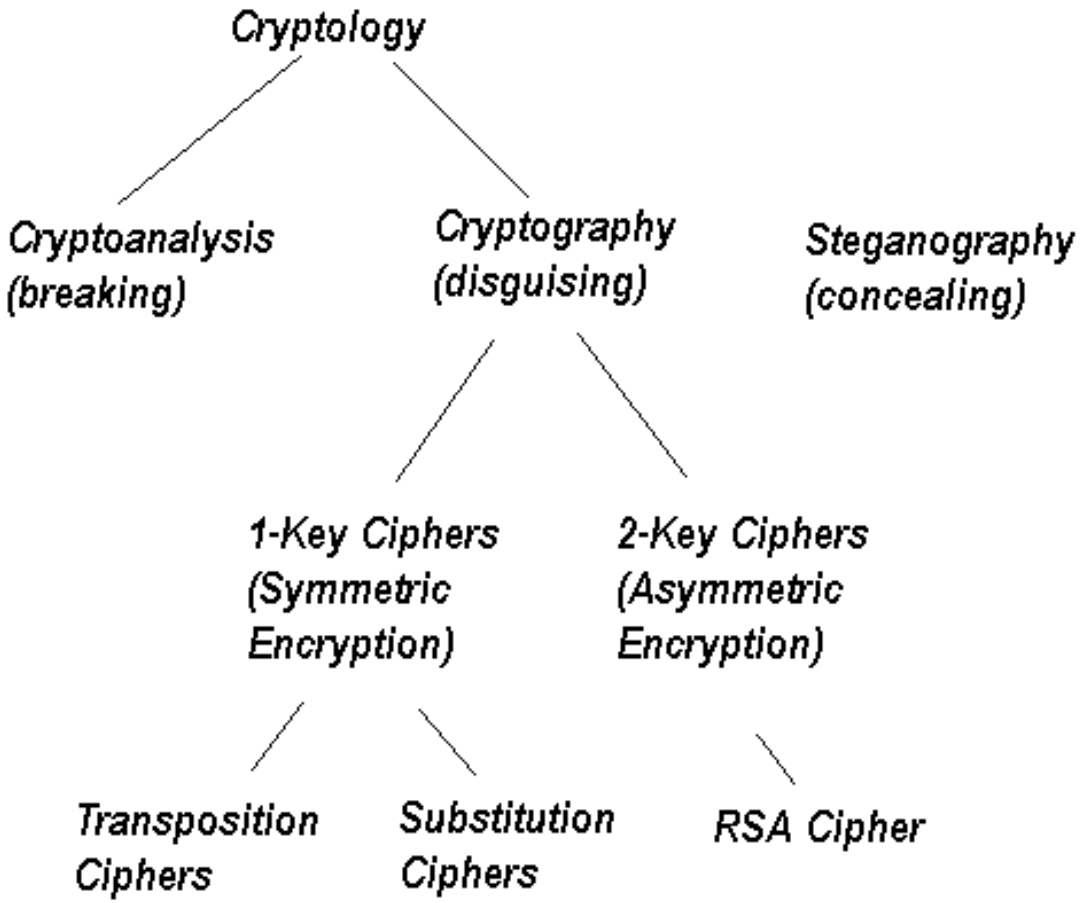
- Φλαμανδός κρυπτογράφος Auguste Kerckhoff (1883)

  (19 January 1835 – 9 August 1903)
- «Όλοι οι αλγόριθμοι πρέπει να είναι δημόσιοι˙ μόνο τα κλειδιά πρέπει να μένουν μυστικά.»
- Η προσπάθεια να κρατήσω μυστικό τον κώδικα είναι μάταιη.
- Επίσης, η κοινοποίηση του κώδικα βοηθά στον έλεγχο της ικανότητάς του από πολλούς ειδικούς.
- Τα κλειδιά πρέπει να αλλάζουν συχνά και να είναι τέτοια ώστε η εύρεσή τους να αποτελεί τη μεγάλη δυσκολία του κώδικα.

Ένα χαρακτηριστικό παράδειγμα

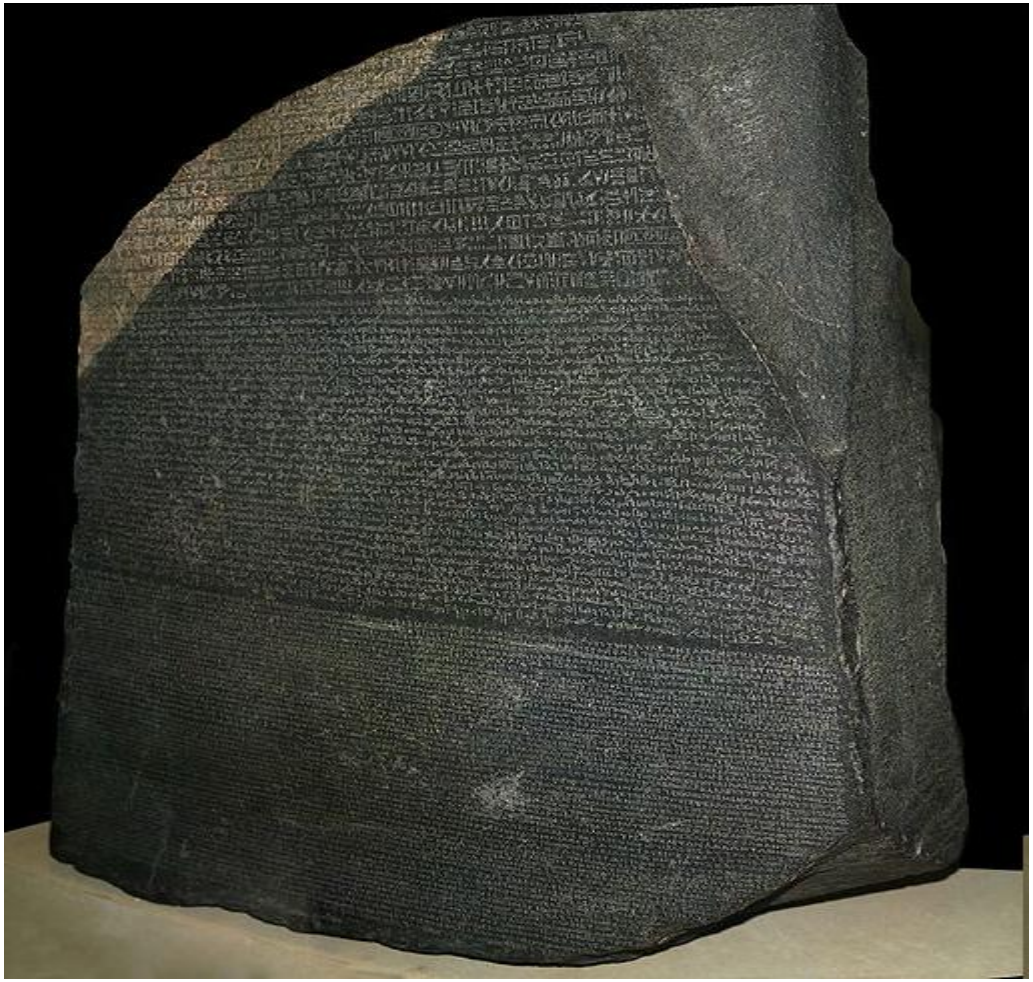
- Οι κλειδαριές με συνδυασμό
- Όλοι ξέρουν πως δουλεύουν
- Αν το κλειδί έχει μήκος 4 ψηφία υπάρχουν 10^4=10.000 συνδυασμοί
- Μέθοδος εξαντλητικής αναζήτησης (exhaustive search).
  - Ο χρόνος εύρεσης εξαρτάται με εκθετικό τρόπο από το μήκος του κλειδιού.
- Η ασφάλεια προκύπτει από έναν ισχυρό (αλλά δημόσιο) αλγόριθμο κι ένα μεγάλο κλειδί.

Μια περίληψη της σύγχρονης επιστήμης της κρυπτογραφίας



Το πρόβλημα της κρυπτανάλυσης

- Ο κρυπταναλυτής βρίσκεται συνήθως αντιμέτωπος μόνο με το κρυπτογραφημένο κείμενο (cyphertext-only)
- Αν έχει ζεύγη απλού και κρυπτογραφημένου κειμένου τότε έχει ένα πρόβλημα γνωστού κειμένου (plaintext-problem)
- Τέλος, αν μπορεί να φτιάξει μόνος του ένα κρυπτογραφημένο κείμενο από δείγματα απλού, τότε έχει το πρόβλημα του επιλεγμένου κειμένου (chosen plaintext problem)



Γράφτηκε το 196 πΧ στα χρόνια του Πτολεμαίου IV.

Ανακαλύφθηκε το 1799 στη Ροζέτα από τον μηχανικό του γαλλικού στρατού Captain Pierre-François Bouchard.

Μελετήθηκε από τον Βρετανό επιστήμονα Thomas Young και τον Γάλλο ακαδημαϊκό Jean-François Champollion.

Το 1822 οδήγησε στην αποκρυπτογράφηση της ιερογλυφικής γραφής.

Κώδικες αντικατάστασης

- Κάθε γράμμα ή ομάδα γραμμάτων αντικαθίσταται από ένα άλλο γράμμα ή ομάδα γραμμάτων για να τα κρύψουμε
- Ο κώδικας του Καίσαρα
  - Αποδίδεται στον Ιούλιο Καίσαρα
  - Το αλφάβητο μετατοπίζεται κατά *k* χαρακτήρες. Το *k* είναι το κλειδί του κώδικα.

Βελτίωση του κώδικα του Καίσαρα

- Μονοαλφαβητική αντικατάσταση (monoalphabetic substitution).

Plaintext: α β γ δ ε ζ η θ ι κ λ μ ν ξ ο π ρ σ τ υ φ χ ψ ω

Cyphertext: Ε Ρ Τ Υ Θ Ι Ο Π Α Σ Δ Φ Γ Η Ξ Κ Λ Ζ Χ Ψ Ω Β Ν Μ

24! Συνδυασμοί = 6 x 10^{23} πιθανά κλειδιά.

- Με διάρκεια δοκιμής 1nsec χρειάζονται 10^{8} έτη για να δοκιμαστούν όλα τα πιθανά κλειδιά.

Το εύκολο σπάσιμο ενός κώδικα

- Στατιστικές ιδιότητες των φυσικών γλωσσών
- Συχνότητα εμφάνισης γραμμάτων: e, t, o, a, n, i, …
- Διγράμματα (digrams): th, in ,er, re, an, …
- Τριγράμματα (trigrams): the, ing, and, ion, …
- Τακτική σπασίματος κώδικα:
  - Βρίσκω τη συχνότητα εμφάνισης των κωδικών γραμμάτων, διγραμμάτων, τριγραμμάτων, κ.α.
  - Τα πιο συχνά κωδικά γράμματα αντιστοιχούν μάλλον στο e και το t.
  - Το πιο συχνό τρίγραμμα είναι μάλλον το tXe, οπότε βρίσκουμε την κωδικοποίηση του h(X).
  - Αν πάλι συναντήσουμε συχνά μια λέξη thYt τότε το Y=a.

- Μια άλλη τακτική είναι να εντοπιστεί μια πολύ πιθανή λέξη ή φράση

Κώδικες αντιμετάθεσης
(transposition ciphers)

- Οι κώδικες αντικατάστασης διατηρούν τη θέση των γραμμάτων αλλά τα αλλοιώνουν (μασκαρεύουν).
- Οι κώδικες αντιμετάθεσης δεν αλλοιώνουν τα γράμματα αλλά αλλάζουν τη θέση τους.
- Το κλειδί πρέπει να είναι μια λέξη στην οποία κάθε γράμμα υπάρχει μια μόνο φορά.

Ένας κώδικας αντιμετάθεσης

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Σπάσιμο κώδικα αντιμετάθεσης

- Καταρχήν πρέπει να ξέρω ότι πρόκειται για κώδικα αντιμετάθεσης.
- Μπορώ να ελέγξω τη συχνότητα εμφάνισης των γραμμάτων που θα ταίριαζε με εκείνη ενός απλού κειμένου.
  - Πρέπει να μαντέψω τον αριθμό των στηλών
  - Βοηθάει αν έχω κάποια εικόνα ή γνώση μιας λέξης μέσα στο κείμενο, π.χ. milliondollars.
  - Βρίσκω διγράμματα και ψάχνω την αλληλουχία. Αν βρω το κλειδί, π.χ. 8, μένει να βρω τη σωστή διάταξη των στηλών.
  - Μπορεί κανείς να δοκιμάσει k(k-1) συνδυασμούς μέχρι να βρει κάποιον του οποίου οι συχνότητες εμφάνισης διγραμμάτων και τριγραμμάτων να ταιριάζουν με εκείνες μιας φυσικής γλώσσας.

One-time pads
«ένας άσπαστος κώδικας»

- Επέλεξε ως κλειδί μια τυχαία ακολουθία από bits με μήκος ίσο με το μήνυμα.
- Μετέτρεψε το μήνυμα σε ακολουθία από bits και εκτέλεσε XOR με το κλειδί.
- Το αποτέλεσμα δεν μπορεί να αποκρυπτογραφηθεί από κανέναν χωρίς το κλειδί.
- Ο λόγος προκύπτει άμεσα από τη θεωρία της πληροφορίας.
  - Επειδή το κλειδί είναι τυχαίο, οποιοδήποτε απλό κείμενο με το ίδιο μήκος είναι το ίδιο πιθανό να είναι το αρχικό. Με άλλα λόγια, σε ένα αρκετά μεγάλο κρυπτογραφημένο κείμενο η πιθανότητα εμφάνισης όλων των γραμμάτων, διγραμμάτων, τριγραμμάτων, κλπ, θα είναι εξίσου πιθανή, δίνοντας μηδενική πληροφορία για το σπάσιμο του κώδικα.

One-time pad

Message 1:	1001001	0100000	1101100	1101111	1110110	1100101	0100000	1111001	1101111	1110101	0101110
Pad 1:	1010010	1001011	1110010	1010101	1010010	1100011	0001011	0101010	1010111	1100110	0101011
Ciphertext:	0011011	1101011	0011110	0111010	0100100	0000110	0101011	1010011	0111000	0010011	0000101
Pad 2:	1011110	0000111	1101000	1010011	1010111	0100110	1000111	0111010	1001110	1110110	1110110
Plaintext 2:	1000101	1101100	1110110	1101001	1110011	0100000	1101100	1101001	1110110	1100101	1110011

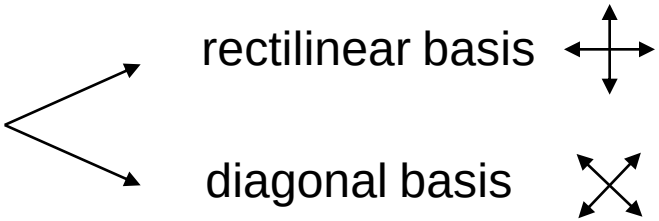
Μειονεκτήματα

- Το κλειδί δεν μπορεί να απομνημονευθεί
- Το μήκος του κειμένου που μπορεί να κρυπτογραφηθεί εξαρτάται από το μήκος του κλειδιού.
- Είναι μέθοδος ευαίσθητη στην απώλεια ή εισαγωγή δεδομένων
- Αν ο αποστολέας και ο δέκτης χάσουν το συγχρονισμό τους τα δεδομένα θα γίνουν ακατάληπτα.

Κβαντική κρυπτογραφία

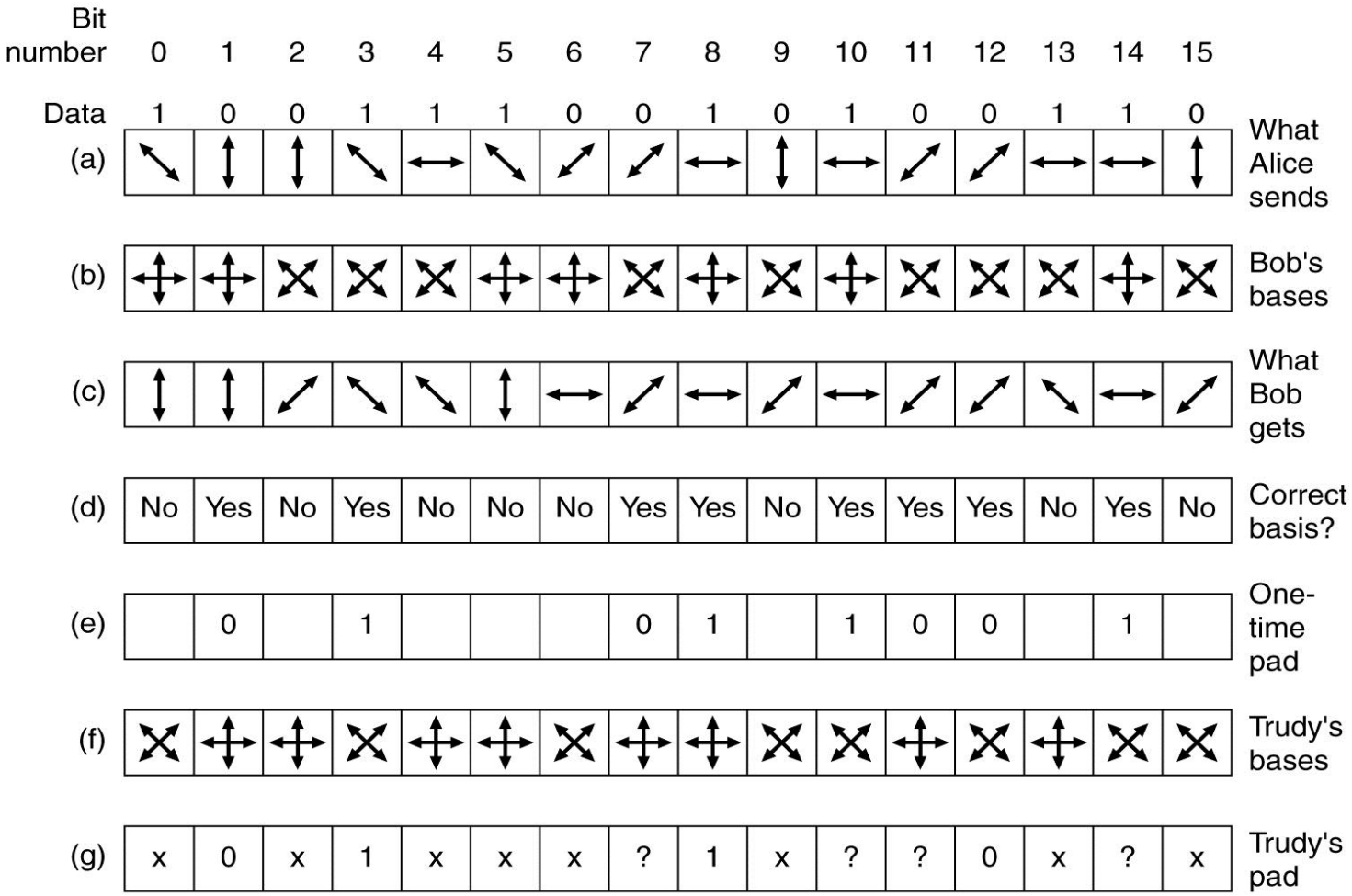
- Το πρωτόκολλο BB84 (Bennet and Brassard 1984)
- Η Alice και ο Bob ονομάζονται principals
- Trudy: intruder

- Φωτόνια → πόλωση



- qubits → bits που αποστέλλονται με φωτόνια
- Αρχή της απροσδιοριστίας –Werner Heisenberg 1927
  - Pockels cell – polarizer
  - κρύσταλλος $CaCO_3$
- privacy amplification

Κβαντική κρυπτογραφία



Βασικές αρχές κρυπτογραφίας

- Πλεονασμός (redundancy)
  - Χρειάζεται και για την κρυπτογράφηση αλλά και για τη διόρθωση σφαλμάτων
- Φρεσκάδα (freshness)
  - Πρέπει να υπάρχει μια μέθοδος που να εντοπίζει τις επανεκπομπές παλαιότερων μηνυμάτων που έχουν σα σκοπό τους να προκαλέσουν σύγχυση στο δέκτη.

Τέλος Ενότητας