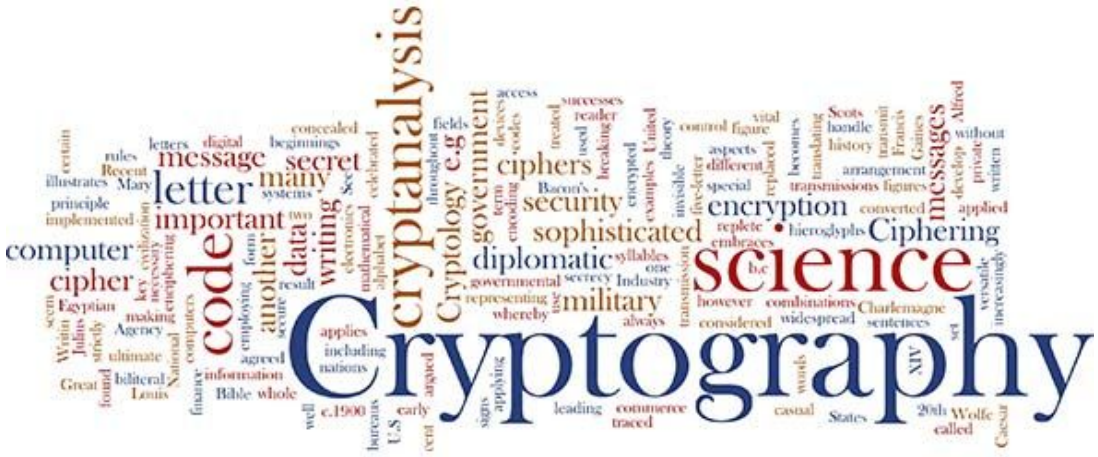
ΚΡΥΠΤΟΓΡΑΦΙΑ



IEEE Volos Student Branch

IEEE Student Branch
University of Thessaly

Νικητάκης Παναγιώτης

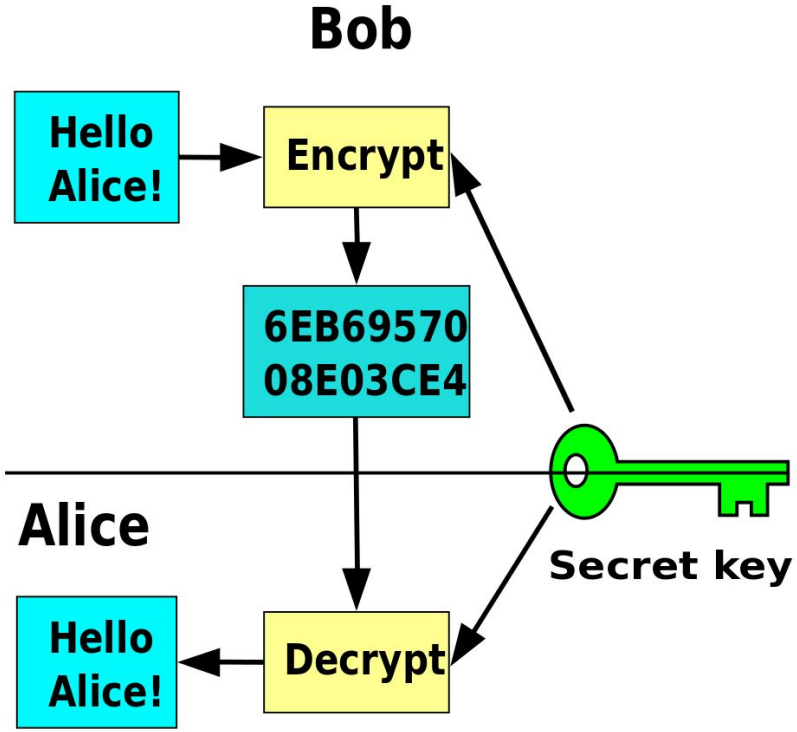
Δομή παρουσίασης

- Τι είναι η κρυπτογραφία?
- Σημαντικότητα & ιστορική αναδρομή
- Παραδείγματα κρυπτογράφησης και πως “σπάσανε”
- Τι θεωρείται ασφαλές?
- Ποιο είναι το σημερινό πρότυπο?
- Διαφορετικού είδους επιθέσεις (active & side-channel attacks)
- Ακεραιότητα μηνύματος
- Αναφορά στην “Δημόσια” κρυπτογράφηση (public encryption)
- Τι έπεται στον τομέα της κρυπτογραφίας?

Τι είναι η Κρυπτογραφία και ποια η σημασία της

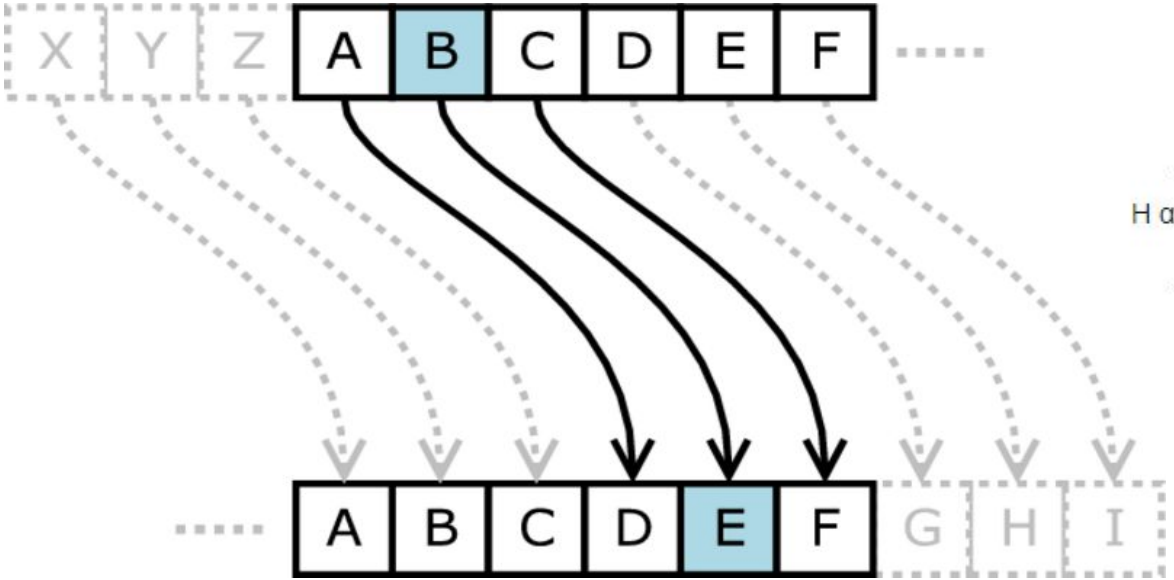
Η κωδικοποίηση της πληροφορίας έτσι ώστε να έχουν πρόσβαση σε αυτήν συγκεκριμένα άτομα

π.χ. χρειάζεται για emails, αρχεία σε ενα υπολογιστή, online λογαριασμούς, facebook, twitter, eshop κ.α.



Ιστορική διαδρομή

Οι πρώτες αναφορές το 60 π.Χ. από τον Ιούλιο Καίσαρα : **Caesar cipher**



$$E_n(x) = (x + n) \mod 24.$$

Η αποκρυπτογράφηση γίνεται αναλόγως.

$$D_n(x) = (x - n) \mod 24.$$

π.χ. Attack at dawn -> Dwwdf dw gdzq

Αλλά...

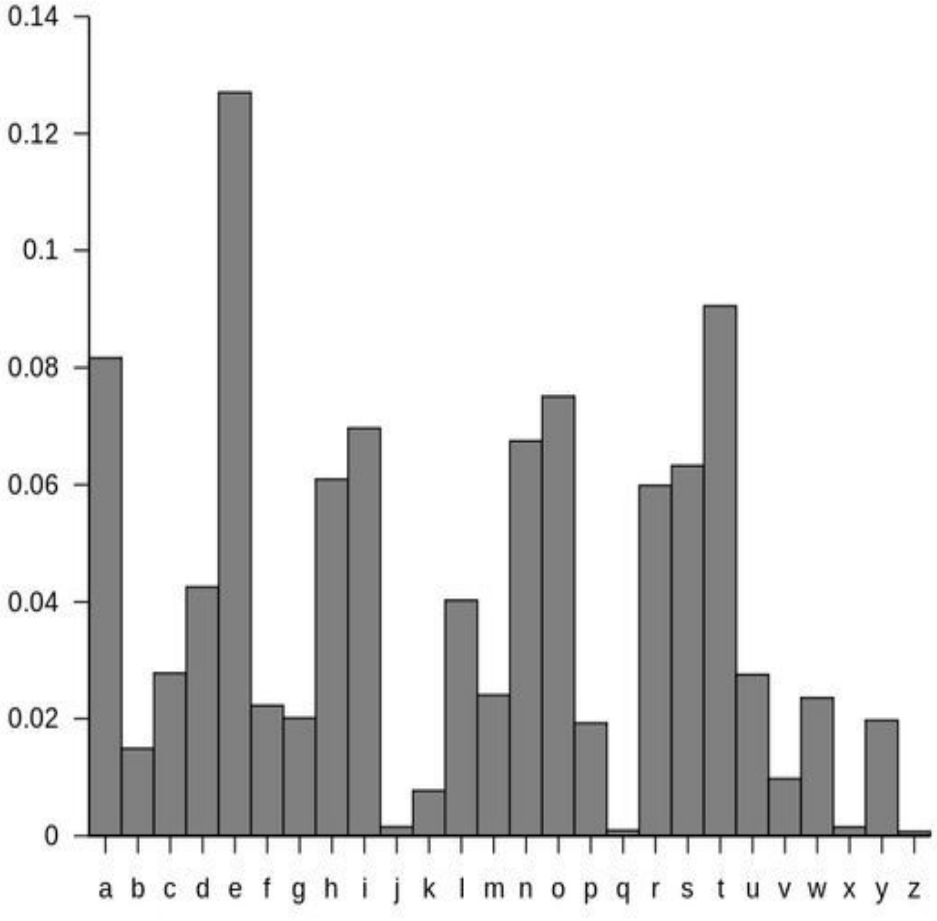
https://en.wikipedia.org/wiki/Caesar_cipher

Ιστορική διαδρομή

Caesar cipher

2 τρόποι να “σπάσει”:

- Brute force: δοκίμασε όλους τους δυνατούς συνδυασμούς
- Χρησιμοποίησε letter frequency



https://en.wikipedia.org/wiki/Brute-force_attack
https://en.wikipedia.org/wiki/Letter_frequency

Ιστορική διαδρομή

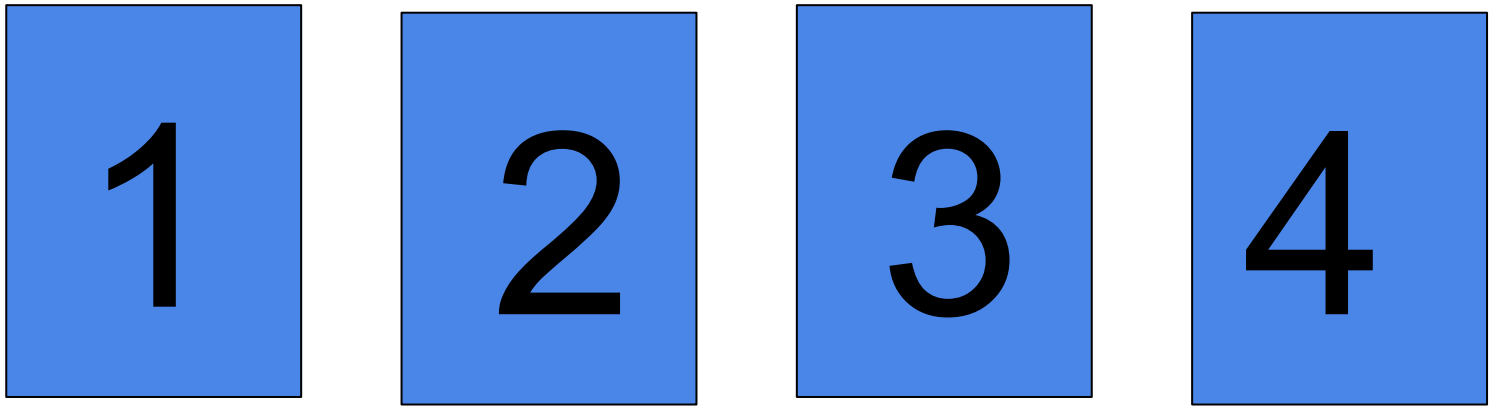
World War II : Enigma machine

Αλλά…

https://en.wikipedia.org/wiki/Enigma_machine

Test !!!!

Διαλέξτε έναν απο αυτούς τους αριθμούς:



Παραδείγματα: OTP

Ας δοκιμάσουμε κάτι απλό βασιζόμενοι στο κώδικα του Καίσαρα: **OTP**

One-time Pad: Encryption

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Encryption: Plaintext ⊕ Key = Ciphertext

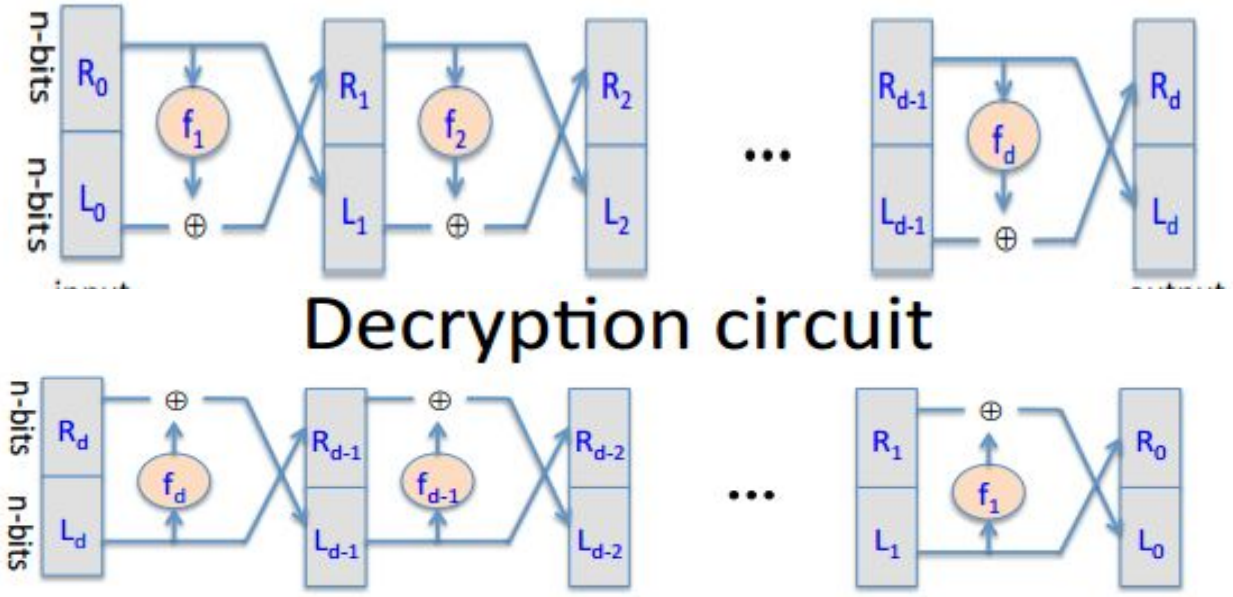
	h	e	i	l	h	i	t	l	e	r
Plaintext:	001	000	010	100	001	010	111	100	000	101
Key:	111	101	110	101	111	100	000	101	110	000
Ciphertext:	110	101	100	001	110	110	111	001	110	101
	s	r	l	h	s	s	t	h	s	r

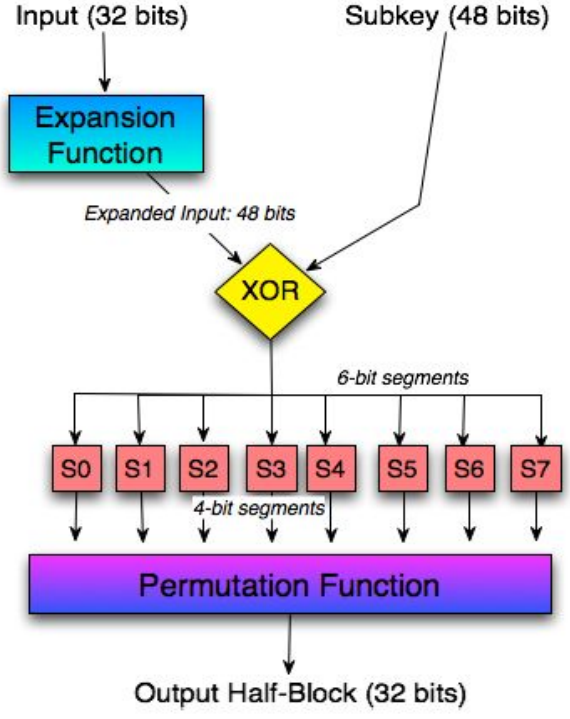
Αλλά.. (για άλλη μια φορά!)

https://en.wikipedia.org/wiki/One-time_pad

Παραδείγματα: DES

Ένας πιο πολύπλοκος τρόπος κρυπτογράφησης είναι ο DES. Ανακαλύφθηκε το 1970 από την IBM και ήταν ο καθιερωμένος μέχρι το 1997. (2^56 -> 2^48)

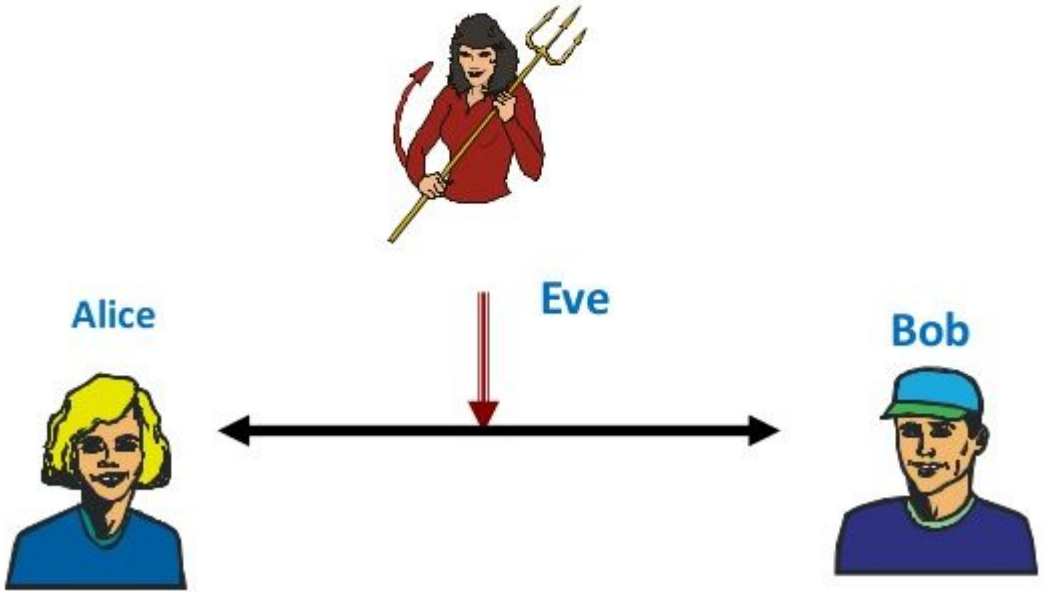




https://en.wikipedia.org/wiki/Data_Encryption_Standard

Meet Alice and Bob

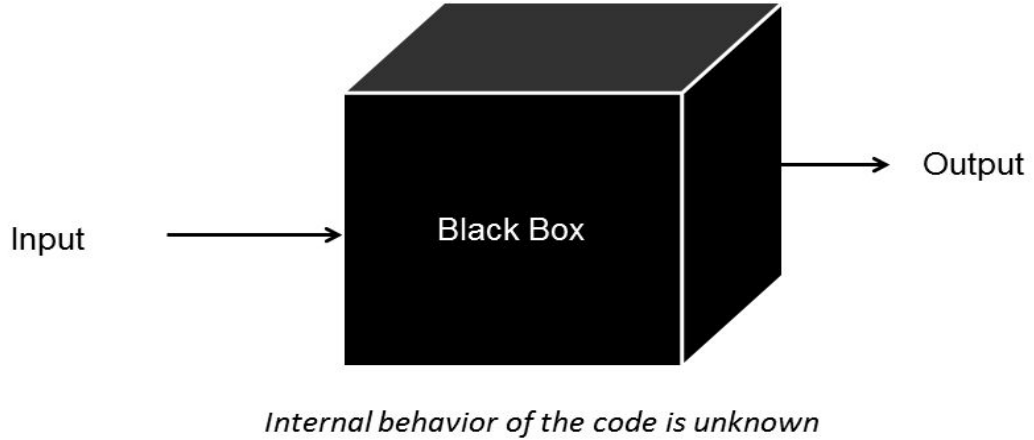
We have to prevent **Eve** from **eavesdropping** on communications between **Alice** and **Bob**.



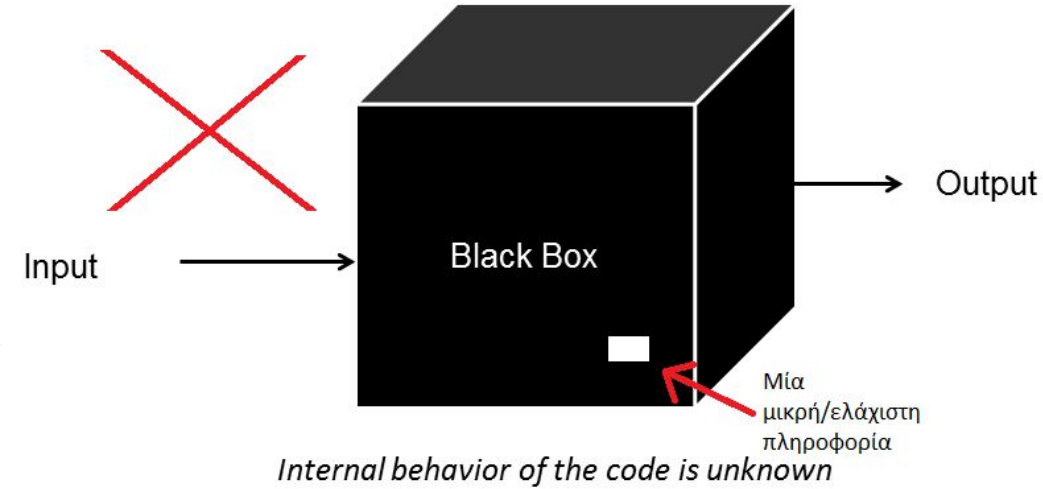
Don’t judge me from the photo!!!

Ασφάλεια?

Και η πιο μικρή παράλειψη ή διαρροή πληροφορίας είναι αρκετή… για να γίνει το κακό!



Η Eve χαίρεται τώρα!



Ασφάλεια?

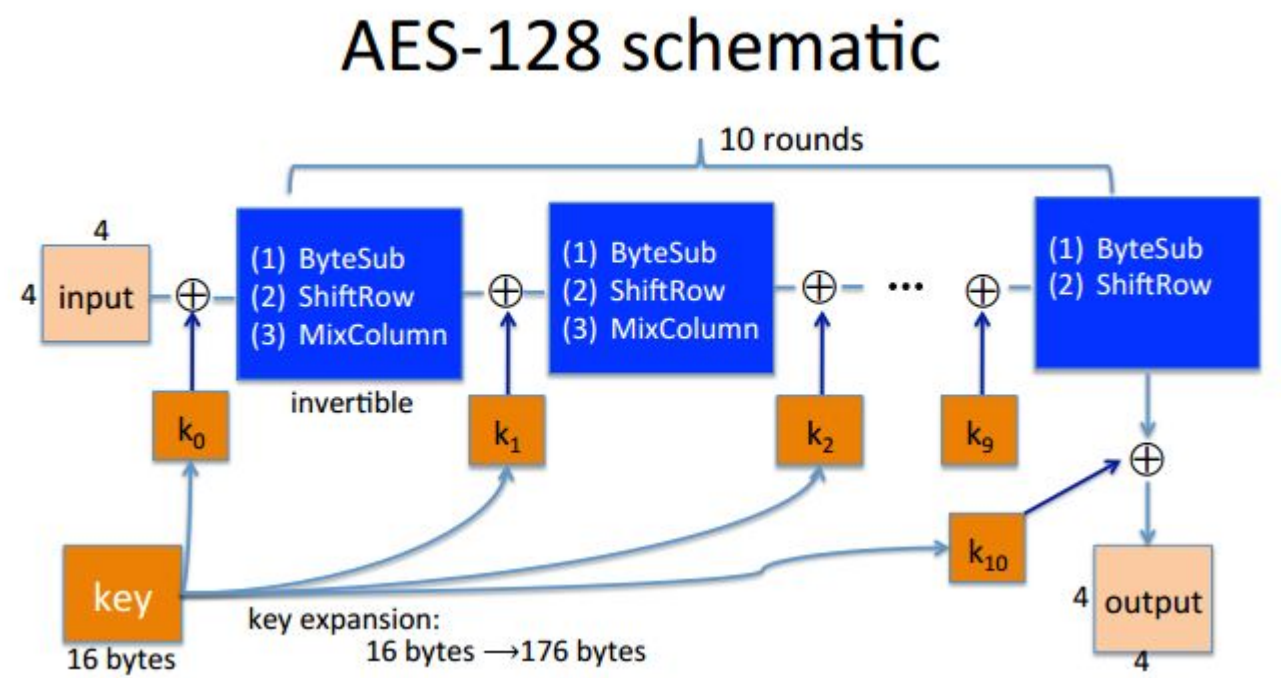
Αν δεν έχω κανένα ελάττωμα στον τρόπο κρυπτογραφίας μου, τότε σημαίνει ότι είμαι ασφαλής? :D

ΟΧΙ.. :(

Γιατί μπορεί η Eve να χρησιμοποιήσει brute force, δηλαδή να δοκιμάσει όλα τα δυνατά κλειδιά: 2^N όπου N το μήκος του δυαδικού κλειδιού… Τι γίνεται τώρα?

Advanced Encryption Standard (AES)

Χρησιμοποιεί κλειδί 128, 192 ή 256 bits. Η καλύτερη επίθεση σε 2^99 επομένως είναι ασφαλής!



Active & Side-channel attacks

Είμαστε πλήρως καλυμμένοι?

Όχι..

Υπάρχουν και.. ύπουλες επιθέσεις!

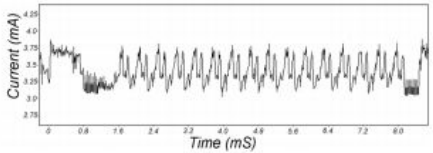
π.χ.

- Timing attack
- Power-monitoring attack
- Acoustic cryptanalysis
- Differential fault analysis
- Data remanence
- Row hammer

Attacks on the implementation

1. Side channel attacks:
   - Measure **time** to do enc/dec, measure **power** for enc/dec

smartcard



[Kocher, Jaffe, Jun, 1998]

2. Fault attacks:
   - Computing errors in the last round expose the secret key k

Man in The Middle - wiki

Από τις σημαντικότερες απειλές!

Alice

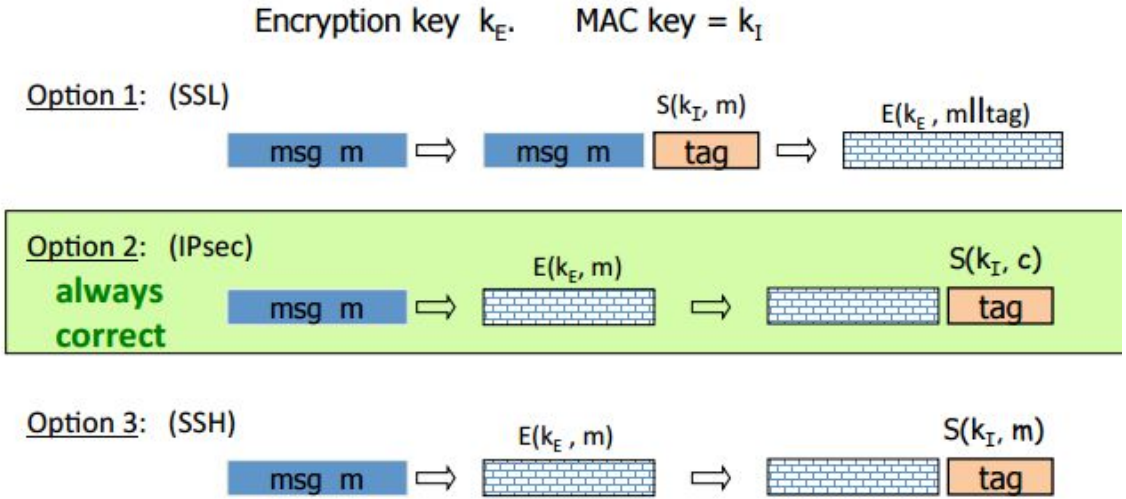
Bob

Eve

Ακεραιότητα

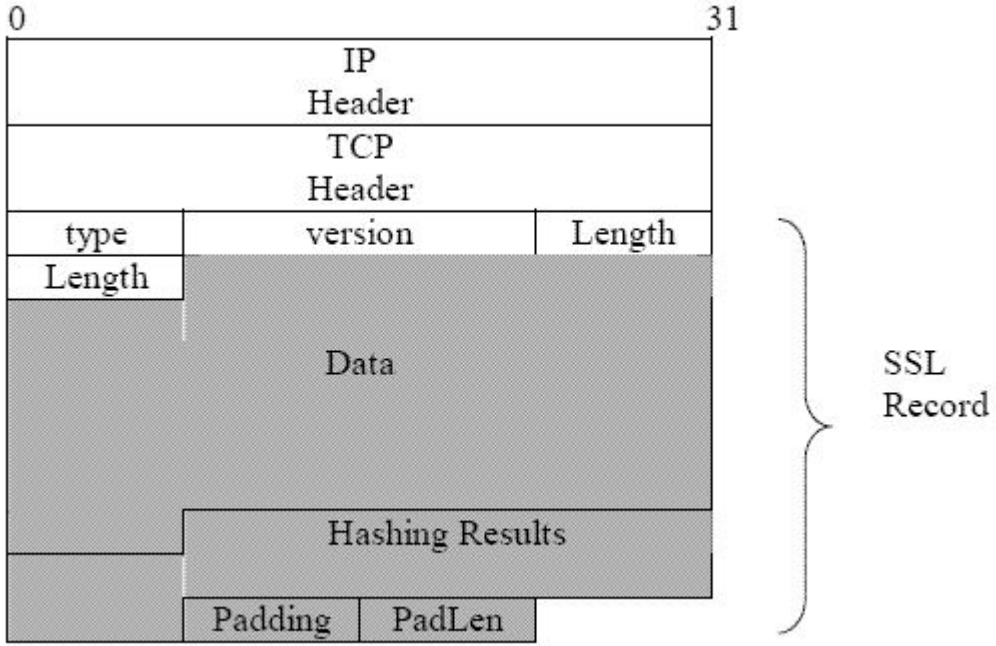
Τίθεται το θέμα εαν η Eve “πείραξε” το κείμενο που μου σταλθηκε. Πως το καταλαβαίνουμε? Ή αν η Eve προσπαθεί να το αναπαράγει? (π.χ. να ξαναστείλει το αρχικό μήνυμα “θέλω να αγοράσω αυτό το βιβλίο για 100$” με αποτέλεσμα ο αληθινός αποστολέας να πληρώσει 200$ για 2 ίδια βιβλία)

Tags δημιουργημένα από συναρτήσεις hashing. Δηλαδή?



Ακεραιότητα

π.χ. πακέτα στο ιντερνετ



https://en.wikipedia.org/wiki/Public-key_cryptography

Public Encryption

Μέχρι τώρα είδαμε symmetric encryption, δηλαδή η Alice και ο Bob μοιράζονται το ίδιο κλειδί μεταξύ τους.

Asymmetric encryption:

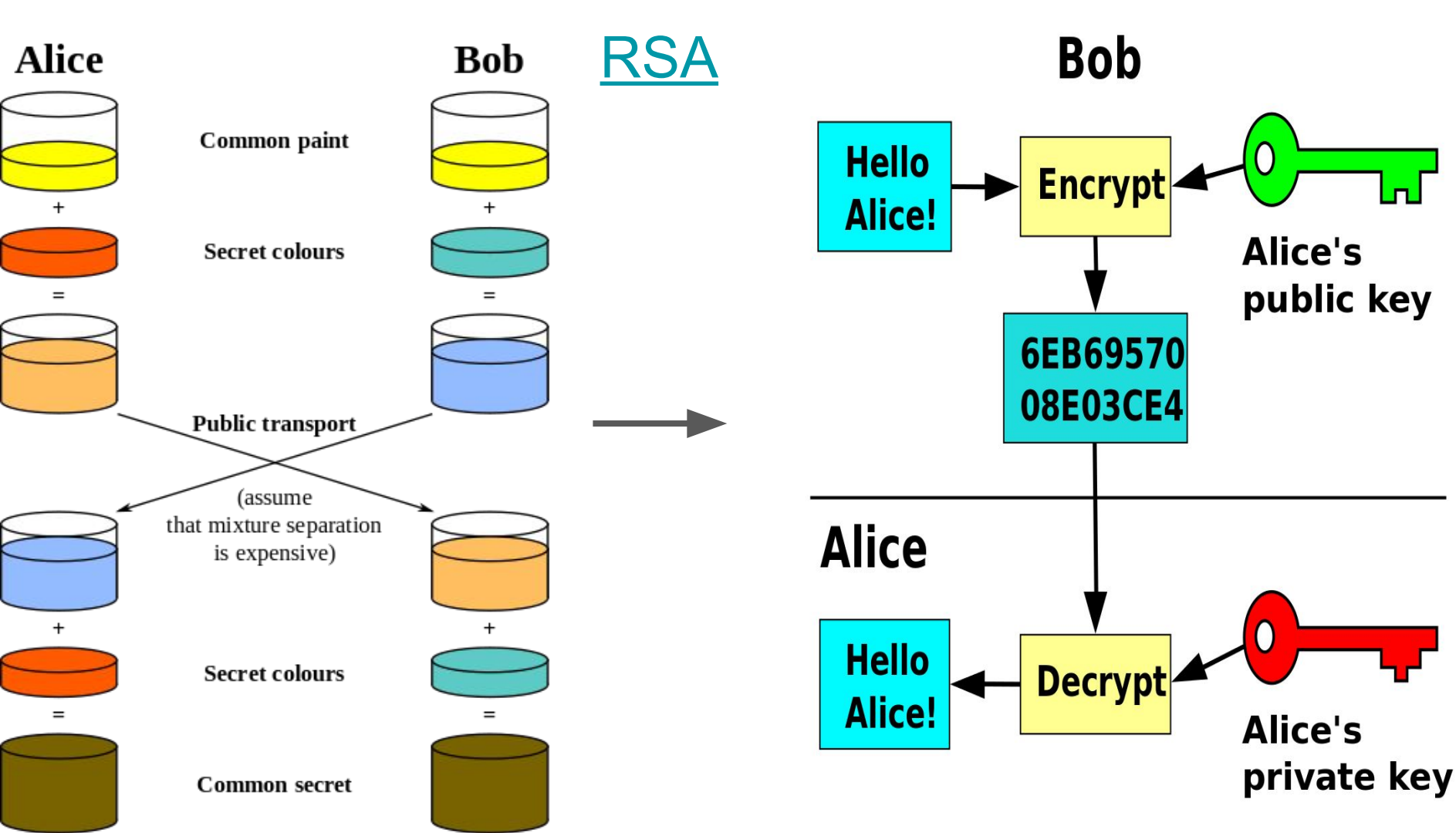
Alice →

Βασίζεται σε:

- integer factorization
- discrete logarithm
- elliptic curve

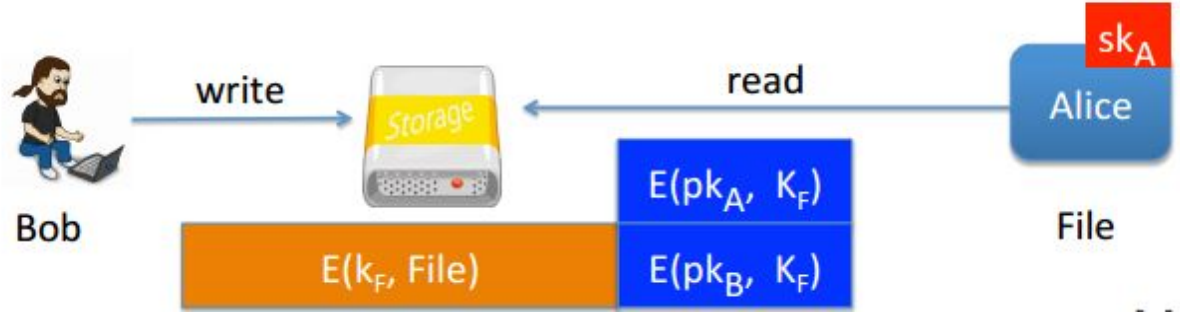
Bob →

.
.
.

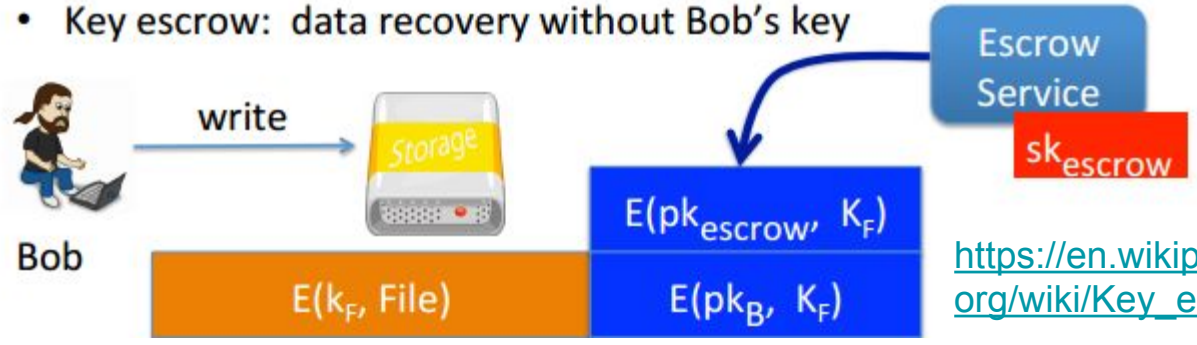

Alice
Bob
Common paint
+
+
Secret colours
=
=
Public transport
(assume
that mixture separation
is expensive)
+
+
Secret colours
=
=
Common secret
RSA
Bob
Hello
Alice!
Encrypt
Alice's
public key
6EB69570
08E03CE4
Alice
Hello
Alice!
Decrypt
Alice's
private key

Public Encryption

Άλλη εφαρμογή: κλείδωμα αρχείων!



- Key escrow: data recovery without Bob's key



https://en.wikipedia.org/wiki/Key_escrow

Future of Cryptography

Κβαντικοί υπολογιστές ⟶ Κβαντική Κρυπτογραφία

Πολλά θεωρήματα που χρειάζεται να αποδειχθούν για να μπορούμε να τα χρησιμοποιήσουμε. (π. χ. Diffie-Hellman open problem for more than 4 parties - wiki)

Υπάρχουν και αναπτύσσονται ακόμα πιο περίπλοκοι μεθόδοι για να βελτιστοποιήσουμε τον χρόνο κωδικοποίησης και το μέγεθος. Για αυτές τις μεθόδους χρειαζόμαστε ολοένα και πιο πολύπλοκα μαθηματικά.

Κάποιες αναγκαίες παραλείψεις

- PRG: pseudo random generator
- PRF & PRP
- Adversary computation
- CBC: cipher block chaining
- CTR
- MAC in detailed
- CBC-MAC
- Padding
- Collision Resistance (Birthday paradox)
- Hashing
- HMAC
- CPA: chosen plaintext attack
- CCA: chosen ciphertext attack
- Odds, ends & arithmetics
- HKDF
- Merkle Puzzles
- Diffie-Hellman(!)
- RSA(!)
- TDF: trapdoor functions
- PKCS
- ElGamal system

The end!

- Wikipedia
- Wikibooks

Full courses:

- Coursera
- Udacity
- Khan Academy