Κρυπτογραφία: Εισαγωγή & Ιστορικά συστήματα

Διδασκαλία: Δ. Ζήνδρος

Επιμέλεια διαφανειών:
Δ. Ζήνδρος, Α. Παγουρτζής, Σ. Ζάχος

Στόχοι του σημερινού μαθήματος

- Τι είναι κρυπτογραφία;
- Ορισμοί και ορολογίες
- Ιστορία της κρυπτογραφίας
- xor
- Κωδικοποιήσεις: base64, base58
- Το κρυπτοσύστημα Καίσαρα και rot13
- Κρυπτανάλυση με ανάλυση συχνότητας
- Το κρυπτοσύστημα Vigenère
- Κρυπτανάλυση με δείκτες σύμπτωσης

Τι είναι κρυπτογραφία;

- Τομέας της **επιστήμης των υπολογιστών**
- **Μαθηματικός** κλάδος
- Μελετά τεχνικές **ασφαλών επικοινωνιών**
- Δεδομένου ότι υπάρχουν **αντίπαλοι**
- Σχεδιάζει **πρωτόκολλα** που αμύνονται έναντι αντιπάλων

Γιατί να ασχοληθώ με την κρυπτογραφία;

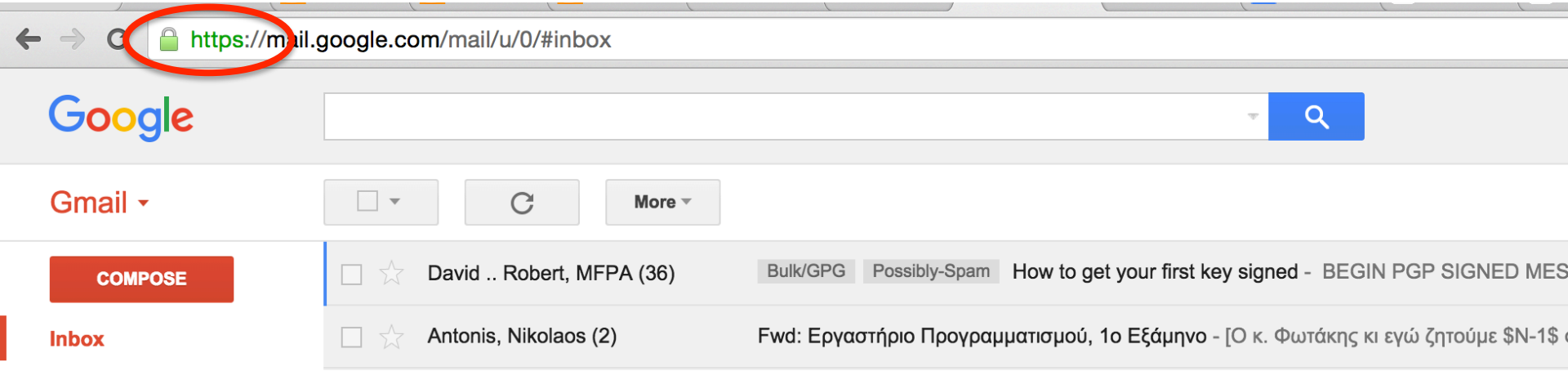
- Έχει θεωρητικό ενδιαφέρον
- Εφαρμόζει μαθηματικά που παραδοσιακά ήταν ανεφάρμοστα
  - π.χ. Θεωρία αριθμών
- Συχνά περιέχει δύσκολες και ενδιαφέρουσες μαθηματικές τεχνικές και περιοχές
  - π.χ. Θεωρία αλγεβρικών καμπυλών

Γιατί να ασχοληθώ με την κρυπτογραφία;

- Έχει πρακτικό ενδιαφέρον
- Είναι γέφυρα που ενώνει την επιστήμη των υπολογιστών με:
  - Τη νομική επιστήμη
  - Τις πολιτικές επιστήμες
  - Τα οικονομικά
- Έχει εφαρμογές που μπορούν να κάνουν τον κόσμο καλύτερο

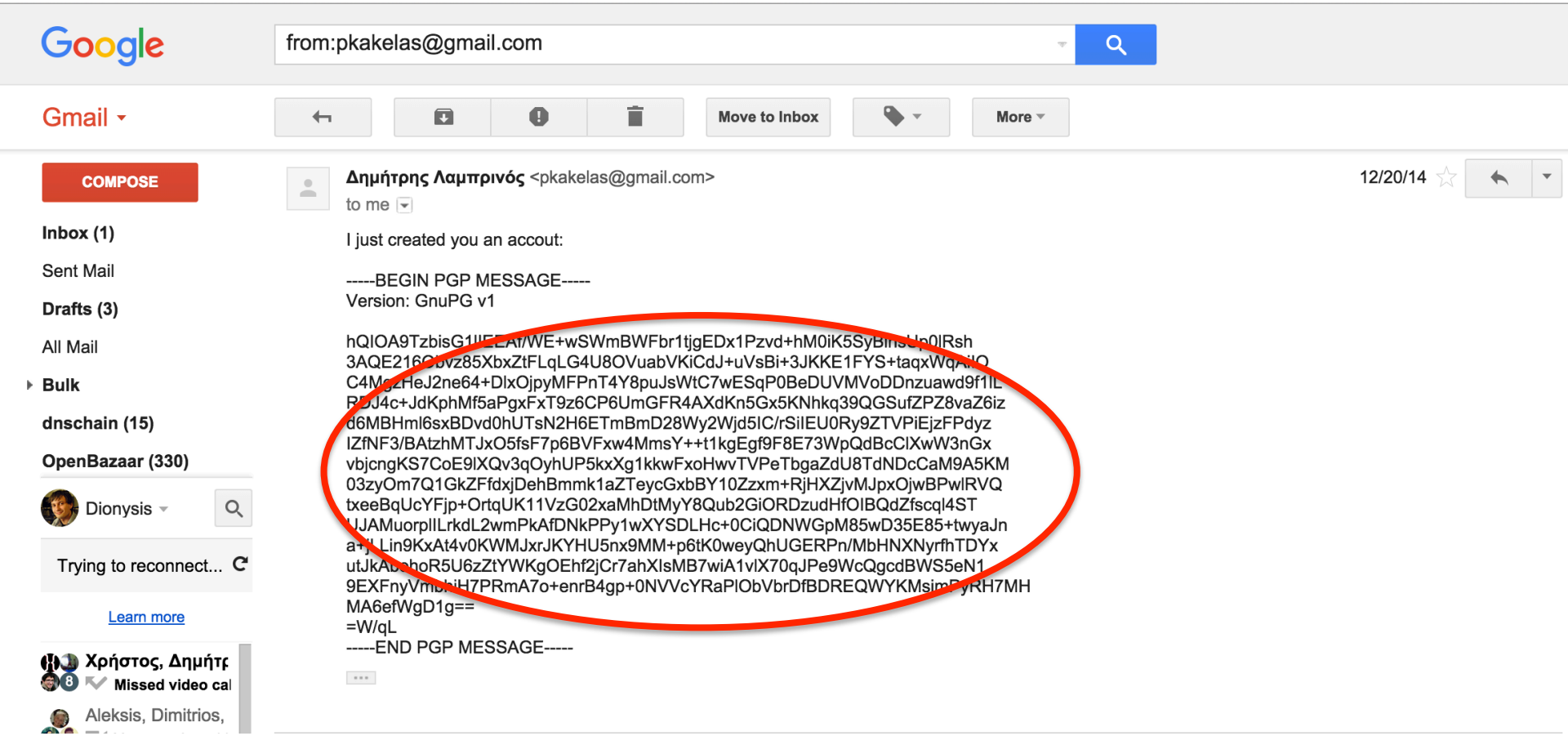
Εφαρμογές της κρυπτογραφίας

- Κρυπτογράφηση στο web



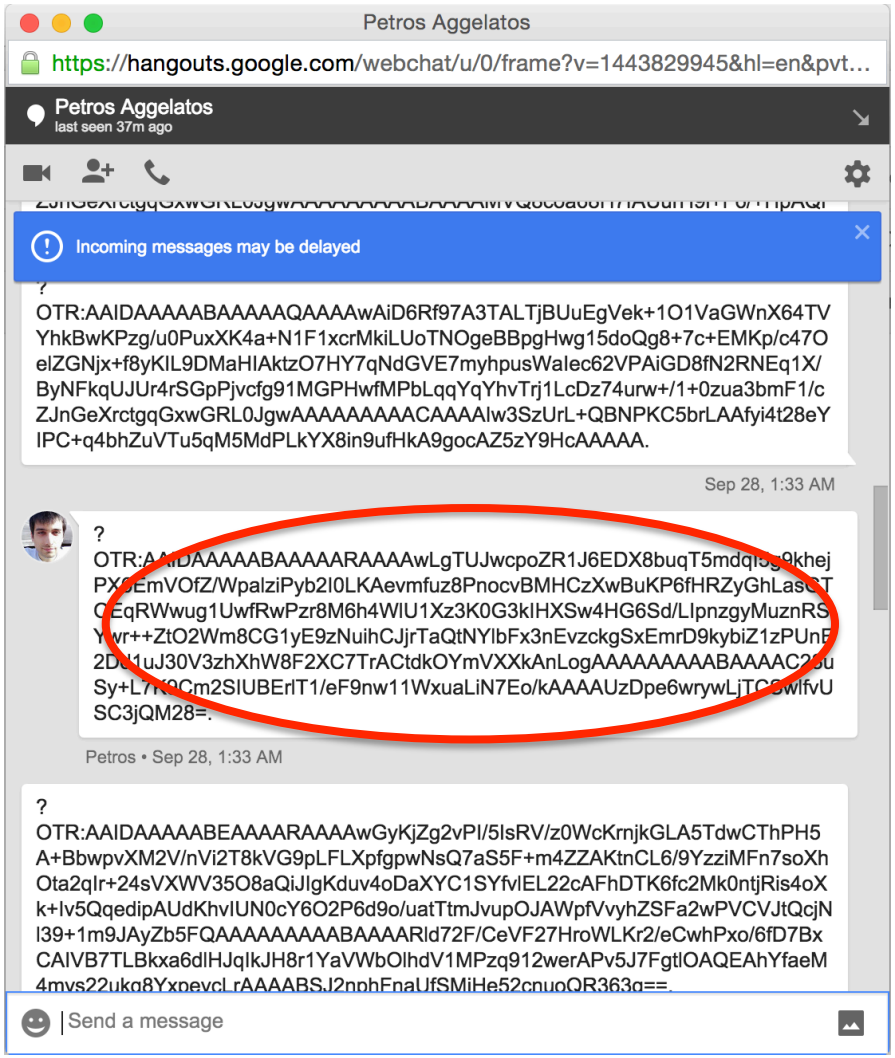
Εφαρμογές της κρυπτογραφίας

- Κρυπτογράφηση e-mail



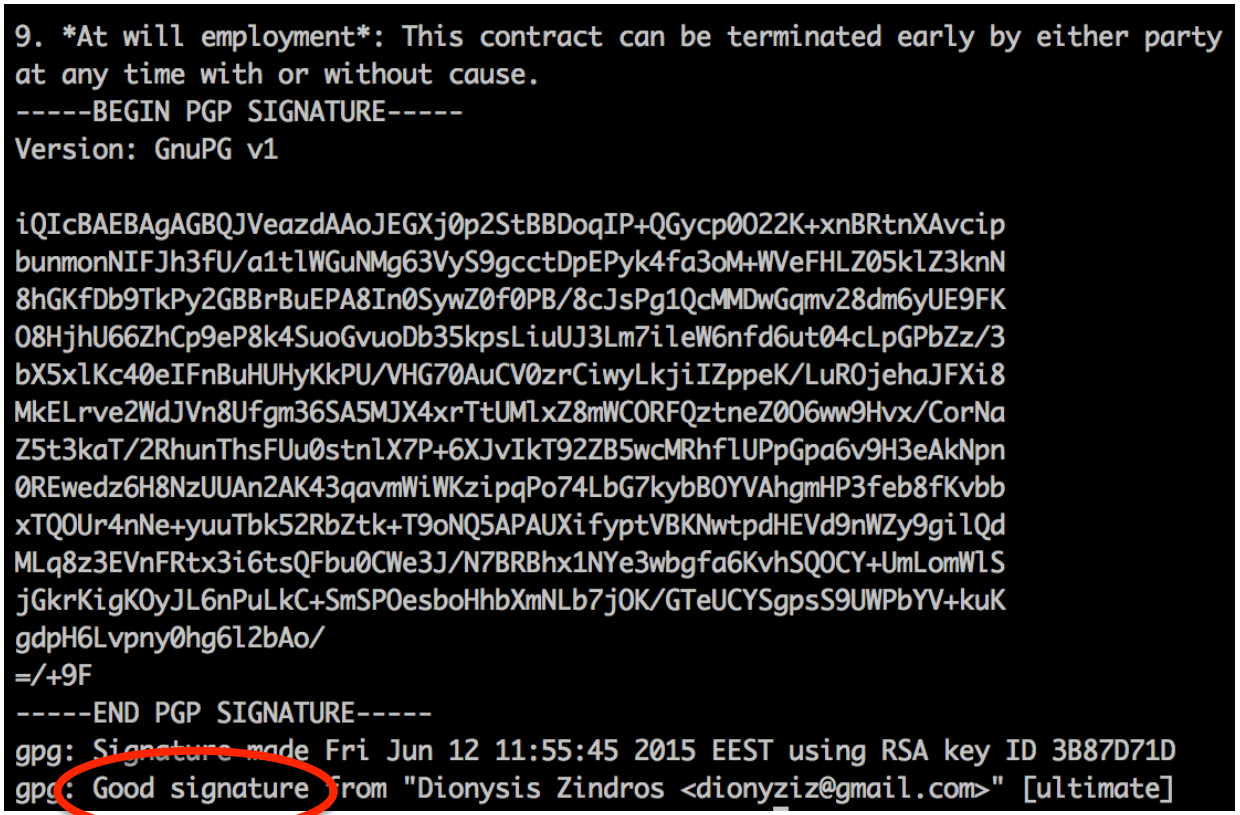
Εφαρμογές της κρυπτογραφίας

- Κρυπτογράφηση chat



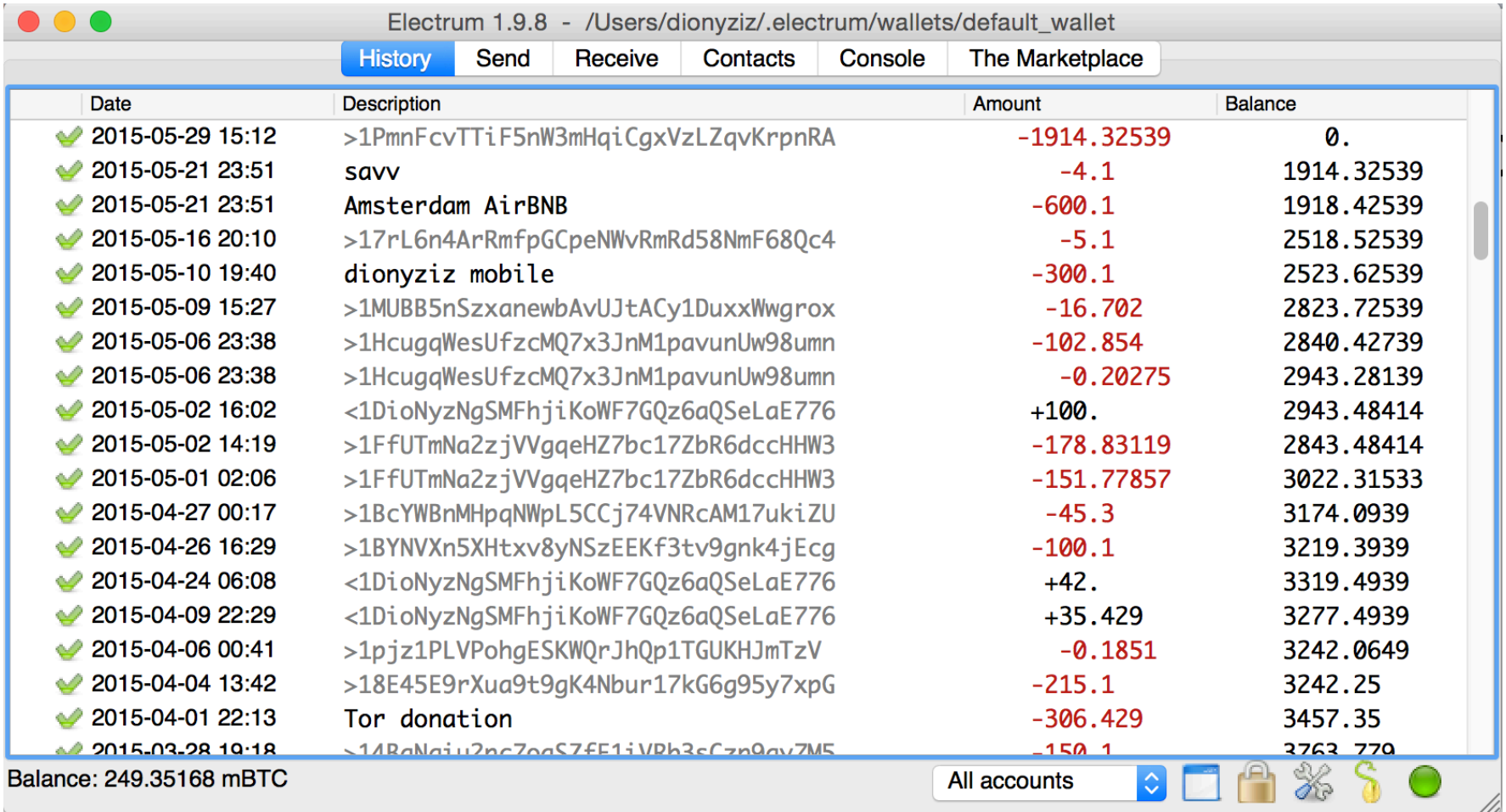
Εφαρμογές της κρυπτογραφίας

- Ψηφιακές υπογραφές
- Ηλεκτρονικά συμβόλαια



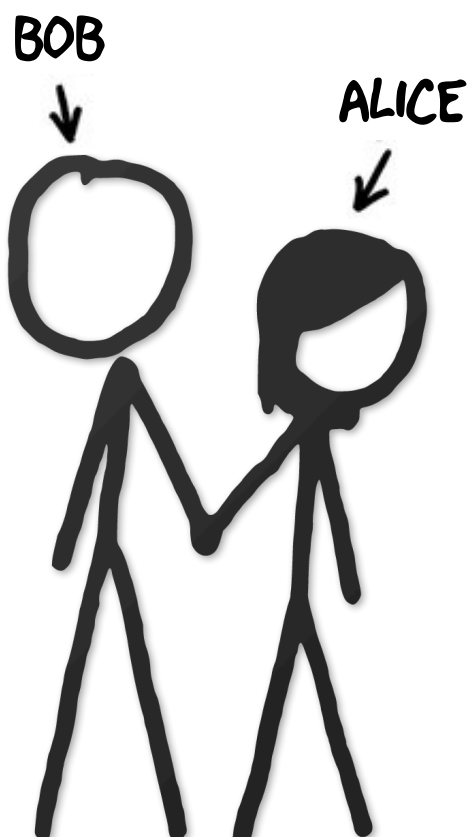
Εφαρμογές της κρυπτογραφίας

- Ηλεκτρονικό χρήμα



Οι πρωταγωνιστές μας

οι καλοί

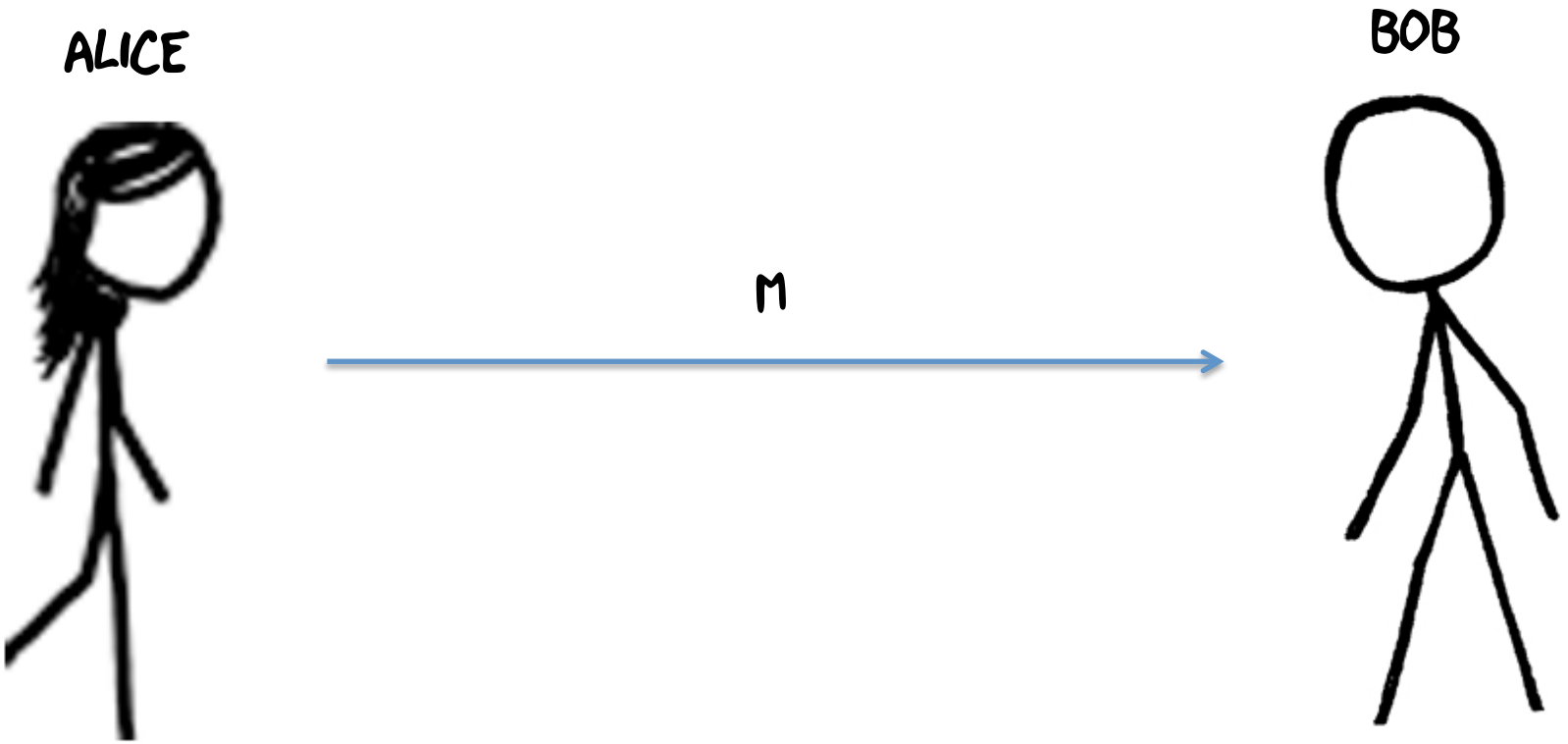


οι κακοί

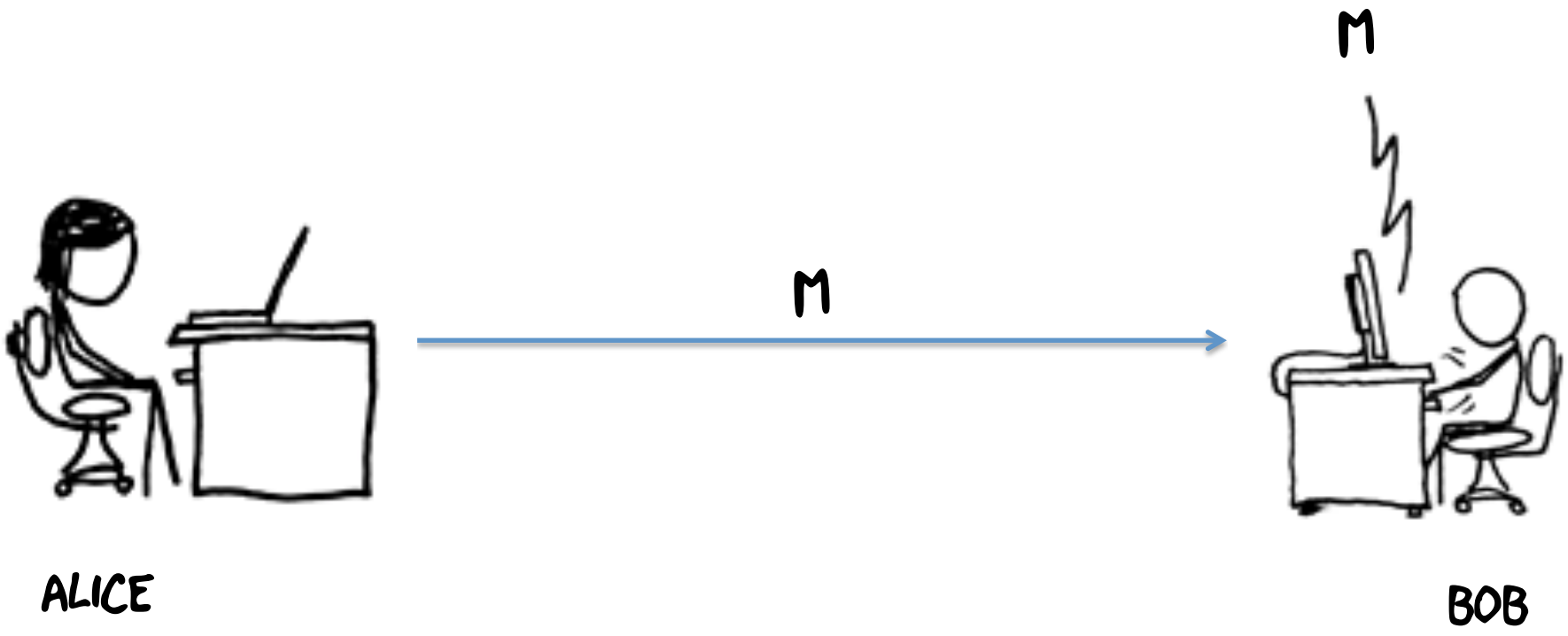
Επικοινωνία

- Η κρυπτογραφία αφορά την ανταλλαγή δεδομένων ανάμεσα σε παίκτες
- Η **Alice** θέλει να στείλει μία εντολή **στην τράπεζά της**
- Η **Alice** θέλει να στείλει ένα προσωπικό chat στον **Bob**
- Η **Alice** θέλει να κρυπτογραφήσει το σκληρό της δίσκο (ένα μήνυμα στον «**εαυτό της στο μέλλον**»)

Επικοινωνία στο δίκτυο



Επικοινωνία στο δίκτυο



Threat model

- Μοντελοποιούμε κατά περίπτωση τη δύναμη του εχθρού μας
- Ρωτάμε πράγματα όπως:
  - Τι δύναμη έχει;
    - Μπορεί να «διαβάσει» το δίκτυο;
    - Μπορεί να «αλλάξει» τα δεδομένα στο δίκτυο;
    - Τι υπολογιστική δύναμη έχει;
  - Τι θέλει να πετύχει;
- Μοντελοποιούμε τις επιθυμίες μας, για παράδειγμα:
  - Θέλουμε να μείνει το μήνυμά μας μυστικό;
  - Θέλουμε να μείνουμε ανώνυμοι;

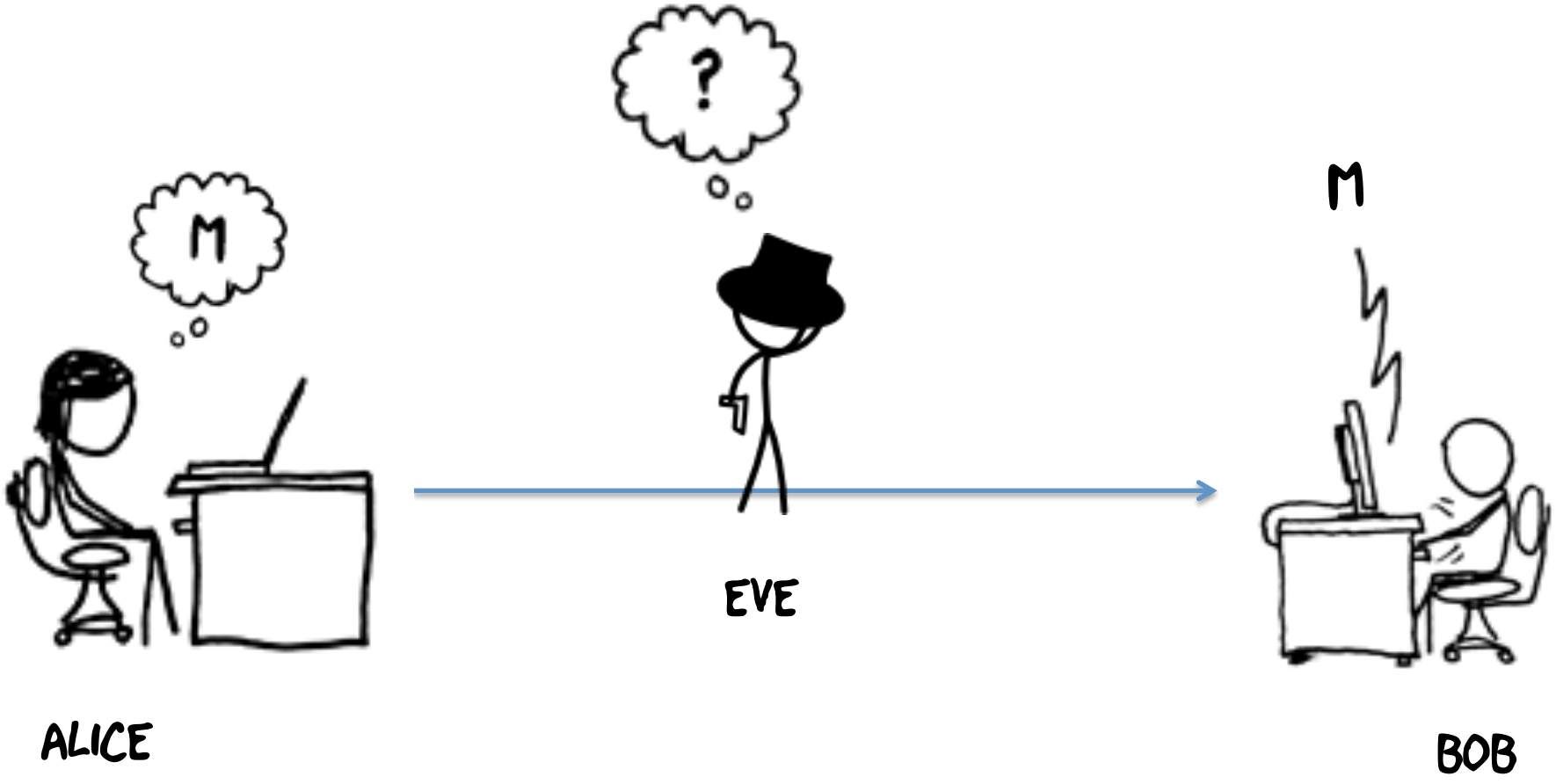
Τι είναι κρυπτογραφία;

- Επιτυγχάνει τα δεδομένα μας να παραμένουν:
  - Ιδιωτικά
  - Ακέραια
  - Πιστοποιημένα
  - (Un)deniable
  - Ανώνυμα
  - Forward secret

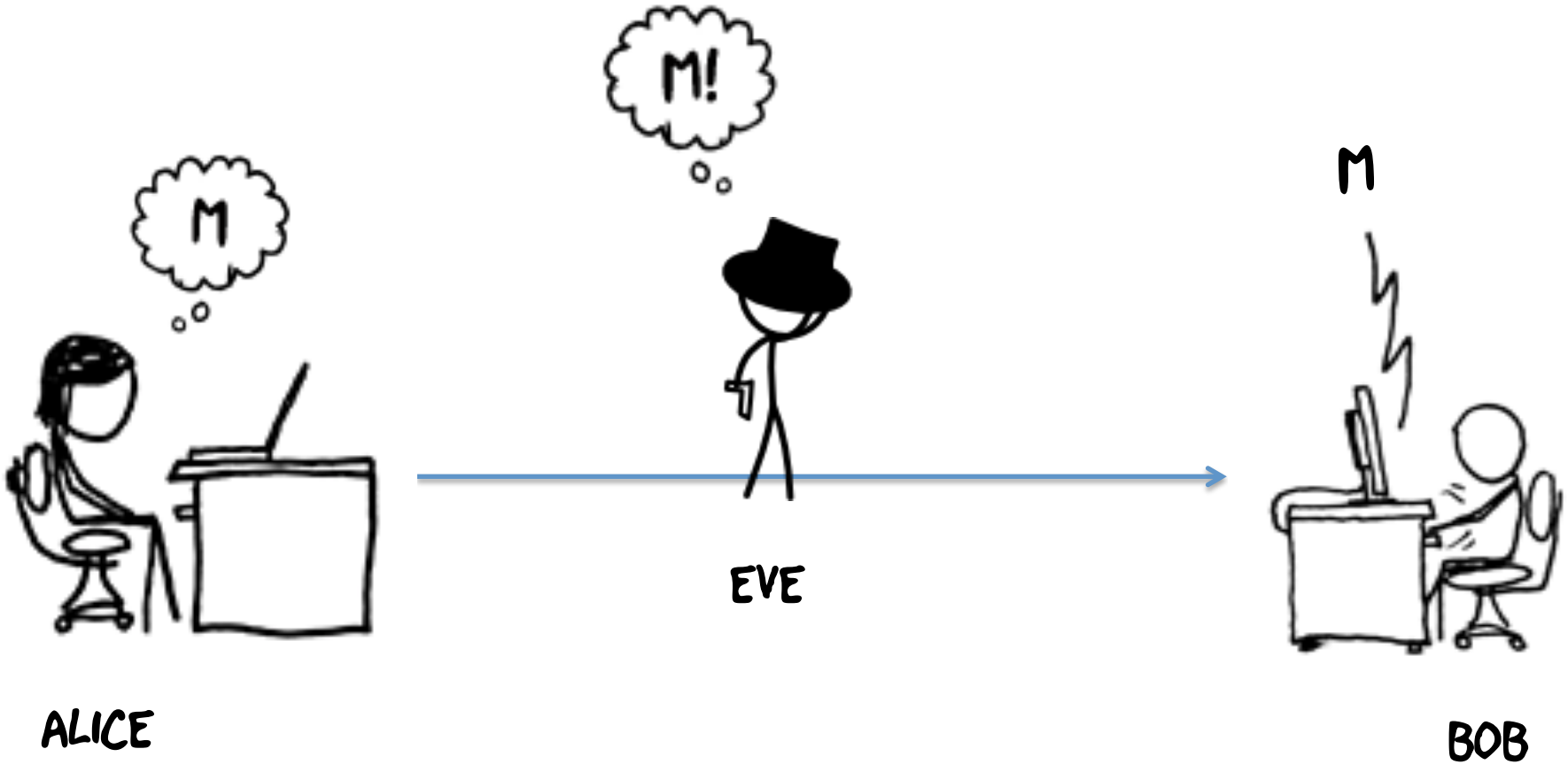
Ιδιωτικότητα (confidentiality)

- Ο αντίπαλος δεν μπορεί να **διαβάσει** τα δεδομένα μας
- Δεν μπορεί να εξάγει κανενός είδους πληροφορία για τα μηνύματά μας
- Η κρυπτογραφία το πετυχαίνει ακόμη και αν ο αντίπαλος μπορεί να διαβάσει **κάθε** πληροφορία στο δίκτυο. Κάθε byte που ανταλλάσσουμε και κάθε ηλεκτρικό σήμα!

Ιδιωτικότητα



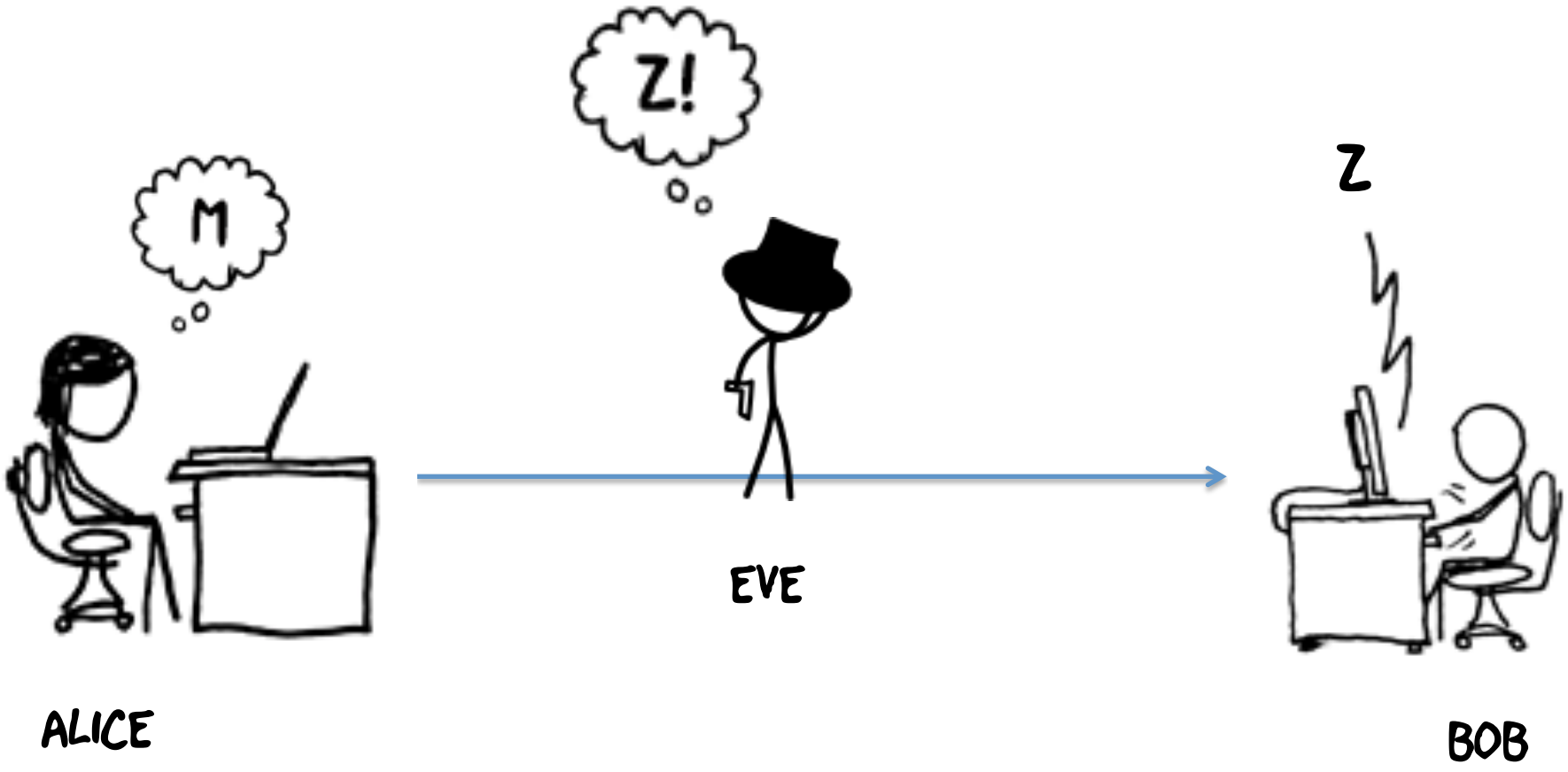
Παραβίαση ιδιωτικότητας



Ακεραιότητα (integrity)

- Ο αντίπαλος δεν μπορεί να **αλλάξει** τα δεδομένα μας
- Η κρυπτογραφία το πετυχαίνει αυτό ακόμη και αν ο αντίπαλος μπορεί να αλλάξει τα bytes στο δίκτυο!

Παραβίαση ακεραιότητας



Πιστοποίηση (authentication)

- Μπορούμε να πιστοποιήσουμε ότι τα δεδομένα τα έστειλε ένας συγκεκριμένος παίκτης
- Η κρυπτογραφία μπορεί να πετύχει end-to-end πιστοποίηση.
  - π.χ. στο GPG ένα email που έρχεται από το Gmail ξέρουμε ότι δεν είναι κάτι ψεύτικο που απλά φτιάχτηκε από τη Google, αλλά πραγματικά το έγραψε αυτός που λέει ότι το έγραψε

Undeniability

- Μπορούμε να αποδείξουμε **σε τρίτους** ότι τα δεδομένα στάλθηκαν από κάποιον συγκεκριμένο παίκτη
- Η κρυπτογραφία μπορεί να πετύχει ψηφιακές υπογραφές σε ένα ηλεκτρονικό συμβόλαιο που «στέκουν» νομικά
  - π.χ. GPG, PKI

Deniability

- Ένας **τρίτος** δεν μπορεί να αποδείξει ότι τα δεδομένα στάλθηκαν από ένα συγκεκριμένο παίκτη
- Το undeniability και το authentication είναι δύο διαφορετικά πράγματα
- Η κρυπτογραφία μπορεί να πετύχει ταυτόχρονα authentication + deniability!
  - π.χ. OTR

Ανωνυμία (Anonymity)

- Η φυσική **πηγή** ή **προορισμός** ενός μηνύματος παραμένουν κρυφά

Forward secrecy

- Η υποκλοπή **μετέπειτα** κλειδιών δεν επιτρέπει την αποκρυπτογράφηση **προηγούμενων** μηνυμάτων

Παράδειγμα ιδιοτήτων

- Η κρυπτογραφία μπορεί να πετύχει ταυτόχρονα:
  - Confidentiality
  - Integrity
  - Authentication
  - Deniability
  - Anonymity
  - Forward secrecy

Παράδειγμα ιδιοτήτων

- Η Alice και ο Bob κάνουν chat
- Confidentiality:
  - Ο ISP (Forthnet, OTE) δεν μπορεί να δει τι λένε
- Integrity:
  - Ο ISP δεν μπορεί να αλλάξει λέξεις στα μηνύματά τους επιλεκτικά
- Authentication:
  - Το Facebook δεν μπορεί να στείλει ψεύτικα μηνύματα στην Alice προσποιούμενο ότι ήρθαν από τον Bob

Παραδείγματα ιδιοτήτων

- Deniabilty:
  - Αν αργότερα η δίωξη ηλεκτρονικού εγκλήματος αναγκάσει τον Bob και την Alice να παραδώσουν τα κλειδιά τους, κανείς δεν μπορεί να αποδείξει ότι πράγματι ήταν **εκείνοι** που έγραψαν αυτά τα μηνύματα
- Anonymity:
  - Η Alice δεν μπορεί να εντοπίσει την φυσική τοποθεσία του Bob και αντίστροφα

Παραδείγματα ιδιοτήτων

- Forward secrecy:
  - Αν η Eve υποκλέψει τα κλειδιά του Bob σήμερα, δεν μπορεί να διαβάσει τα χθεσινά μηνύματα που αντάλλαξε με την Alice
- Ο συγκεκριμένος συνδυασμός επιτυγχάνεται:
  - OTR chat μέσω Facebook πάνω από Tor

Διάλλειμα

Βασικοί όροι

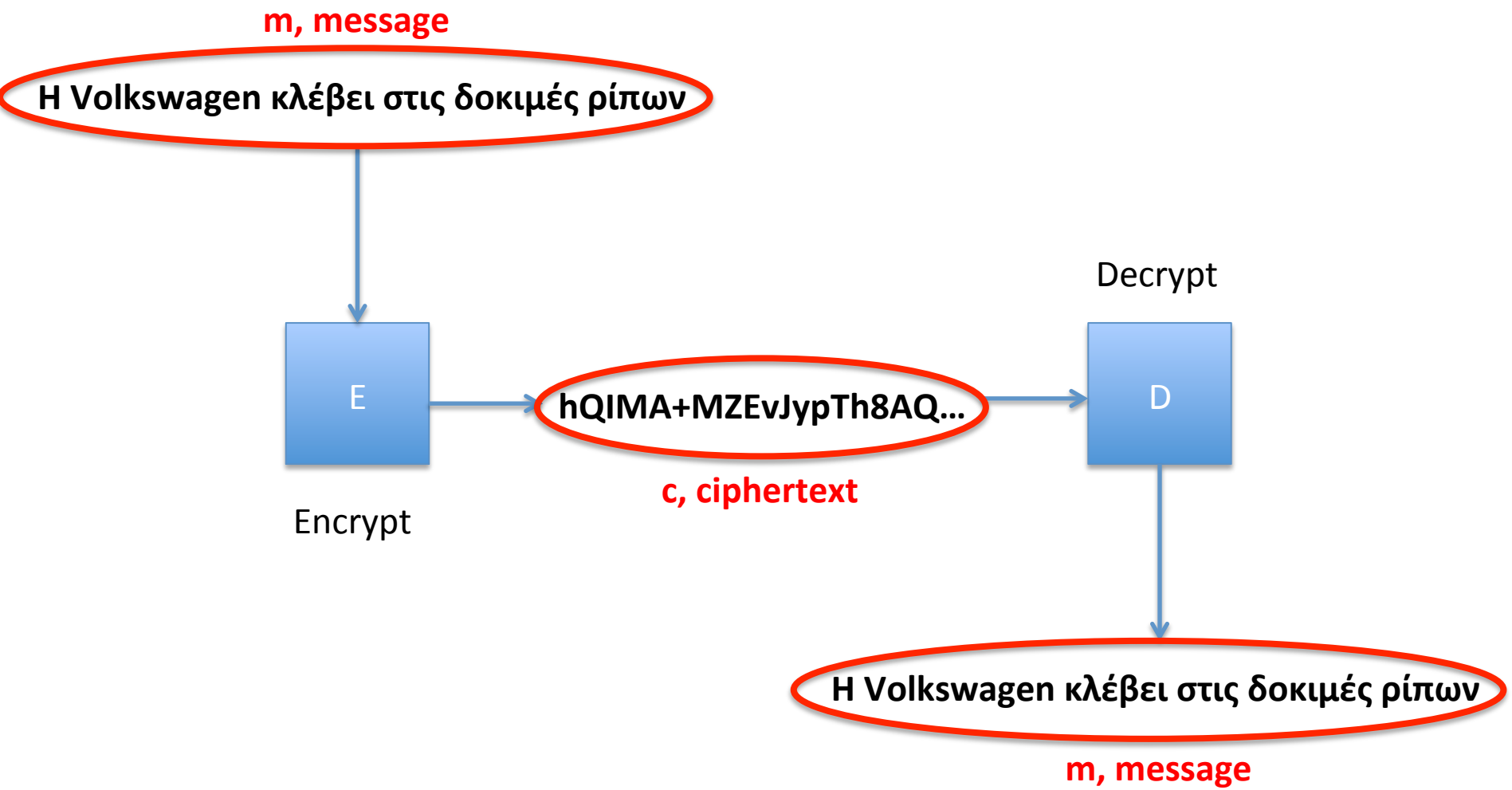
- m: message (plaintext)
  - Το αρχικό ακρυπτογράφητο μήνυμα
- c: ciphertext
  - Το κρυπτογραφημένο μήνυμα
- Η ανταλλαγή μηνυμάτων περνάει από 2 συναρτήσεις
- E: Συνάρτηση encrypt, τρέχει **πριν την αποστολή** του μηνύματος
- D: Συνάρτηση decrypt, τρέχει **μετά την λήψη** του μηνύματος

Εξίσωση ορθότητας

$c = E(m)$

$m = D(c)$

$D(E(m)) = m$


m, message
Η Volkswagen κλέβει στις δοκιμές ρίπων
E
Encrypt
hQIMA+MZEvJypTh8AQ…
c, ciphertext
Decrypt
D
Η Volkswagen κλέβει στις δοκιμές ρίπων
m, message

Κρυπτογραφία και Στεγανογραφία

- **Κρυπτογραφία**: Ασχολείται με την απόκρυψη ενός μηνύματος με ισχυρούς, μαθηματικά αποδείξιμους τρόπους, χωρίς να κρύβεται η ύπαρξη του μηνύματος ή ο τρόπος κρυπτογράφησης.
- **Στεγανογραφία**: Αποκρύπτει ένα μήνυμα κρύβοντας την **ύπαρξή** του από τον αντίπαλο. Ο τρόπος στεγανογράφησης συχνά παραμένει μυστικός.

Τι συστήματα στεγανογραφίας μπορείτε να σκεφτείτε;

Κωδικοποίηση και Κρυπτογράφηση

- **Κωδικοποίηση**: Η αλλαγή της μορφής ενός μηνύματος για λόγους συμβατότητας, χωρίς σκοπό την ιδιωτικότητα. Δεν αμύνεται έναντι αντιπάλων.
- **Κρυπτογράφηση**: Η αλλαγή ενός κειμένου με σκοπό να κρύψουμε τα περιεχόμενά του από έναν αντίπαλο.

Τι συστήματα κωδικοποίησης μπορείτε να σκεφτείτε;

yva lnjrp bq cny qrbpbcg, eky gxrrnobcg bcyn x cal yjxcqcxybncxr pwqynobx. yvbq paharnodacy vxq cny eaac ojnoajrw jaungcbfap nkyqbpa ns cxybncxr qaukjbyw ubjuraq. by vxq eaac vbppac ew qaujauw, undoraibyw xcp quxra. yva bcyajcay, nkj gjaxyaqy ynnr ns adxcuboxybnc, vxq eaac yjxcqsnjdap bcyn yva dnqy pxcgajnkq sxubrbyxynj ns ynyxrbyxjbxcbqd la vxha ahaj qaac. yva bcyajcay bq x yvjaxy yn vkdxc ubhbrbfxybnc.

yvaqa yjxcqsnjdxybncq vxha unda xenky qbracyrw, eauxkqa yvnqa lvn zcnl lvxy bq gnbcg nc lnjz bc yva grnexr qkjhabrrxcua bcpkqyjw xcp vxha cn bcuacybhaq yn qoaxz nky. rasy yn byq nlc yjxtauynjw, lbyvbc x sal waxjq, grnexr ubhbrbfxybnc lbrr ea x onqydnpajc qkjhabrrxcua pwqynobx, sjnd lvbuv aquxoa snj xrr eky yva dnqy qzbrrap bcpbhbpkxrq lbrr ea bdonqqbera. bc sxuy, la dxw xrjaxpw ea yvaja.

lvbra dxcw ljbyajq vxha uncqbpajap lvxy yva bcyajcay daxcq snj grnexr ubhbrbfxybnc, yvaw xja ljncg. yvaw xja ljncg eauxkqa yvaw pn cny vxha yva qacqa ns oajqoauybha yvxy pbjauy aioajbacua ejbcgq. yvaw xja ljncg eauxkqa yvaw vxha cahaj day yva acadw

yvbqbqyvaoxgawnkxjarnnzbcgsnj/enckq/ww2r9rs7

Συστήματα κωδικοποίησης

- **base64**: Μετατρέπει ένα κείμενο όπου κάθε ψηφίο του είναι ένα byte (βάση 256) σε βάση 64 όπου τα ψηφία είναι τα ακόλουθα:
  - A-Z (26 ψηφία)
  - a-z (26 ψηφία)
  - 0-9 (10 ψηφία)
  - “+”, “/” (2 ψηφία)

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Συστήματα κωδικοποίησης

- **base64**: Χρησιμοποιείται για να ανταλλάξει binary μέσω συστημάτων που υποστηρίζουν μόνο απλό κείμενο
- Πώς μοιάζει: SGVsbG8gTlRVQSE=

Συστήματα κωδικοποίησης

- **base58**: Παρόμοιο με το base64
- Λείπουν οι εξής χαρακτήρες:
  - 0 (μηδέν)
  - O (κεφαλαίο ο)
  - I (κεφαλαίο i)
  - l (πεζό L)
- Έχει τον ίδιο σκοπό με το base64, αλλά είναι εύκολο να το διαβάσει άνθρωπος

xor

- “The XOR gate is the only one used throughout all cryptography”
- Βασική συνάρτηση που θα χρησιμοποιήσουμε πολύ

xor

- Binary:
  - $0 \oplus 0 = 0$
  - $0 \oplus 1 = 1 \oplus 0 = 1$
  - $1 \oplus 1 = 0$
- Bitwise:
  - Γράφουμε τους δύο αριθμούς σε bits και εφαρμόζουμε binary xor ανά bit

xor

- $172 \oplus 99 = 207$

$$(172)_{10} = (10101100)_2$$
$$(99)_{10} = (01100011)_2$$
$$(207)_{10} = (11001111)_2$$

xor

- Αντιμεταθετικότητα
  - $x \oplus y = y \oplus x$
- Προσεταιριστικότητα
  - $x \oplus (y \oplus z) = (x \oplus y) \oplus z$
- Απορροφητικότητα
  - $x \oplus x = 0$
- Ουδέτερο στοιχείο
  - $x \oplus 0 = x$
- Άρα:
  - $(x \oplus y) \oplus y = x$

Συμμετρική κρυπτογραφία

- Η Alice θέλει να στείλει ένα μήνυμα στον Bob
- Αρχικά, η Alice και ο Bob συναντιούνται και ανταλλάσσουν ένα κοινό **μυστικό κλειδί** s (secret)
- Το s **πρέπει να μείνει κρυφό**
- Στη συνέχεια χρησιμοποιούν το s για να επικοινωνήσουν
- Προς το παρόν η ανταλλαγή του s δε θα μας απασχολήσει

Ορθότητα συμμετρικής κρυπτογραφίας

$c = E(m, s)$

$m = D(c, s)$

$D(E(m, s), s) = m$

Κρυπτανάλυση

- Η δυνατότητα ενός εχθρού **να μάθει το plaintext χωρίς να γνωρίζει το μυστικό κλειδί**
- Η δυνατότητα ενός εχθρού **να μάθει το μυστικό κλειδί** όταν έχει άλλα δεδομένα
- Θέλουμε να σχεδιάσουμε συστήματα που να μην επιδέχονται κρυπτανάλυση

Η αρχή του Kerckhoff

- Υποθέστε ότι ο εχθρός σας **έχει τον πηγαίο σας κώδικα**
- Οι **συναρτήσεις E** και **D** είναι γνωστές από τον αντίπαλο
- Υποθέστε ότι οι **αλγόριθμοι** κρυπτογράφησης και αποκρυπτογράφησης είναι δημοσιευμένοι
- Το μόνο που μπορεί να είναι **μυστικό είναι το κλειδί**
  - Αν υποκλαπούν, τα κλειδιά αλλάζουν εύκολα
  - Οι αλγόριθμοι όχι

Η αρχή του Kerckhoff

- Τα κρυπτοσυστήματα πρέπει να μην επιδέχονται κρυπτανάλυση **ακόμη** και υπό αυτές τις συνθήκες
- Όταν αναλύουμε την ασφάλεια ενός συστήματος, υποθέτουμε ότι ο τρόπος λειτουργίας του συστήματος είναι γνωστός στον αντίπαλο

Τι δύναμη μπορεί να έχει ο αντίπαλος;

- Διαθέτει **το ciphertext**? (Ciphertext attack)
- Διαθέτει κάποια **ζεύγη plaintext - ciphertext**? (Plaintext attack)
- Διαθέτει τη δυνατότητα να κρυπτογραφήσει **κείμενα της επιλογής** του με το μυστικό κλειδί? (Chosen plaintext)
- Διαθέτει τη δυνατότητα να **αποκρυπτογραφήσει κείμενα της επιλογής του** με το μυστικό κλειδί? (Chosen ciphertext)
  - (εκτός από το κείμενο που τον ενδιαφέρει)
- Διαθέτει τη δυνατότητα να **κρυπτογραφήσει το μυστικό μαζί** με κάποιο κείμενο της επιλογής του? (Partially-chosen plaintext)
- Πιο αυστηροί ορισμοί γι' αυτά την Παρασκευή

Τι συστήματα κρυπτογραφίας μπορείτε να σκεφτείτε;

Μετάθεση

- Παραδοσιακά κρυπτοσυστήματα
- Τα γράμματα στο κείμενο αλλάζουν σειρά

Συμμετρική κρυπτογραφία με σκυτάλη

- Παράδειγμα συστήματος μετάθεσης
- Αρχαία Σπάρτη
- Για στρατιωτικούς σκοπούς
- Το κλειδί είναι 2 ίδιες σκυτάλες

Κρυπτογράφηση με σκυτάλη

- c = E(m = μυστικό κείμενο, s = σκυτάλη):
  - Τυλίγουμε το χαρτί γύρω από τη σκυτάλη
  - Γράφουμε μήνυμα
  - Ξετυλίγουμε
- m = D(c = χαρτί, s = σκυτάλη):
  - Τυλίγουμε το χαρτί γύρω από τη σκυτάλη
  - Διαβάζουμε το μήνυμα

S E C U R I T Y C A N
Y B E A M Y T H O S
Y Y O U S P O K E N

Κρυπτογράφηση σε στήλες

E:

- Γράφουμε το κείμενό μας σε ένα πίνακα οριζόντια
- Διαβάζουμε τις στήλες με σειρά που δίνεται από το κλειδί

D:

- Επανατοποθετούμε το κείμενο στις στήλες με βάση το κλειδί
- Διαβάζουμε το κείμενο στον πίνακα οριζόντια

Κρυπτογράφηση σε στήλες

6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E Q K J E U

EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE

Αντικατάσταση

- Παραδοσιακά κρυπτοσυστήματα
- Αντικαθιστά κάθε γράμμα του κειμένου με κάποιο άλλο
- Διατηρεί τις θέσεις των γραμμάτων
- **Μονοαλφαβητικά**:
  - Το ίδιο γράμμα αντικαθίσταται πάντα με το ίδιο άλλο
- **Πολυαλφαβητικά**
  - Το ίδιο γράμμα μπορεί να αντικατασταθεί με διαφορετικά γράμματα, ανάλογα τη θέση

Καίσαρα

- Μονοαλφαβητικό σύστημα αντικατάστασης
- Κάθε γράμμα αντικαθίσταται με το s-οστό επόμενό του στο αλφάβητο
- Αν ξεπεράσουμε το αλφάβητο, γυρνάμε στην αρχή
- π.χ. s = 3
  - `A -> D`
  - `B -> E`
  - `C -> F`
  - `Z -> C`

rot13

- Ιδιαίτερη περίπτωση στο κρυπτοσύστημα Καίσαρα
- Το κλειδί είναι s = 13
- Έχει την ιδιότητα ότι στα Αγγλικά
  - E(13, m) = D(13, m)
  - Διότι 13 + 13 = 26, το μήκος του αλφαβήτου
- Χρησιμοποιείται στο Internet συχνά για να κρύψει μία λύση σε κάποιο γρίφο (όπως τα περιοδικά που δείχνουν τη λύση ανάποδα)

Πώς μπορούμε να κρυπταναλύσουμε το σύστημα Καίσαρα;

Κρυπτανάλυση με brute-force

- Δοκιμάζουμε όλα τα πιθανά κλειδιά
- Στην περίπτωση του Καίσαρα είναι 26
- Επιχειρούμε να αποκρυπτογραφήσουμε με κάθε κλειδί
- Το σωστό κλειδί δίνει ένα κείμενο που βγάζει νόημα στη γλώσσα που είναι γραμμένο

Γενική αντικατάσταση

- Το κλειδί είναι ένας αυθαίρετος χάρτης αντικατάστασης
- Κάθε γράμμα μπορεί να αντικαθίσταται από οποιοδήποτε άλλο
- Πρόκειται για μία ‘1 - 1’ συνάρτηση
  [A-Z] -> [A-Z]
- Μονοαλφαβητικό σύστημα

Γενική αντικατάσταση

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

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

Πόσα πιθανά κλειδιά υπάρχουν;

$26! = 403291461126605635584000000 = 2^{88}$

- Αδύνατο να κρυπταναλυθεί με brute force
  - ακόμη και από υπολογιστή
- Πώς θα μπορούσαμε να το κρυπταναλύσουμε;

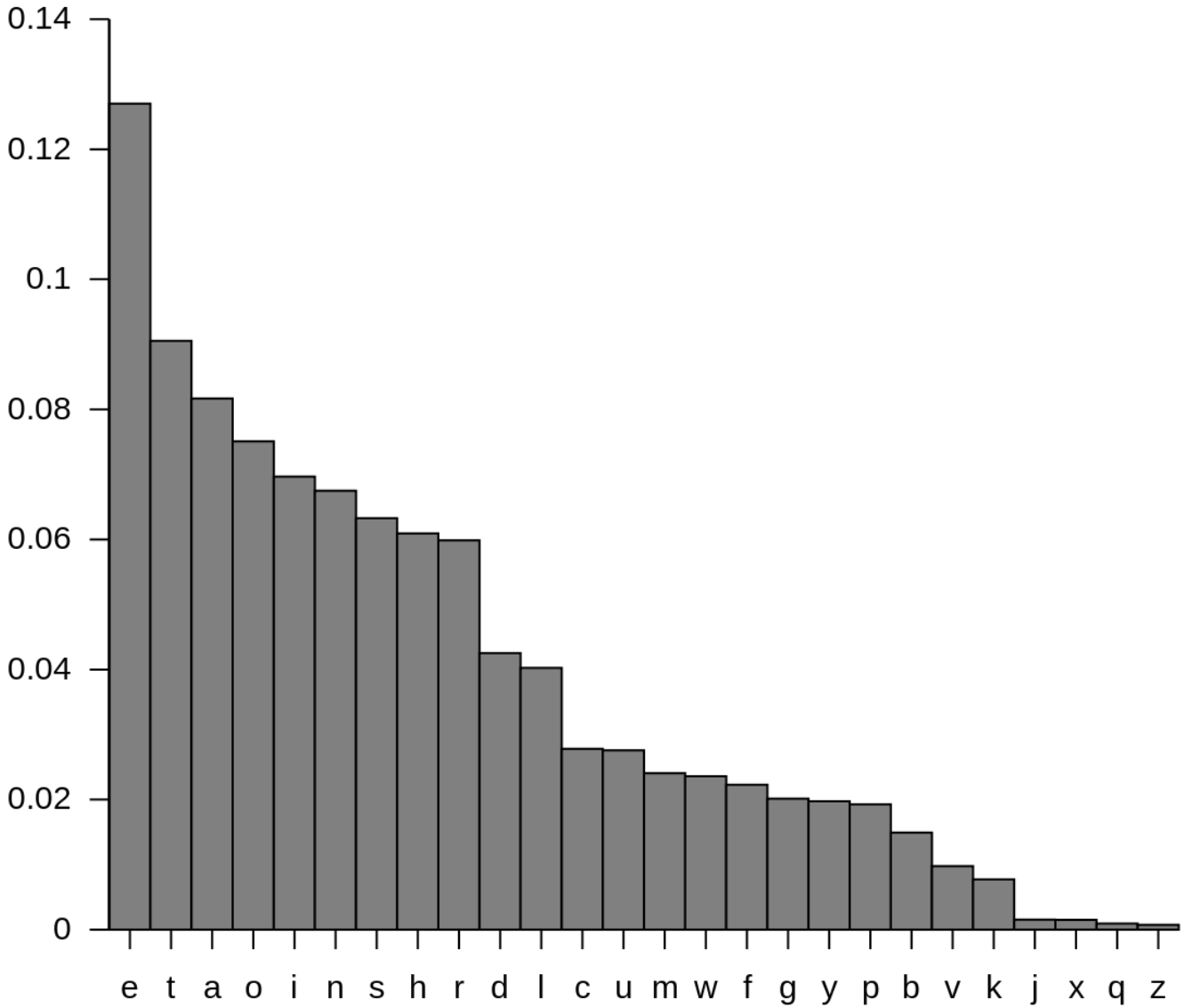
Ανάλυση συχνότητας

- Στα μονοαλφαβητικά συστήματα, η κατανομή συχνοτήτων παραμένει η ίδια, απλώς αλλάζουν τα γράμματα
- Βρίσκουμε το πιο συχνό γράμμα στο κρυπτοκείμενο
- Το αντιστοιχούμε με το πιο συχνό γράμμα της γλώσσας
  - ‘α’ στα Ελληνικά
  - ‘e’ στα Αγγλικά
- Συνεχίζουμε για τα επόμενα γράμματα

Ανάλυση συχνότητας

- Επειδή το κείμενο δεν είναι απείρου μήκους, οι συχνότητες μπορεί να μην είναι τέλειες
- Λαμβάνουμε υπ’ όψιν ότι μπορεί να έχουμε κάνει λάθη
- Χρησιμοποιούμε ως βοήθεια συχνά εμφανιζόμενες λέξεις
  - π.χ. στα Αγγλικά ‘the’, ‘a’, ‘an’, ‘or’, ‘to’, ‘on’, …

Συχνότητα γραμμάτων στα Αγγλικά



Συχνότητα λέξεων στα Αγγλικά

Κατάταξη	Λέξη
1	**the**
2	**be**
3	**to**
4	**of**
5	**and**
6	**a**
7	**in**
8	**that**
9	**have**
10	**I**

Vigenère

- Πολυαλφαβητικό σύστημα
- Παρόμοιο με το κρυπτοσύστημα Καίσαρα
- Όμως το κλειδί είναι πολλές μετατοπίσεις εντός του αλφαβήτου αντί για μία
- Αντιπροσωπεύεται από μία λέξη
- π.χ. LEMON = (11, 4, 12, 14, 13)
- Το πρώτο γράμμα κρυπτογραφείται με το πρώτο γράμμα του κλειδιού, το δεύτερο με το δεύτερο κ.ό.κ.

	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

Κρυπτογράφηση Vigenère

```
   LEMONLEMONLEMONLEMONLEMONLEMON
+ THE NSA IS SPYING ON AMERICANS
-------------------------------
   ELQ ADE WF WBMVYK CA EYSETGMBF
```

Πώς θα κρυπταναλύατε το Vigenère?

Κρυπτανάλυση Vigenère

- **Έστω** ότι γνωρίζουμε το μήκος του κλειδιού. Τότε μπορούμε να κάνουμε ανάλυση συχνότητας κατά γράμμα
- Δοκιμάζω όλα τα πιθανά μήκη κλειδιού
  - Ξεκινώ με 1 (απλή Καίσαρα)
  - Συνεχίζω με 2
  - κ.ό.κ.

Δείκτης σύμπτωσης

- Η πιθανότητα δύο τυχαία επιλεγμένα γράμματα ενός κειμένου φυσικής γλώσσας να είναι τα ίδια

$$\kappa_o = \sum_{i=1}^{|\Sigma|} \frac{n_i(n_i - 1)}{n(n-1)}$$

Δείκτης σύμπτωσης

- Τυχαίο μεγάλο Αγγλικό κείμενο:

$$\kappa_p = 0.067$$

- Τυχαίο κείμενο με ομοιόμορφα τυχαία επιλεγμένα γράμματα:

$$\kappa_r = \frac{1}{26} = 0.0385$$

Δείκτης σύμπτωσης

- Το μήκος του κλειδιού στο Vigenère μπορεί να βρεθεί προσεγγυστικά ως:

$$|S| \approx \frac{K_p - K_r}{K_o - K_r}$$

Εύρεση κλειδιού Vigenère

- Απλούστερα, **μαντεύουμε** μήκη κλειδιών και τοποθετούμε το κείμενο σε στήλες τέτοιου μήκους
- Βρίσκουμε το δείκτη σύμπτωσης σε κάθε στήλη ξεχωριστά
- Κρατάμε το μήκος που έχει μέσο όρο δεικτών σύμπτωσης κοντινότερα στο αναμενόμενο

Μάθαμε

- Ιστορικά κρυπτοσυστήματα
- Κωδικοποιήσεις: base64, base58
- xor
- Συστήματα μετάθεσης
- Καίσαρα
- Vigenère
- Κρυπτανάλυση brute-force, συχνότητας, με δείκτες σύμπτωσης

Την επόμενη φορά...

- Το τέλειο κρυπτοσύστημα: One-time pad
  - ...και απόδειξη γιατί δεν μπορεί να σπάσει ποτέ!
- Αυστηροί ορισμοί, μοντέλα και μέθοδοι αποδείξεων στην κρυπτογραφία
  - CO, KPA, CPA, CPA2, CCA, PCPA
  - Semantic security
  - Indistinguishability
  - Αναγωγές