Cryptography and Network Security Chapter 9

Fifth Edition

by William Stallings

Chapter 9 – Κρυπτογραφια Δημοσιου Κλειδιου και RSA

Every Egyptian received two names, which were known respectively as the true name and the good name, or the great name and the little name; and while the good or little name was made public, the true or great name appears to have been carefully concealed.

—***The Golden Bough,*** **Sir James George Frazer**

Κρυπτογραφια Μυστικου Κλειδιου (Private-Key Cryptography)

- Η παραδοσιακη κρυπτογραφια ιδιωτικου/μυστικου/μοναδικου κειδιου χρησιμοποιει ενα μονο κλειδι.
- Το κλειδι αυτο μοιραζεται αναμεσα στον αποστολεα και τον παραληπτη
- Αν το κλειδι αποκαλυφθει, τοτε πληττεται η ασφαλεια της επικοινωνιας
- Επισης ειναι συμμετρικος, τα μερη ειναι ισα.
- Δεν προστατευει τον μεταδοτη απο το ενδεχομενο να κατασκευασει ο αποδεκτης ενα μηνυμα και να ισχυριστει οτι το εστειλε ο μεταδοτης.

Κρυπτογραφια Δημοσιου Κλειδιου (Public-Key Cryptography)

- Ειναι ισως η μεγαλυτερη ανακαλυψη στη 3000 ετων ιστορια της κρυπτογραφιας
- Χρησιμποιει δυο κλειδια. Το δημοσιο και το ιδιωτικο (public key & private key)
- **Εναι ασυμμερος διοτι τα δυο μερη δεν ειναι ισα.**
- Χρησιμοποιει εξυπνα στοιχεια απο τη θεωρια αριθμων για να λειτουργησει
- Συμπληρωνει και δεν αντικαθιστα την κρυπτογραφια ιδιωτικου κλειδιουο

Γιατι χρειαζομαστε την Κρυπτογραφια Δημοσιου Κλειδιου?

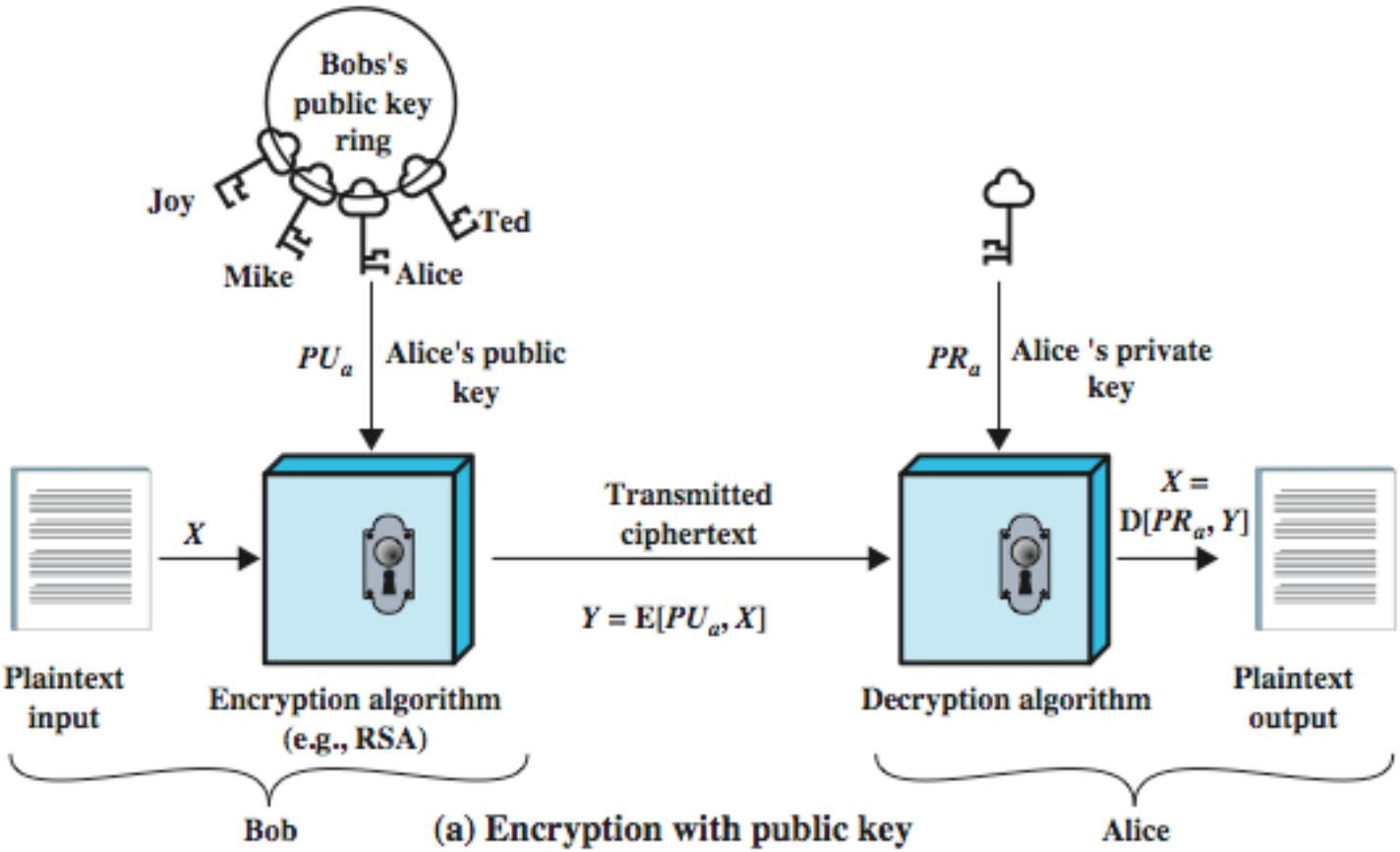
- Αναπτυχθηκε για να αντιμετωπισει δυο βασικα θεματα:
  - **Διανομη Κλειδιου (key distribution)**
  - **Ψηφιακες Υπογραφες (digital signatures)**

- Ανακαλυφθηκε επισημα απο τους Whitfield Diffie & Martin Hellman στο Πανεπιστημιο Stanford το1976
  - Ηταν γνωστος νωριτερα στην κρυπτογραφικη κοινοτητα

Κρυπτογραφια Δημοσιου Κλειδιου (Public-Key Cryptography)

- **Η Κρυπτογραφια Δημοσιου κλειδιου (ή Ασυμμετρη Κρυπτογραφια) χρησιμοποιει δυο κλειδια**:
  - Το δημοσιο κλειδι (public-key), που μπορει να ειναι γνωστο σε ολους και χρησιμοποιειται για την **κρυπτογραφηση μηνυματων** και την **επιβεβαιωση ψηφιακων υπογραφων.**
  - Το ιδιωτικο κλειδι που ειναι γνωστο μονο στον κατοχο του και χρησιμοποιειται για την **αποκρυπτογραφηση μηνυματων** και για **να υπογραψει ο κατοχος του ενα ψηφιακο εγγραφο.**
- Πρεπει να ειναι αδυνατο να προσδιορισει καποιος το ιδιωτικο κλειδι γνωριζοντας μονο το δημοσιο.
- Ειναι Ασυμμετρη γιατι αυτος που μπορει να κρυπτογραφει μηνυματα και να επιβεβαιωνει ψηφιακες υπογραφες, δεν μπορει να αποκρυπτογραφει και να βαζει ψηφιακες υπογραφες.

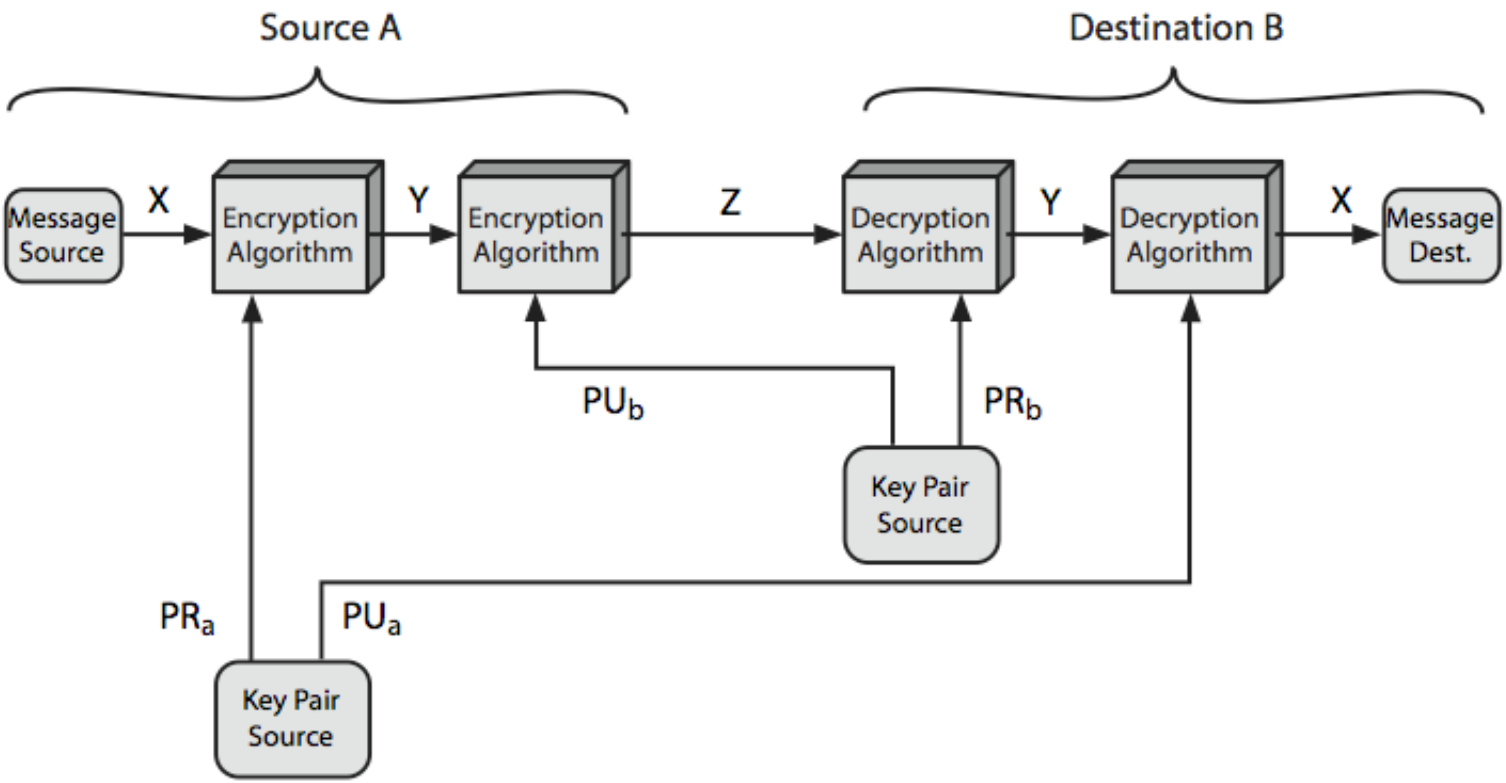
Κρυπτογραφια Δημοσιου Κλειδιου



Συμμετρική vs Δημοσιου Κλειδιου

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Κρυπτοσυστηματα Δημοσιου Κλειδιου



Εφαρμογες Κρυπτογραφιας Δημοσιου Κλειδιου

- **Κρυπτοραφηση/αποκρυπτογραφηση**
- **Ψηφιακες Υπογραφες**
- **Ανταλλαγη Κλειδιου**

- Καποιοι αλγοριθμοι εινναι καταλληλοι και για τις τρεις χρησεις, ενω αλλοι μονο για καποιες απο αυτες

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

Απαιτησεις απο τους Κρυπτογραφικους Αλγοριθμους Δημοσιου Κλειδιου

- Οι αλγοριθμοι Δημοσιου Κλειδιου βασιζονται σε δυο κλειδια τα οποια:
  - Ειναι υπολογιστικα αδυνατο να βρεθει το ιδιωτικο κλειδι απο καποιον που γνωριζει μονο το δημοσιο
  - Ειναι υπολογιστικα ευκολο να κρυπτογραφει/αποκρυπτγραφει καποιος μηνυματα οταν γνωριζει το αντιστοιχο κλειδι
  - Οτι κρυπτογρφειται με το ενα κλειδι αποκρυπτογραφειται με το αλλο, και το αντιστροφο. (δεν ισχυει για ολους τους αλγοριθμους δημοσιου κλειδιου).
- Ειναι εξαιρετικα δυσκολες οι παραπανω απαιτησεις και ελαχιστοι αλγοριθμοι τις πληρουν.

Ασφαλεια συστηματων δημοσιου κλειδιου

- Οπως και στα συμμετρικα συστηματα, παντα μπορει θεωρητικα να γινει επιθεση brute force
- Αλλα εδω τα κλειδια ειναι πολυ μεγαλα (>512bits)
- Η ασφαλεια βασιζεται στη μεγαλη διαφορα της δυσκολιας αναμεσα στην ευκολη κρυπτογραφηση/αποκρυπτογραφηση και τη δυσκολη κρυπταναλυση
- Χρησιμοποιει πολυ μεγαλους αριθμους και αρα ειναι πολυ πιο αργη απο την συμμετρικη κρυπτογραφια

RSA

- Δημιουργοι: Rivest, Shamir & Adleman of MIT in 1977
- Ο πιο γνωστος και ο ευρυτερα χρησιμοποιουμενος αλγοριθμος δημοσιου κλειδιου
- Βασιζεται στην υψωση ακεραιων σε δυναμη και σε αριθμητικη modulo
- Χρησιμοποιει πολυ μεγαλους ακεραιους
- Η ασφαλεια του βασιζεται στη δυσκολια παραγοντοποιησης μεγαλων αριθμων

Κρυπτογραφηση και Αποκρυπτογραφηση με τον RSA

- Κρυπτογραφηση μηνυματος M (στο μεταδοτη):
  - Λαμβανεται το δημοσιο κλειδι του αποδεκτη $PU=\{e,n\}$
  - Υπολογιζεται το : $C = M^e \bmod n$, οπου $0 \leq M < n$
- Αποκρυπτογραφηση το ciphertext C (στον απποδεκτη):
  - Χρησιμοποιειται το ιδιωτικο κλειδι $PR=\{d,n\}$
  - Υπολογιζται το: $M = C^d \bmod n$
- Το μηνυμα M πρεπει να ειναι μικροτερο απο το n (αλλιως πρεπει να χωριστει σε τμηματα)

Δημιουργια κλειδιων στον RSA

- Καθε χρηστης δημιουργει ενα ζευγος δημοσιου/ιδιωτικου κλειδιου:
- Επιλεγοντας δυο μεγαλουν πρωτους αριθμους τυχαια: p, q
- Υπολογίζει το modulus $n=p.q$
  - Ετσι ωστε: $\varphi(n)=(p-1)(q-1)$
- Επιλεγει τυχαια το κλειδι κρυπτογραφησης (δημοσιο κλειδι) e
  - Ετσι ωστε: $1<e<\varphi(n)$, $\text{ΜΚΔ}(e,\varphi(n))=1$
- Λυνει την παρακατω εξισωση για να βρει το κλειδι αποκρυπτογραφησης (ιδιωτικο κλειδι) d
  - $e.d=1 \bmod \varphi(n)$ and $0 \le d \le n$
- Δημοσιοποιει το κλειδι κρυπτογραφησης: PU={e,n}
- Κραταει μυστικο το κλειδι αποκρυπτογραφησης: PR={d,n}

Γιατι λειτουργει ο RSA?

- Απο το θεωρημα του Euler ισχυει:
  - $a^{\varphi(n)} \bmod n = 1$, οπου ΜΚΔ$(a,n)=1$
- Στον RSA έχουμε:
  - $n=p.q$
  - $\varphi(n)=(p-1)(q-1)$
  - Επιλεγουμε προσεκτικα τους e & d ωστε να ειναι αντιστροφοι $\bmod \varphi(n)$
  - Ως εκ τουτου $e.d=1+k.\varphi(n)$ για καποιο k
- Και επομενως:

$$C^d = M^{e.d} = M^{1+k.\varphi(n)} = M^1.(M^{\varphi(n)})^k$$
$$= M^1.(1)^k = M^1 = M \bmod n$$

Παραδειγμα:
RSA – Ορισμος των κλειδιων

1. Επιλέγουμε πρωτους αριθμους: $p=17$ & $q=11$
2. Υπολογίζουμε: $n = pq = 17 \times 11 = 187$
3. Υπολογίζουμε: $\varphi(n)=(p-1)(q-1)=16 \times 10=160$
4. Επιλέγουμε το e, τετοιο ωστε να ειναι πρωτος ως προς το $\varphi(n)=160$ (Δηλ. *ΜΚΔ*$(e,160)=1$); Επιλεγουμε: $e=7$.
5. Οριζουμε το d, τετοιο ωστε:

   $de \bmod 160 = 1$ και $d < 160$

   Η σωστη τιμη ειναι $d=23$ επειδη $23 \times 7=161=10 \times 16+1$
6. Δημοσιευουμε το Δημοσιο Κλειδι $PU=\{7,187\}$
7. Κραταμε μυστικο το ιδιωτικο κλειδι $PR=\{23,187\}$

Παραδειγμα: Κρυπτογραφηση /Αποκρυπτογραφηση RSA

- Μηνυμα $M = 88$ (ισχυει: $88<187$)
- Κρυπτογράφηση:

  $C = 88^{7} \bmod 187 = 11$
- Αποκρυπτογράφηση:

  $M = 11^{23} \bmod 187 = 88$

Υψωση σε δυναμη

- Μπορουμε να χρησιμοποιησουμε τον αλγοριθμο «Square and Multiply» που ειναι γρηγορος και αποδοτικος
- Βασιζεται στην επανειλημενη υψωση στο τετραγωνο και στους πολλαπλασιασμους που ειναι απαραιτητοι για να υπολογισουμε το τελικο αποτελεσμα
- Προσεξτε τη δυαδικη αναπαρασταση του εκθετη.
- Απαιτουνται μονο $O(\log_2 n)$ πολλαπλασιασμοι για εναν αριθμο n
  - eg. $7^5 = 7^4.7^1 = 3.7 = 10 \bmod 11$
  - eg. $3^{129} = 3^{128}.3^1 = 5.3 = 4 \bmod 11$

Υψωση σε δυναμη

```
c = 0; f = 1
for i = k downto 0
    do c = 2 x c
       f = (f x f) mod n
    if b_i == 1 then
       c = c + 1
       f = (f x a) mod n
 return f
```

Αποτελεσματικη Κρυπτογραφηση

- Η κρυπτογραφηση χρησιμοποιει υψωση σε δυναμη e
- Επειδη το e ειναι μικρο, αυτο γινεται γρηγορα,
  - Συχνα επιλεγουμε: e=65537 (2^{16}-1)
- Αλλα αν ειναι υπερβολικα μικρο (π.χ. e=3) μειωνεται η ασφαλεια
- Αν το e ειναι σταθερο, πρεπει να ειμαστε σιγουροι οτι ΜΚΔ$(e,\varphi(n))=1$
  - Απορριπτονται οποιαδηποτε p ή q που δεν ειναι σχετικα πρωτοι ως προς το e

Αποτελεσματικη Αποκρυπτογραφηση

- Η αποκρυπτογραφηση χρησιμοποιει υψωση σε δυναμη d
  - Το d πρεπει να ειναι μεγαλο, αλλιως ειναι μη ασφαλες.
- Μπορουμε να χρησιμοποιησουμε το Chinese Remainder Theorem (CRT) για να υπολογισουμε τα mod p & q ξεχωριστα. Τοτε τα συνδυαζουμε για να παρουμε την επιθυμητη απαντηση
  - Αυτο ειναι περιπου 4 φορες γρηγοροτερο απο το να το κανουμε αμεσα
- Μονο ο κατοχος του ιδιωτικου κλειδιου που γνωριζει τις τιμες τις τιμες των p & q μπορει να εφαρμοσει αυτην την τεχνικη

Δημιουργια κλειδιου RSA

- Οι χρηστες του RSA πρεπει:
  - Να επιλεξουν στην τυχη δυο πρωτους αριθμους `p,q`
  - Να επιλέξουν το ειτε το `e` ειτε το `d` και να υπολογισουν το αλλο.
- Οι πρωτοι αριθμοι `p,q` πρεπει να ειναι αρκετα μεγαλοι ωστε να μην προκυπτουν ευκολα απο το modulus `n=p.q`

Ασφαλεια του RSA

- Πιθανες επιθεσεις στον RSA:
  - brute force key search – αδυνατο λογω των τεραστιων αριθμων που χρησιμοποιουνται
  - Μσθηματικες επιθεσεις – βασιζονται στη δσκολια υπολογισμου του $\varphi(n)$, παραγοντοποιωντας το modulus n
  - Επιθεσεις χρονισμου
  - Επιθεσεις επιλεγμενου ciphertext (Chosen ciphertext attacks)

Το προβλημα της παραγοντοποιησης

- Η μαθηματικη προσεγγιση εχει τρεις μορφες:
  - Παραγοντοποιησε το $n=p.q$, και στη συνεχεια υπολογισε το $\varphi(n)$ και τελος το d
  - Βρες απ'ευθειας το $\varphi(n)$ και υπολογισε το d
  - Βρες απ'ευθειας το d

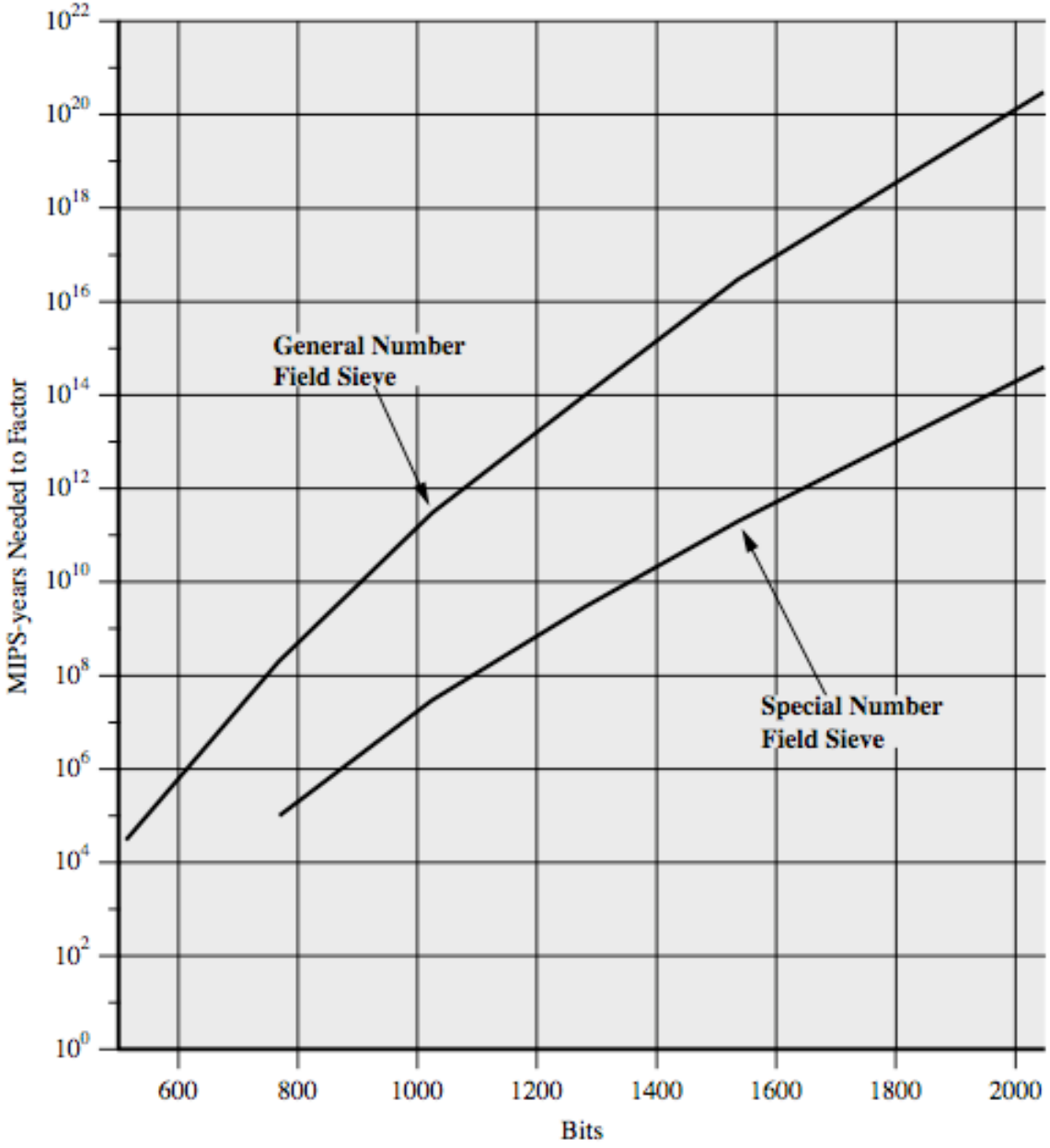
Σημερα RSA με κλειδια 1024-2048 bit θεωρειται ασφαλης

- Εφοσον τα p, q ειναι παρομοιου μεγεθους και πληρουν ολα τα κριτηρια που εχουν τεθει.

Progress in Factoring

Number of Decimal Digits	Approximate Number of Bits	Date Achieved	MIPS-years	Algorithm
100	332	April 1991	7	quadratic sieve
110	365	April 1992	75	quadratic sieve
120	398	June 1993	830	quadratic sieve
129	428	April 1994	5000	quadratic sieve
130	431	April 1996	1000	generalized number field sieve
140	465	February 1999	2000	generalized number field sieve
155	512	August 1999	8000	generalized number field sieve
160	530	April 2003	—	Lattice sieve
174	576	December 2003	—	Lattice sieve
200	663	May 2005	—	Lattice sieve

Η προοδος στην παραγοντο ποιηση



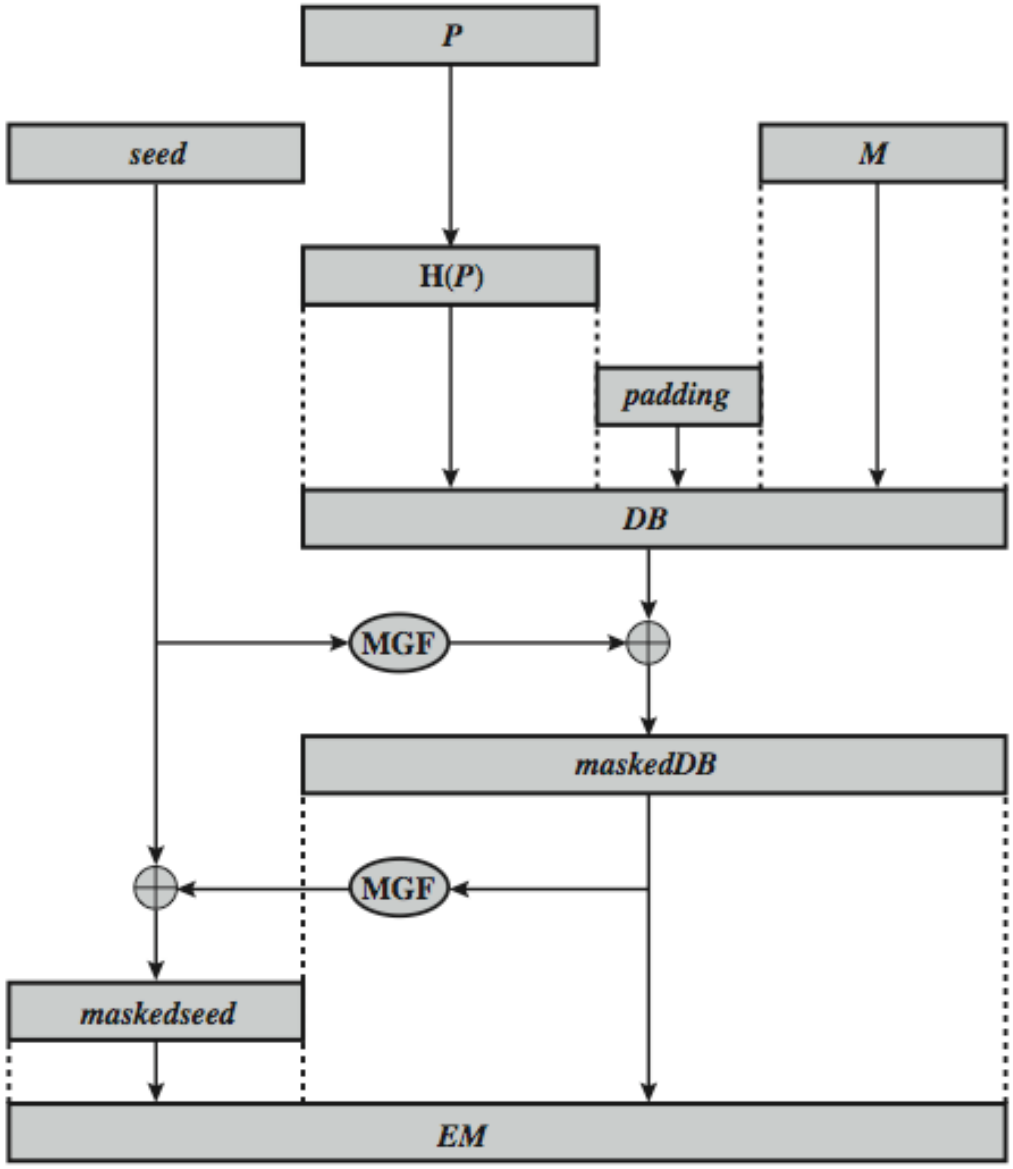
Επιθεσεις Χρονισμου στον RSA (Timing Attacks)

- Αναπτυχθηκαν απο τον Paul Kocher στα μεσα της δεκαετιας του ’90.
- Εκμεταλλεύονται τη διαφοροποιηση στη χρονικη διαρκεια των λειτουργιων
  - π.χ. Ο πολλαπλασιασμος μικρου αριθμου εναντι του πολλαπλασιασμου μεγαλου αριθμου
  - ή το ποιες εντολες εκτελουνται μετα απο ενα IF
- Συμπεραινει το μεγεθος του ορισματος με βαση το χρονο που παιρνει η εντολη για να εκτελεστει
- Στην περιπτωση του RSA εκμεταλευεται το χρονο που παιρνει η υψωση σε δυναμη.
- Αντιμετρα:
  - Χρηση σταθερου χρονου υψωσης σε δυναμη
  - Προσθηκη τυχαιων καθυστερησεων
  - Πολλαπλασμος του ciphertext με εναν τυχαιο αριθμο πριν την υψωση του σε δυναμη.

Επιθεσεις Επιλεγμενου Ciphertext (Chosen Ciphertext Attacks, CCA)

- Ο RSA ειναι ευπαθης σε επιθεσεις Επιλεγμενου Ciphertext
- Ο επιτιθεμενος εχει τη δυνατοτητα να επιλεγει το ciphertext και να παιρνει πισω το αποκρυπτογραφημενο κειμενο
- Επιλεγει το ciphertext ετσι ωστε να εκμεταλευεται τις ιδιοτητες του RSA και με τον τροπο αυτο να παιρνει πληροφοριες που τον βοηθουν στην κρυπταναλυση
- Ως αντιμετρο η RSA προτεινει την τροποποιηση του plaintext μεσω μιας διαδικασιας που ονομαζεται Optimal Asymmetric Encryption Padding (OASP)

Optimal Asymmetric Encryption Padding (OASP)



Συνοψη

- Συζητησαμε:
  - Τις αρχες της κρυπτογραφιας δημοσιου κλειδιου
  - Τον αλγοριθμο RSA, την υλοποιηση του και την ασφαλεια του