Μέθοδοι Κρυπτογραφίας στη Πληροφορική

Παρουσίαση: Θωμάς Σκόδρας, Α.Μ.: 052960

Υπεύθυνος Καθηγητής : Κωνσταντίνος Διαμαντάρας

Α.Τ.Ε.Ι.Θ.: Τμήμα Πληροφορικής

Θεσσαλονίκη, Φεβρουάριος 2009

Περιεχόμενα

- Κρυπτογραφία και Κρυπτοσυστήματα - Υπηρεσίες της Κρυπτογραφίας.
- Συμμετρική Κρυπτογραφία.
- Ασύμμετρη Κρυπτογραφία.
- Βασικές έννοιες της Θεωρίας Αριθμών.
- Ο Αλγόριθμος του Καίσαρα.
- Ο Αλγόριθμος DES (Data Encryption Standard).
- Ο Αλγόριθμος IDEA (International Data Encryption Algorithm).
- Ο Αλγόριθμος του AES (Advanced Encryption Standard).
- Αλγόριθμος ανταλλαγής κλειδιών Diffie-Hellman.
- Αλγόριθμος RSA (Rivest Shamir Adelman Algorithm).
- Οι Συναρτήσεις Hash.
- Αλγόριθμος ElGamal.
- Κρυπτογραφία με Ελλειπτικές Καμπύλες
- Σύγκριση της χρήσης των ελλειπτικών καμπυλών στη λύση του προβλήματος DLP με τη χρήση συμβατικών κρυπτογραφικών συστημάτων.
- Οι κυριότερες εφαρμογές των Ελλειπτικών Καμπυλών στην Κρυπτογραφία (ECC) και οι αλγόριθμοι τους.

Ιστορική Αναδρομή της Κρυπτογραφίας.

- Η κρυπτογραφία ξεκίνησε πριν από περίπου 3500 χρόνια ως μια τέχνη απόκρυψης μυστικών.
- Μερικά παραδείγματα χρήσης της Κρυπτογραφίας:
  - 2500 π.Χ.: Τα Ιερογλυφικά στις πυραμίδες της Αιγύπτου αποτελούσαν κρυπτογραφημένα κείμενα.
  - 500 π.Χ.: Οι Σπαρτιάτες κάνανε τατουάζ στο σώμα τους κωδικοποιημένα μηνύματα για να μη τα καταλαβαίνει ο αντίπαλος.
  - Στο Ρωμαϊκό στρατό εφαρμόστηκε ο αλγόριθμος του Καίσαρα για την κρυπτογράφηση μηνυμάτων.
    - Από τις παλιότερες μεθόδους κρυπτογράφησης είναι ο αλγόριθμος του Καίσαρα , όπου αν ένα γράμμα στο αρχικό κείμενο είναι το *N*ιοστό στο αλφάβητο ,αντικαθίσταται από το (*N+K*)ιοστό γράμμα του αλφαβήτου , όπου *K* είναι ένας σταθερός ακέραιος (για τον αλγόριθμο του Καίσαρα *K=3*).
  - Αγγλία 1900 μ.Χ.: Δημιουργία κρυπτογραφημένων μηνυμάτων της Βασίλισσας Σκότιας Μαρίας με το στρατό της.
  - Α’ Παγκόσμιος πόλεμος: Γερμανία – Δημιουργία του συστήματος Enigma.
  - Β’ Παγκόσμιος πόλεμος: Ιαπωνία – Δημιουργία του συστήματος Purple.
  - Β’ Παγκόσμιος πόλεμος: ΗΠΑ – Δημιουργία του συστήματος Sigaba.
  - Β’ Παγκόσμιος πόλεμος: Αγγλία – Δημιουργία του συστήματος TypeX.

Τι είναι η κρυπτογραφία - Τι είναι το Κρυπτοσύστημα (1).

- *Η **κρυπτογραφία** μελετά τρόπους με τους οποίους μπορούμε να μετασχηματίσουμε ένα μήνυμα σε φαινομενικά ακατάληπτη μορφή.*
- Ο ορισμός που δόθηκε από τον Rivest (1990) εισάγει την έννοια του *αντιπάλου* και είναι ίσως ο πιο ακριβής και πλήρης ορισμός.
  - Η ύπαρξη αντιπάλου σε κάποια επικοινωνία είναι η βασική αιτία ύπαρξης και εφαρμογής της κρυπτογραφίας. Εκτός από την επιθυμία μας να κρύψουμε ένα μήνυμα από τα μάτια των αντιπάλων, θα πρέπει με κάποιο τρόπο να μην αλλοιωθεί το μήνυμα μας, ή αν αλλοιωθεί να γίνει αντιληπτό από τον παραλήπτη, και επίσης να φτάσει στον πραγματικό παραλήπτη και όχι σε κάποιον που τον υποδύεται.

Τι είναι η κρυπτογραφία - Τι είναι το Κρυπτοσύστημα (2).

- Η αρχική μορφή ενός μηνύματος, αποτελεί το **απλό κείμενο** (plaintext).
- Το κρυπτογραφημένο κείμενο αποτελεί το **κρυπτοκείμενο** (ciphertext).
- Ο μετασχηματισμός του απλού κειμένου σε κρυπτοκείμενο ονομάζεται **κρυπτογράφηση** (encryption).
- Ο μετασχηματισμός του κρυπτοκειμένου σε απλό κείμενο ονομάζεται **αποκρυπτογράφηση** (decryption).
- Οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης υλοποιούνται με τον **αλγόριθμο κρυπτογράφησης** και **αποκρυπτογράφησης** αντίστοιχα. Οι δύο αυτοί αλγόριθμοι συνιστούν τον **κρυπταλγόριθμο** (cipher).
- Η διαδικασία κρυπτογράφησης (και αποκρυπτογράφησης) απαιτεί μια επιπλέον ποσότητα πληροφορίας που την ονομάζουμε **κλειδί** (key).
- Η περιγραφή των διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης αποτελούν το **κρυπτοσύστημα.**
- Η **κρυπτανάλυση** είναι η επιστήμη που ασχολείται με την αποκρυπτογράφηση του κρυπτοκειμένου χωρίς την κατοχή του κλειδιού.

Αρχές της Κρυπτογραφίας

- Κατά την αποστολή μηνυμάτων μεταξύ δύο ενδιαφερομένων μέσα από ένα μη ασφαλές κανάλι πρέπει να διασφαλιστούν οι αρχές της **Εμπιστευτικότητας** (**Confidentiality**), της **Αυθεντικοποίησης** (**Authentication**), της **Ακεραιότητας** (**Integrity**) και της **μη αποποίηση ευθύνης** (**Non-Repudiation**).
  - Με τον όρο **εμπιστευτικότητα** εννοούμε την προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίηση τους. Η εμπιστευτικότητα μπορεί να παρομοιασθεί με έναν αδιαφανή φάκελο.
  - Η **αυθεντικοποίηση** είναι η επιβεβαίωση της ταυτότητας ενός ατόμου ή η επιβεβαίωση της πηγής αποστολής των πληροφοριών .
  - Η **ακεραιότητα** είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάσταση τους. Η υπηρεσία αυτή παρέχεται από μηχανισμούς κρυπτογραφίας όπως είναι οι ψηφιακές υπογραφές.
  - Τέλος, η **μη αποποίηση ευθύνης** (Non-Repudiation) συνδυάζει τις υπηρεσίες της αυθεντικότητας και της ακεραιότητας που παρέχονται σε μια τρίτη οντότητα. Έτσι, ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί την εγκυρότητα και τη δημιουργία και αποστολή του μηνύματος.

Εφαρμογές της Κρυπτογραφίας στη πληροφορική.

- Ασφαλές Ηλεκτρονικό Ταχυδρομείο.
- Πρόσβαση σε ασφαλείς δικτυακούς τόπους.
- Προστασία ευαίσθητων δεδομένων σε γραμματείες τμημάτων και διοικητικούς φορείς.
- Προστασία ερευνητικών δεδομένων.
- Πρόσβαση σε ηλεκτρονικές βιβλιοθήκες.
- Δημιουργία ερευνητικών ιστοσελίδων με δημόσια και ιδιωτικά τμήματα.
- Υπογεγραμμένο Λογισμικό.
- Ασφαλές ηλεκτρονικό εμπόριο.

Συμμετρική Κρυπτογραφία

- Ο παραλήπτης του μηνύματος θα πρέπει να γνωρίζει τον αλγόριθμο ή το κλειδί (key) για να μπορέσει να αποκωδικοποιήσει και να διαβάσει το μήνυμα. Στην παραδοσιακή κρυπτογραφία ο αποστολέας και ο παραλήπτης του μηνύματος χρησιμοποιούν το ίδιο (κοινό) κλειδί.
- Ο αποστολέας κρυπτογραφεί το μήνυμα με βάση αυτό το κλειδί και ο παραλήπτης το αποκρυπτογραφεί με βάση το ίδιο κλειδί.
- Πρέπει με κάποιον τρόπο να ανταλλάξουν το κοινό κλειδί.
- Αυτό ενέχει τον κίνδυνο να υποκλαπεί το κλειδί από κάποιον τρίτο που παρακολουθεί τις γραμμές επικοινωνίας ή και να διαρρεύσει από το ένα από τα δύο μέρη.
- Πλεονέκτημα: Γρηγορότερη αποκρυπτογράφηση των δεδομένων.
- Μειονέκτημα: Μικρότερη Ασφάλεια
- Γνωστές μέθοδοι συμμετρικής κρυπτογράφησης είναι ο αλγόριθμος DES (Data Encryption Standard), που χρησιμοποιείται και από την κυβέρνηση των ΗΠΑ, και το σύστημα Kerberos του γνωστού Πανεπιστημίου MIT (Massachusetts Institute of Technology).

Ασύμμετρη Κρυπτογραφία

- Χρησιμοποιούμε διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση ενός μηνύματος.
- Αυτά είναι το δημόσιο κλειδί (public key) και το ιδιωτικό κλειδί (private key), τα οποία έχουν τις εξής πολύ σημαντικές ιδιότητες :
  - Ένα μήνυμα που έχει κρυπτογραφηθεί με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το αντίστοιχο ιδιωτικό κλειδί και αντίστροφα.
  - Αν μας είναι γνωστό το ένα κλειδί δεν μπορούμε να δημιουργήσουμε το άλλο κλειδί.
- Πλεονέκτημα: Μεγαλύτερη ασφάλεια
- Μειονέκτημα: Αργή αποκρυπτογράφηση – Δε συνίσταται για χρήση σε περισσότερο από 1Kb δεδομένων

Κρυπτογραφία δημοσίου κλειδιού.

- Το 1976, οι Diffie και Hellman, έφεραν επανάσταση στο χώρο της κρυπτογραφίας με την εισαγωγή σε αυτήν των κρυπτογραφικών συστημάτων δημοσίου κλειδιού.
- Για να μπορέσει κάποιος τρίτος να αποκρυπτογραφήσει τα μηνύματα που ανταλλάζουν δύο άτομα μεταξύ τους θα πρέπει να γνωρίζει δύο κλειδιά, και το δημόσιο και το ιδιωτικό.
- Τα μηνύματα που αποστέλλονται δεν είναι δυνατό να τροποποιηθούν κατά τη διάρκεια της μετάδοσής τους, καθώς η οποιαδήποτε αλλοίωσή τους τα καθιστά μη δυνάμενα να αποκρυπτογραφηθούν, κάτι που θα γίνει αμέσως αντιληπτό από τον παραλήπτη.
- Το RSA είναι το πρώτο σύστημα δημόσιου κλειδιού που εφαρμόστηκε και βασίστηκε στο περίφημο πρόβλημα της **παραγοντοποίησης** μεγάλων ακεραίων.

Σύγκριση Συμμετρικής-Ασύμμετρης Κρυπτογραφίας (1)

- Τα ασύμμετρα κρυπτοσυστήματα είναι πολύ πιο αργά, αλλά παρέχουν μεγαλύτερη ασφάλεια.
- Στη συμμετρική κρυπτογραφία πρέπει το δημόσιο κλειδί να μοιραστεί στους χρήστες και παράλληλα να μείνει κρυφό από τους αντιπάλους.
- Στη συμμετρική κρυπτογραφία η ασφαλής μεταφορά του δημόσιου κλειδιού στους πιστοποιημένους χρήστες αποτελεί πολλές φορές σημαντικότερο θέμα επίλυσης και από την ασφαλή κρυπτογράφηση του μηνύματος.
- Το μήκος των κλειδιών που χρησιμοποιούνται στη συμμετρική κρυπτογράφηση είναι της τάξης των 56-bit ή 128-bit, τα οποία είναι πολύ μικρότερα των αντίστοιχων της ασύμμετρης κρυπτογραφίας.
- Ένα 80-bit συμμετρικό κλειδί ισοδυναμεί περίπου με ένα 1024-bit ασύμμετρο κλειδί.

Σύγκριση Συμμετρικής-Ασύμμετρης Κρυπτογραφίας (2)

- Για να επιτύχουμε την ασφάλεια που μας προσδίδει ένα 128-bit συμμετρικό κλειδί θα πρέπει να χρησιμοποιήσουμε ένα ασύμμετρο κλειδί μήκους 3000-bit.
- Η συμμετρική κρυπτογράφηση είναι πολύ πιο γρήγορη από την ασύμμετρη.
- Η συμμετρική κρυπτογράφηση χρησιμοποιείται για την κρυπτογράφηση μεγάλου μήκους κειμένου, το οποίο θέλουμε όμως να μείνει κρυφό από τους αντιπάλους για μικρό χρονικό διάστημα.
- Η κρυπτογράφηση με τον αλγόριθμο DES, είναι 100 φορές πιο γρήγορη από την αντίστοιχη με τον αλγόριθμο ασύμμετρης κρυπτογραφίας RSA σε έναν σύγχρονο επεξεργαστή και 10.000 φορές πιο γρήγορη όταν υλοποιηθεί σε ειδικό επεξεργαστή.
- Ένα συμμετρικό κρυπτογραφικό σύστημα που βασίζεται σε ένα κλειδί μήκους 56-bit είναι μη ασφαλές, αλλά είναι τόσο οικονομικό που μπορεί να χρησιμοποιηθεί από απλούς χρήστες που δεν πρέπει να διαφυλάξουν πολύτιμα δεδομένα, τα οποία μάλιστα δε είναι δυνατόν να διαφυλαχτούν από αποφασισμένους εισβολείς.

Βασικές έννοιες της Θεωρίας Αριθμών.

- Η πράξη modulo. $x_1 = x_2 (\mathrm{mod}\ n)$
  - Η ισότητα ισχύει αν και μόνο αν:
    - $x_1 - x_2 = \alpha / \beta$ με α, β ακέραιους
    - gcd (α, β) = 1 (μέγιστος κοινός διαιρέτης)
    - α διαιρείται από το n
- Ο **αντίστροφος** ενός αριθμού x_1, x_1^{-1} (modn), ορίζεται σαν τον αριθμό ο οποίος αν πολλαπλασιαστεί με τον x_1 δίνει 1(mod n).
- Δύο αριθμοί είναι **σχετικά πρώτοι** όταν ο μέγιστος κοινός διαιρέτης τους είναι η μονάδα.

Παραδείγματα αναγωγής σε modulo n.

- 25 = 4 (mod 7) (γιατί 25 - 4 = 21 = $3 \cdot 7$)
- -5 = 3 (mod 4) (γιατί -5 -3 = -8 = $-2 \cdot 4$)
- 6^{-1}= 1 (mod 5)
  (γιατί $1 \cdot 6 = 6$ και 6 = 1 (mod 5))

- $\frac{2}{5} = 1 (\mathrm{mod} 3)$ (γιατί $\frac{2}{5} - 1 = \frac{-3}{5} = 3 \cdot \frac{-1}{5}$)

Τι είναι ομάδα.

- **Ομάδα** (group) ονομάζουμε ένα σύνολο αριθμών οι οποίοι έχουν μια καθορισμένη αριθμητική πράξη.
- Δύο ομάδες που χρησιμοποιούνται στην κρυπτογραφία είναι η Z_n, η προσθετική ομάδα των ακεραίων modulo του αριθμού n και η ομάδα Z_p^*, η πολλαπλασιαστική ομάδα ακεραίων modulo του πρώτου αριθμού p.

Η ομάδα Z_n.

- Η ομάδα Z_n χρησιμοποιεί μόνο ακέραιους από το 0 έως το n – 1.
- Η βασική της πράξη είναι η πρόσθεση, η οποία καταλήγει ανάγοντας το τελικό αποτέλεσμα στο modulo n.
- Η modulo μείωση κατά n εξασφαλίζει ότι το αποτέλεσμα της άθροισης είναι μεταξύ του 0 και του n – 1.

Παράδειγμα: Η προσθετική ομάδα Z_{15}.

- Η Z_{15} χρησιμοποιεί ακεραίους από το 0 έως το 14.
- (10 + 12) mod 15 = 22 mod 15 = 7
  (4 + 11) mod 15 = 15 mod 15 = 0.
  Στο Z_{15}, 10 + 12 = 7 και 4 + 11 = 0.
- Παρατηρείστε ότι και οι δύο υπολογισμοί έχουν αποτέλεσμα μεταξύ του 0 και του 14.
- Άλλες πράξεις μπορούν να εξαχθούν από την πρόσθεση. Π.χ. η αφαίρεση x – y μπορεί να παρουσιαστεί σαν πρόσθεση του x + (-y) mod n.
- Στο Z_{15} για παράδειγμα είναι: 1 - 4 = 1 + (-4) = 1 + 11 mod 15 = 12.

Η ομάδα Z_p^*.

- Η πολλαπλασιαστική ομάδα Z_p^* χρησιμοποιεί μόνο ακεραίους ανάμεσα στο 1 και το p – 1 (p είναι ένας πρώτος αριθμός), και η βασική της πράξη είναι ο πολλαπλασιασμός.
- Ο πολλαπλασιασμός ολοκληρώνεται παίρνοντας το υπόλοιπο της διαίρεσης με το p.

Παράδειγμα: Η πολλαπλασιαστική ομάδα Z_{11}^*.

$$4 \cdot 7 \bmod 11 = 28 \bmod 11 = 6 \quad 9 \cdot 5 \bmod 11 = 45 \bmod 11 = 1$$

Έτσι, στο Z_{11}^* : $4 \cdot 7 = 6$ και $9 \cdot 5 = 1$

Κάθε αριθμός x σε μια πολλαπλασιαστική ομάδα έχει κάποιο στοιχείο στην ομάδα ως πολλαπλασιαστικό αντίστροφο. Αυτό είναι κάποιος ακέραιος αριθμός x^{-1} τέτοιος ώστε $x \cdot x^{-1} = 1$ στην ομάδα.

Αβελιανές Ομάδες.

- Μια αριθμητική πράξη λέγεται ότι είναι αντιμεταθετική αν η σειρά από τα σύμβολα των πράξεων της είναι ασήμαντη.
- Μια ομάδα λέγεται **αβελιανή** αν η βασική της πράξη είναι αντιμεταθετική. Έτσι μια προσθετική ομάδα λέγεται αβελιανή αν ισχύει: a + b = b + a για όλα τα στοιχεία a, b που ανήκουν στην ομάδα.
- Η προσθετική ομάδα Z_n και η πολλαπλασιαστική ομάδα Z_p^* είναι και οι δύο αβελιανές ομάδες.

Πεπερασμένα Σώματα.

- **Σώμα** ονομάζεται ένα σύνολο από στοιχεία με δύο ορισμένες αριθμητικές πράξεις μέσα σε αυτό: πιο συχνά είναι, η πρόσθεση και ο πολλαπλασιασμός.
- Τα στοιχεία του σώματος είναι μια προσθετική αβελιανή ομάδα, και τα μη μηδενικά στοιχεία του σώματος αποτελούν μια πολλαπλασιαστική αβελιανή ομάδα.
- Όλα τα στοιχεία του σώματος έχουν αντίθετο, και όλα τα μη μηδενικά στοιχεία της ομάδας έχουν πολλαπλασιαστικό αντίστροφο.
- Ένα σώμα ονομάζεται **πεπερασμένο** όταν έχει ένα πεπερασμένο αριθμό στοιχείων. Τα πιο γνωστά πεπερασμένα σώματα δεδομένης τάξης, που χρησιμοποιούνται στην κρυπτογραφία είναι τα σώματα F_p (όπου p ένας πρώτος αριθμός) και F_2m.

Το σώμα F_p.

- Το πεπερασμένο σώμα F_p (το p είναι ένας πρώτος αριθμός) αποτελείται από τους αριθμούς από το 0 μέχρι το p – 1. Οι πράξεις του σώματος είναι η πρόσθεση και ο πολλαπλασιασμός. Οι πράξεις αυτές ορίζονται για τις ομάδες Z_n και Z_p^* αντίστοιχα: όλοι οι υπολογισμοί ολοκληρώνονται με αναγωγή στο modulo p.
- Ο περιορισμός ώστε το p να είναι πρώτος αριθμός είναι απαραίτητος έτσι ώστε όλα τα μη μηδενικά στοιχεία να έχουν πολλαπλασιαστικό αντίστροφο.

Παράδειγμα: Το σώμα F_{23}.

$$10 \cdot 4 - 11 \bmod 23 =$$
$$= 29 \bmod 23 = 6$$

$$7^{-1} \bmod 23 =$$
$$= 10$$

αφού

$$7 \cdot 10 \bmod 23 =$$
$$= 70 \bmod 23 = 1$$

$$8^3/_7 \bmod 23 =$$
$$= 512/_7 \bmod 23 =$$
$$= 6 \cdot 7^{-1} \bmod 23 =$$
$$= 6 \cdot 10 \bmod 23 = 14$$

Το σώμα F_2m.

- Παρόλο που η περιγραφή του σώματος F_2m είναι πολύπλοκη, αυτό το σώμα είναι πάρα πολύ χρήσιμο διότι οι υπολογισμοί σε αυτό μπορούν να γίνουν αποτελεσματικά όταν υλοποιούνται στους υπολογιστές.
- Υπάρχουν αρκετοί τρόποι για να περιγραφεί η αριθμητική στο σώμα F_2m. Η **πολυωνυμική αναπαράσταση**, είναι η πιο γνωστή.

Πολυωνυμική Αναπαράσταση.

- Τα στοιχεία του σώματος F_2m είναι πολυώνυμα βαθμού μικρότερου του m, με συντελεστές στο σώμα F_2. Έτσι είναι, $\mathbf{\{a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + ... + a_2x^2 + a_1x + a_0 \mid a_i = 0 \text{ ή } 1\}}$. Αυτά τα στοιχεία μπορούν να γραφούν σε μορφή διανύσματος ως εξής: $\mathbf{(a_{m-1} ... a_1 a_0)}$. Το σώμα F_2m έχει 2^m στοιχεία.
- Οι βασικές πράξεις στο σώμα F_2m είναι η πρόσθεση και ο πολλαπλασιασμός.
- Το πολυώνυμο f(x) που χρησιμοποιείται στον πολλαλασιασμό πρέπει να είναι μη αναγόμενο, δηλαδή δε μπορεί να παραγοντοποιηθεί σε 2 μικρότερα πολυώνυμα.

Πράξεις στην Πολυωνυμική Αναπαράσταση (1).

- **Πρόσθεση**
  - **$(a_{m-1} \dots a_1\ a_0) + (b_{m-1} \dots b_1\ b_0) = (c_{m-1} \dots c_1\ c_0)$** όπου το **$c_i = a_i + b_i$** ανήκει στο F_2.
  - Η πρόσθεση είναι θεωρητικά το XOR του **$(a_{m-1} \dots a_1\ a_0)$** και **$(b_{m-1} \dots b_1\ b_0)$**.
- **Αφαίρεση**
  - Στο σώμα F_2m, κάθε στοιχείο **$(a_{m-1} \dots a_1\ a_0)$** έχει σαν συμμετρικό τον ίδιο τον εαυτό του, αφού ισχύει **$(a_{m-1} \dots a_1\ a_0) + (a_{m-1} \dots a_1\ a_0) = (0 \dots 0\ 0)$.**
  - Έτσι η πρόσθεση και η αφαίρεση είναι ισοδύναμες πράξεις στο F_2m .

Πράξεις στην Πολυωνυμική Αναπαράσταση (2).

- **Πολλαπλασιασμός**
  - Έχουμε $(a_{m-1} \ldots a_1\ a_0)\ (b_{m-1} \ldots b_1\ b_0) = (r_{m-1} \ldots r_1\ r_0)$, όπου $r_{m-1}x_{m-1} + \ldots + r_1x + r_0$ είναι το υπόλοιπο του πολυωνύμου $(a_{m-1}x_{m-1} + \ldots + a_1x + a_0)\ (b_{m-1}x_{m-1} + \ldots + b_1x + b_0)$ διαιρούμενο με το πολυώνυμο f(x) στο σώμα F_2. (Σημειώστε ότι όλοι οι συντελεστές του πολυωνύμου μειώνονται modulo 2).
  - Όλοι οι συντελεστές του πολυωνύμου μειώνονται modulo 2.
- **Εκθετοποίηση**
  - Η εκθετοποίηση $(a_{m-1} \ldots a_1\ a_0)^e$ παρουσιάζεται πολλαπλασιάζοντας μαζί e αντίγραφα του $(a_{m-1} \ldots a_{1\ a0})$.

Παράδειγμα Πολυωνυμικής Αναπαράστασης (στο $F_2 4$) (1).

- Τα στοιχεία του $F_2 4$ είναι παρακάτω 16 διανύσματα:

(0000) (0001) (0010) (0011) (0100) (0101) (0110) (0111)
(1000) (1001) (1010) (1011) (1100) (1101) (1110) (1111).

•Το μη αναγόμενο πολυώνυμο θα είναι το **$f(x) = x^4 + x + 1$.**

•Πρόσθεση: (0110) + (0101) = (0011)

•Πολλαπλασιασμός: (1101) (1001)
$= (x^3 + x^2 + 1)(x^3 + 1) \bmod f(x)$
$= x^6 + x^5 + 2x^3 + x^2 + 1 \bmod f(x)$
$= x^6 + x^5 + x^2 + 1 \bmod f(x)$ **(οι συντελεστές μειώνονται κατά modulo 2)**

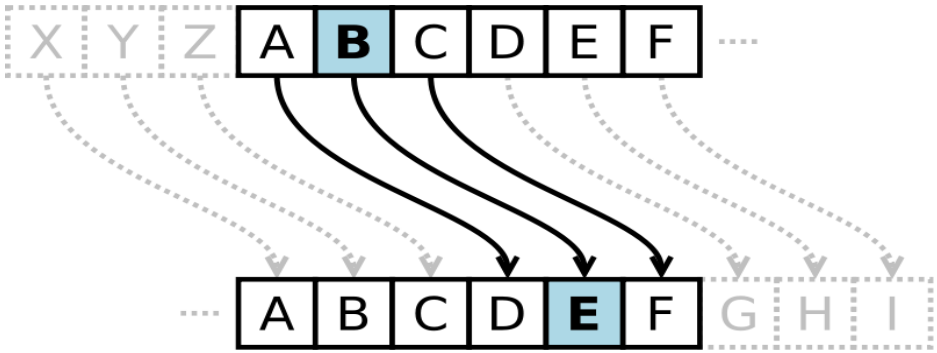
$= (x^4 + x + 1)(x^2 + x) + (x^3 + x^2 + x + 1) \bmod f(x)$ **(Διαιρέσαμε το $x^6 + x^5 + x^2 + 1$ με το $x^4 + x + 1$)**
$= x^3 + x^2 + x + 1 = (1111).$

Το Κινέζικο Θεώρημα του υπολοίπου.

- Το Κινέζικο Θεώρημα υπολοίπου μας παρέχει μια αντιστοιχία μεταξύ ενός συστήματος εξισώσεων modulo, το οποίο είναι ένα σύστημα ανά δύο σχετικά πρώτων moduli (όπως για τους αριθμούς 3, 5, 7) και μιας εξίσωσης modulo με το γινόμενό τους (όπως 105).
- Το Κινέζικο Θεώρημα του Υπολοίπου εφαρμόζεται κατά την μέτρηση των σημείων μιας ελλειπτικής καμπύλης.
- Ας υποθέσουμε ότι ο ακέραιος n παραγοντοποιείται ως $n= n_1 \cdot n_2 \cdots n_k$, όπου οι παράγοντες n_i είναι ανά δύο σχετικά πρώτοι. Το Κινέζικο θεώρημα υπολοίπων περιγράφει τη δομή του Z_n ως ταυτόσημη με τη δομή του Καρτεσιανού γινομένου $Z_{n1} \times Z_{n2} \times \ldots \times Z_{nk}$ με πρόσθεση και πολλαπλασιασμό modulo n_i στην i^n συνιστώσα.
- Μπορεί να χρησιμοποιηθεί προκειμένου να προκύψουν αποτελεσματικοί αλγόριθμοι, επειδή το να δουλεύει κανείς σε καθένα από τα αλγεβρικά συστήματα Z_{ni} είναι δυνατό να είναι πιο αποτελεσματικό από το να δουλεύει modulo n.
- Αντίστοιχο παράδειγμα παρατίθεται στην εργασία.

Ο Αλγόριθμος του Καίσαρα.

- Ο αλγόριθμος του Καίσαρα, ή αλλιώς Αλγόριθμος Αλλαγής Κατεύθυνσης, είναι ο πιο απλός και ο πιο γνωστός αλγόριθμος κρυπτογράφησης.
- Η ονομασία του αλγορίθμου πάρθηκε από τον Ιούλιο Καίσαρα που τον χρησιμοποίησε για να επικοινωνεί με τα στρατεύματα του μυστικά.
- Η λειτουργία του βασίζεται στην αντικατάσταση κάθε χαρακτήρα του μηνύματος από έναν άλλο χαρακτήρα, ο οποίος βρίσκεται μερικές συγκεκριμένες θέσεις πιο μακριά από τον πρώτο χαρακτήρα.
- Για παράδειγμα, αν το κλειδί που θα χρησιμοποιήσουμε είναι το 3 τότε οι θέσεις της μετακίνησης είναι τρεις. Έτσι, το A θα γίνει D, το B θα γίνει E και ούτω καθεξής



Παραδείγματα του Αλγόριθμου του Καίσαρα.

- Αν το κλειδί είναι το 3 θα έχουμε:
- Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Cipher: DEFGHIJKLMNOPQRSTUVWXYZABC
- Έτσι, κάθε γράμμα στη πρώτη σειρά θα αντικατασταθεί από το αντίστοιχο του στη δεύτερη. Έτσι, στο παρακάτω παράδειγμα θα έχουμε:
- Plaintext: the quick brown fox jumps over the lazy dog
- Ciphertext: wkh txlfn eurzq ira mxpsv ryhu wkh odcb grj Επίσης, μπορούμε να χρησιμοποιήσουμε και την modulo αριθμητική για την μετατροπή των χαρακτήρων σε αριθμούς. Αντικαθιστούμε κάθε χαρακτήρα με έναν αριθμό: A=0, B=1, …, Z=25. Η κρυπτογράφηση ενός χαρακτήρα x, με κλειδί το n θα μας δώσει τον y.
- Το αποτέλεσμα είναι πάντα modulo 26 και μας δίνει πάντα ακέραιους αριθμούς από το 0 ως το 25.

Δυνατότητες και σπάσιμο του Αλγόριθμου του Καίσαρα.

- Ο αλγόριθμος μπορεί να σπάσει μέσα σε δευτερόλεπτα με τη μέθοδο της εξαντλητικής αναζήτησης ή αλλιώς brutal force attack, αρκεί ο επιτιθέμενος απλά να υποπτευθεί ότι γίνεται χρήση κρυπτογράφησης με αντικατάσταση.
- Έχοντας το κρυπτογραφημένο κείμενο δοκιμάζουμε όλα τα κλειδιά ένα ένα μέχρι να δούμε ότι παίρνουμε το αρχικό κείμενο.
- Επίσης, μία άλλη μέθοδος αποκρυπτογράφησης και εντοπισμού του κλειδιού κρυπτογράφησης είναι αυτή της ανάλυση σε σχέση με τη συχνότητα Frequency Analysis.
- Με τη μέθοδο αυτή βλέπουμε ποια γράμματα συναντάμε πιο συχνά στο κρυπτογραφημένο κείμενο. Έτσι, γνωρίζοντας ποια γράμματα γενικά συναντάμε πιο συχνά στην αλφαβήτα (π.χ. το Ε και το Τ συναντιούνται συχνά με μια συγκεκριμένη συχνότητα) μπορούμε να μαντέψουμε ποιο αντιστοιχεί σε ποιο και έτσι να βρούμε το κλειδί κρυπτογράφησης.

Η Ιστορία του Αλγόριθμου DES.

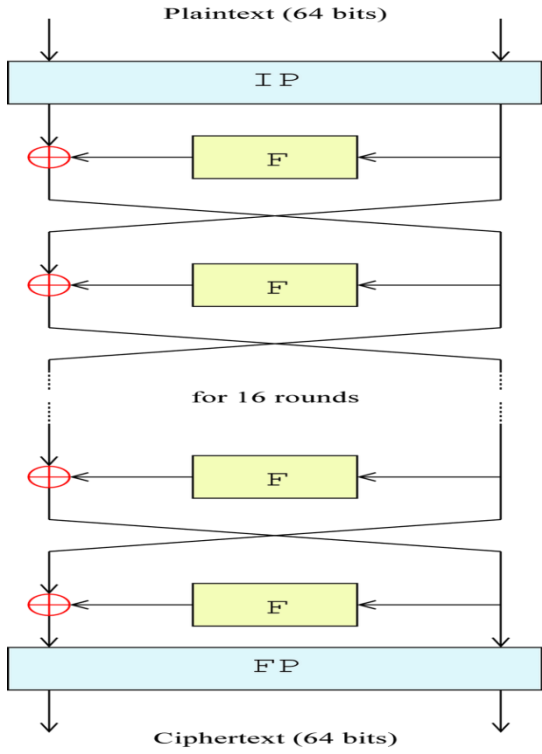
- Η αρχή της δημιουργίας του DES (Data Encryption Standard) ή αλλιώς DEA (Data Encryption Algorithm) χρονολογείται γύρω στο 1970.
- Συγκεκριμένα, το 1972 το NIST (National Institute of Standards and Technology) στις Ηνωμένες Πολιτείες Αμερικής όρισε διαγωνισμό με σκοπό τη δημιουργία κρυπτογραφικού συστήματος για να προστατευθούν κρίσιμες πληροφορίες του Υπουργείου Εμπορίας της χώρας.
- Μετά από διάφορες αποτυχημένες προσπάθειες μέσα στο 1973, τον Αύγουστο του 1974 η IBM υπέβαλε υποψηφιότητα με έναν αλγόριθμο, που βασιζόταν στον αλγόριθμο Lucifer του Horst Feistel. Ο Lucifer χρησιμοποιήθηκε το 1970 σε μια εφαρμογή για e-banking.
- Έτσι, το 1977 η ομάδα της IBM, που αποτελούταν από τους Feistel, Tuchman, Coppersmith, Konheim, Meyer, Matyas, Adler, Grossman, Notz, Smith και Tuckerman, υλοποίησε τη τελική μορφή του DES.

Ο Data Encryption Standard (DES)

- Αρχικά τα πλεονεκτήματα ήταν τα εξής:
  - Υψηλό επίπεδο Ασφάλειας
  - Χαμηλό κόστος υλοποίησης
  - Γρήγορη Κρυπτογράφηση – Αποκρυπτογράφηση
- Όμως, το κλειδί του είναι πολύ μικρό: 56 bits μέγεθος, δηλαδή $2^{56} \approx 72 \cdot 10^{15}$ κλειδιά
- Το ισχύον DES (Data Encryption Standard), είναι αρκετά παλιό και πλέον ευάλωτο σε επιθέσεις από τους όλο και ισχυρότερους Η/Υ.

Περιγραφή του Data Encryption Standard (DES)

- Παίρνει ένα string από bits IP (Initial Permutation) και με σύνθετες διεργασίες το μετατρέπει σε ένα διαφορετικό string από bits FP (Final Permutation).
- Το μήκος του string αυτού είναι 64 bits (τα 8 χρησιμοποιούνται σαν bits ισοτιμίας).
- Για να γίνει αυτή η μετατροπή χρησιμοποιείται ένα κλειδί 64άρων bits, από τα οποία μόνο τα 56 χρησιμοποιούνται.
- Ουσιαστικά γίνονται 16 αντιμεταθέσεις των bits μέχρι να πάμε από την αρχική μορφή IP του string από bits στη τελική του μορφή FP.
- Αν η σειρά των κλειδιών που χρησιμοποιούνται για τη κρυπτογράφηση είναι {k1, k2, k3,….,k15}, τότε η σειρά των κλειδιών για την αποκρυπτογράφηση θα είναι η αντίστροφη, δηλαδή {k15, k14, k13,….,k1}.
- Αρχικά το block χωρίζεται σε 2 ίσα μέρη των 32 bits.
- Η συνάρτηση F μπερδεύει το μισό block με τη βοήθεια του κλειδιού και το αποτέλεσμα συνδυάζετε με το άλλο μισό block με ένα XOR.
- Στο νέο block που προκύπτει από το XOR εφαρμόζουμε το 2ο κλειδί και ξαναμπερδεύεται το block για να συνδυαστεί με τη χρήση XOR με το block των bits που υπήρχε πριν εφαρμοστεί το 1ο κλειδί επάνω του.
- Αυτό γίνεται 15 φορές μέχρι τη τελική αντιμετάθεση.



Ασφάλεια και απαιτήσεις του DES. (1)

- Το σπάσιμο του DES μπορεί να γίνει με την «εξαντλητική αναζήτηση». Το σύνολο των κλειδιών που πρέπει να δοκιμαστούν είναι περίπου 72 τετράκις εκατομμύρια. Επομένως ήταν θέμα χρόνου και κόστους για να σπάσει ο αλγόριθμος. Ο χρόνος με το κόστος είναι αντιστρόφως ανάλογα.
- 10 χρόνια χρειάζονται για έναν απλό σύγχρονο επεξεργαστή και 1 απόγευμα για έναν νέο επεξεργαστή που θα κατασκευαστεί αποκλειστικά για το σπάσιμο του DES. Ο επεξεργαστής αυτός θα κόστιζε όμως πάνω από 20.000.000 $ το 1997 (Garon – Outbridge).

Απαιτήσεις σε δολάρια $ για το σπάσιμο του DES

Έτος	1 Χρόνος	1 Μήνας	1 Εβδομάδα	1 Ημέρα
1990	129.000	1.532.000	6.664.000	46.622.000
1995	52.000	600.000	2.611.000	18.265.000
2000	10.300	117.000	510.000	3.580.000

Ασφάλεια και απαιτήσεις του DES. (2)

•Ο προηγούμενος πίνακας έγινε μετά από υπολογισμούς που έγιναν από τον Garon και τον Outerbridge

•Οι τιμές των micro-chips διαφέρουν κάθε χρονολογικό έτος. Έτσι, οι τιμές τους ήταν οι εξής:

- •Το 1990, το 1 Mhz chip κόστιζε 25$, το 2 Mhz chip κόστιζε 250$, ενώ το 4 Mhz chip ήταν πολύ ακριβό για την εποχή.
- •Το 1995, το 2 Mhz chip κόστιζε 25$, το 4 Mhz chip κόστιζε 250$, ενώ το 32 Mhz chip ήταν πολύ ακριβό για την εποχή.
- •Το 2000, το 4 Mhz chip κόστιζε 25$, το 32 Mhz chip κόστιζε 250$, ενώ το 256 Mhz chip ήταν πολύ ακριβό για την εποχή.

Συμπεράσματα χρήσης του DES.

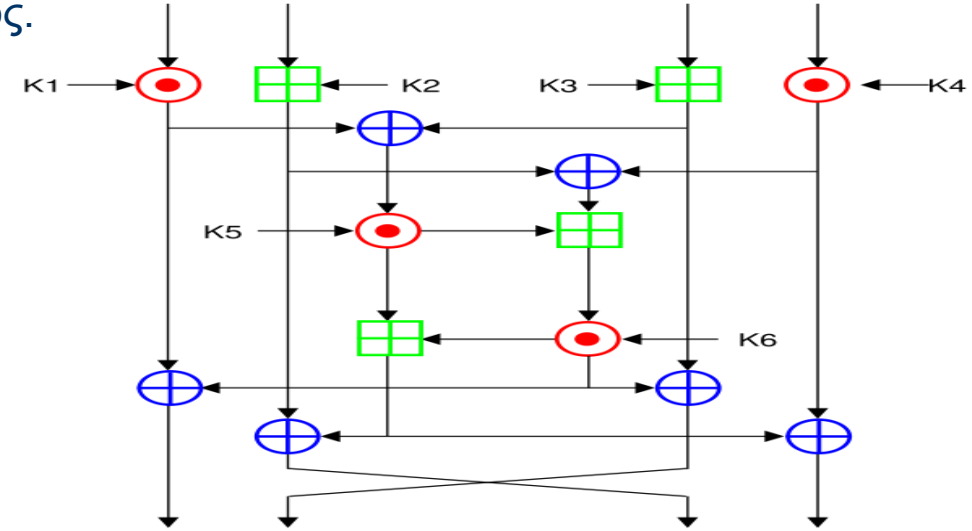
- Συμπεράσματα:
  - Εύκολη και φθηνή υλοποίηση
  - Μικρή ασφάλεια
  - Χρήση μόνο για την ασφάλεια δεδομένων που θέλουμε να διαφυλαχτούν προσωρινά.
  - Χρήση για την ακεραιότητα των δεδομένων και όχι για την μόνιμη απόκρυψή τους
  - Χρήση μόνο όταν ο χρόνος για την εύρεση του κλειδιού είναι μικρότερος από τον αντίστοιχο χρόνο για την απόκρυψη των δεδομένων.

Η Ιστορία του Αλγόριθμου IDEA (International Data Encryption Algorithm)

- Ο IDEA (International Data Encryption Algorithm) είναι ένας κρυπτογραφικός αλγόριθμος που σχεδιάστηκε από τους Lai X. και Massey J. του Πανεπιστημίου Τεχνολογίας της Ζυρίχης το 1991.
- Σχεδιάστηκε για να αντικαταστήσει τον DES και αποτελεί μια επανάληψη του αλγόριθμου PES (Proposed Encryption Standard), γι' αυτό και ο IDEA αποκαλείται αλλιώς και IPES (Improved PES).
- Είναι ελεύθερος για μη-εμπορική χρήση και τα δικαιώματά του ανήκουν στην εταιρεία MediaCrypt, μέχρι το 2011.
- Χρησιμοποιήθηκε στην εφαρμογή PGP (Pretty Good Privacy) v2.0. Η εφαρμογή αυτή παρέχει κρυπτογράφηση και πιστοποίηση και χρησιμοποιείται ευρέως για την κρυπτογράφηση και αποκρυπτογράφηση στο ηλεκτρονικό ταχυδρομείο, όπου και παρέχει ασφάλεια. Δημιουργήθηκε το 1991 από τον Philip Zimmermann.

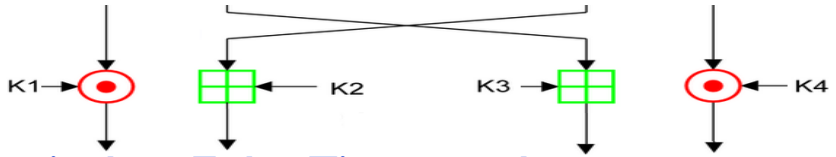
Περιγραφή του Αλγόριθμου IDEA (1).

- Ο αλγόριθμος IDEA χρησιμοποιεί κλειδιά μεγέθους 128-bit, τα οποία τα εφαρμόζει στο κείμενο σε 8 γύρους. Έτσι, λόγω του μεγαλύτερου μεγέθους κλειδιού από αυτό του DES παρέχει μεγαλύτερη ασφάλεια από αυτόν. Η κρυπτογράφηση γίνεται σε ένα block μήκους 64-bit με τη χρήση κλειδιού μήκους 128-bit. Η κρυπτογράφηση ολοκληρώνεται μετά από 8 γύρους και μια τελευταία μετατροπή που ονομάζεται μισός γύρος.



Περιγραφή του Αλγόριθμου IDEA (2).

- Οι πράξεις που λαμβάνουν χώρα είναι οι εξής:
  - Η αποκλειστική διάζευξη, το γνωστό XOR (eXclusive OR) (συμβολίζεται με έναν μπλε σταυρό ⊕).
  - Η πρόσθεση modulo 2^{16} (συμβολίζεται με έναν πράσινο σταυρό).
  - Ο πολλαπλασιασμός modulo $2^{16}+1$, (συμβολίζεται με μία κόκκινη βούλα).
- Όπως βλέπουμε η είσοδος είναι τετραπλή, δηλαδή η 64-bit ψηφιολέξη χωρίζεται σε 4 ψηφιολέξεις των 16-bit. Το κλειδί K έχει μήκος 128-bit και διασπάται σε 6 κλειδιά (k1, k2, k3, …, k6) των 16-bit. Τα πρώτα 8 bits του κλειδιού αφαιρούνται από το κλειδί από την αρχή. Έτσι, το k1 του πρώτου γύρου αποτελείται από τα πρώτα 16 bits του κλειδιού και κάθε φορά που ξεκινάει ο κάθε γύρος μετακινούνται όλα τα ψηφία του κλειδιού κατά 25 θέσεις αριστερά.
- Οι πράξεις αυτές θα γίνουν 8 φορές όπως φαίνεται στο σχήμα. Κατόπιν, θα εφαρμοστεί ο τελευταίος «μισός γύρος».



Ασφάλεια του Αλγόριθμου IDEA.

- Οι σχεδιαστές όταν δημιούργησαν τον αλγόριθμο, τον ανέλυσαν και μέτρησαν τις αντοχές του σε επιθέσεις με διαφορική κρυπτανάλυση.
- Τα συμπεράσματα ήταν αρκετά ικανοποιητικά.
- Το 1994, βρέθηκαν κάποιες ομάδες κλειδιών του αλγορίθμου που ήταν πολύ πιο ευπαθείς από τις άλλες. Όμως, λόγω του μεγάλου μήκους κλειδιού (128-bit) και επομένως και του μεγάλου αριθμού κλειδιών που υπάρχουν (2^{128} κλειδιά), αυτό δεν αποτέλεσε σπουδαίο πρόβλημα.
- Το 2005 όμως, δημοσιεύτηκε μία εργασία που με τη μέθοδο της εξαντλητικής αναζήτησης έβρισκε το κλειδί του αλγορίθμου, ο οποίος τότε υλοποιούταν σε 6 γύρους και όχι σε 8.
- Έτσι, το 2005 η MediaCrypt δημιούργησε μια νέα έκδοση του αλγόριθμου με μεγαλύτερη ασφάλεια, τον IDEA NTX.

Η ιστορία του Αλγόριθμου Advanced Encryption Standard (AES).

- Ο AES δημιουργήθηκε με την προοπτική να αντικαταστήσει τον DES, όταν αυτός είχε πια φτάσει στο τέλος της ζωής του και όταν πια η ασφάλεια του ξεπεράστηκε.
- Το 1997, ανακοινώθηκε ένας διαγωνισμός από το NIST (National Institute of Standards and Technology) στις Η.Π.Α, στον οποίο υπήρξαν 15 υποψηφιότητες.
- Τελικά νικητής του διαγωνισμού ανακηρύχτηκε το προϊόν του οποίου δημιουργοί ήταν οι Joan Daemen και Vincent Rijmen από το Βέλγιο. Αυτοί ήταν και οι δημιουργοί του αλγόριθμου με την ονομασία Rijndael.
- Ο συγκεκριμένος αλγόριθμος είναι αρκετά πολύπλοκος, αλλά η ασφάλεια που παρέχει είναι αρκετά καλή και επίσης είναι αρκετά γρήγορος. Ο AES χρησιμοποιείται κυρίως στις έξυπνες κάρτες.

Η ιστορία του Αλγόριθμου Advanced Encryption Standard (AES).

- Ο AES δημιουργήθηκε με την προοπτική να αντικαταστήσει τον DES, όταν αυτός είχε πια φτάσει στο τέλος της ζωής του και όταν πια η ασφάλεια του ξεπεράστηκε.
- Το 1997, ανακοινώθηκε ένας διαγωνισμός από το NIST (National Institute of Standards and Technology) στις Η.Π.Α, στον οποίο υπήρξαν 15 υποψηφιότητες.
- Τελικά νικητής του διαγωνισμού ανακηρύχτηκε το προϊόν του οποίου δημιουργοί ήταν οι Joan Daemen και Vincent Rijmen από το Βέλγιο. Αυτοί ήταν και οι δημιουργοί του αλγόριθμου με την ονομασία Rijndael.
- Ο συγκεκριμένος αλγόριθμος είναι αρκετά πολύπλοκος, αλλά η ασφάλεια που παρέχει είναι αρκετά καλή και επίσης είναι αρκετά γρήγορος. Ο AES χρησιμοποιείται κυρίως στις έξυπνες κάρτες.

Η λειτουργία του Αλγόριθμου AES (1).

- Έστω έχουμε τη πληροφορία: 11010100
- Σχηματισμός πολυώνυμου βαθμού < 8 ,οπότε σχηματίζεται το πολυώνυμο $\mathbf{x^7 + x^6 + x^4 + x^2}$
- Γενικά θα ισχύει:
  - Ένα byte θα αποτελείται από τα εξής bits

$$\{b_7,\ b_6,\ b_5,\ b_4,\ b_3,\ b_2,\ b_1,\ b_0\}$$

  - Το πολυώνυμο που θα προκύπτει θα είναι της μορφής

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 = \sum_{i=0}^{7} b_i x^i$$

Η λειτουργία του Αλγόριθμου AES (2).

- Ο αλγόριθμος χρησιμοποιεί σε κάθε στάδιο λειτουργίας του αρκετές μαθηματικές πράξεις οι οποίες θεωρούμε ότι επενεργούν στα στοιχεία του πεπερασμένου σώματος **GF(2^8)**:
  - ***Πρόσθεση***:Η πρόσθεση είναι η XOR των bits, πχ.

    $$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) =$$
    $$x^7 + x^6 + x^4 + x^2$$

  - ***Πολλαπλασιασμός***: Πολλαπλασιασμός στο **GF(2^8)** είναι ο πολλαπλασιασμός μεταξύ πολυωνύμων modulo(ένα ανάγωγο (irreducible) πολυώνυμο βαθμού 8). Ανάγωγο ονομάζεται ένα πολυώνυμο αν διαιρείται μονάχα από τον εαυτό του και την μονάδα. Το πολυώνυμο που έχει επιλεχθεί για το AES είναι το :

    $$m(x)= x^8 + x^4 + x^3 + x + 1$$

Η λειτουργία του Αλγόριθμου AES (3).

- Αρχικά ας πολλαπλασιάσουμε το $x^7 + x^6 + x^3 + x+1$ με το x :

  $(x^7 + x^6 + x^3 + x+1)\cdot x = x^8 + x^7 + x^4 + x^2 + x$

  $\equiv x^8 + x^7 + x^4 + x^2 + x \bmod (x^8 + x^4 + x^3+ x+1)$

  $\equiv (x^7 + x^3 + x^2 +1)$

- Η ίδια πράξη με bits γίνεται:

  11001011 => 110010110 (ολίσθηση (shift) αριστερά και προσθήκη ενός 0) =>110010110 + 100011011 = 010001101 που αντιστοιχεί στο προηγούμενο αποτέλεσμα.

Η λειτουργία του Αλγόριθμου AES (4).

- Συμμετρική μπλοκ διαδικασία κρυπτογράφησης μυστικού κλειδιού
- Μήκος κλειδιού 128,192,256 bits (cipher keys). AES-128, AES-192, AES-256
- Είσοδοι και έξοδοι αλγορίθμου σταθερού μήκους 128 bits

Η λειτουργία του Αλγόριθμου AES (5).

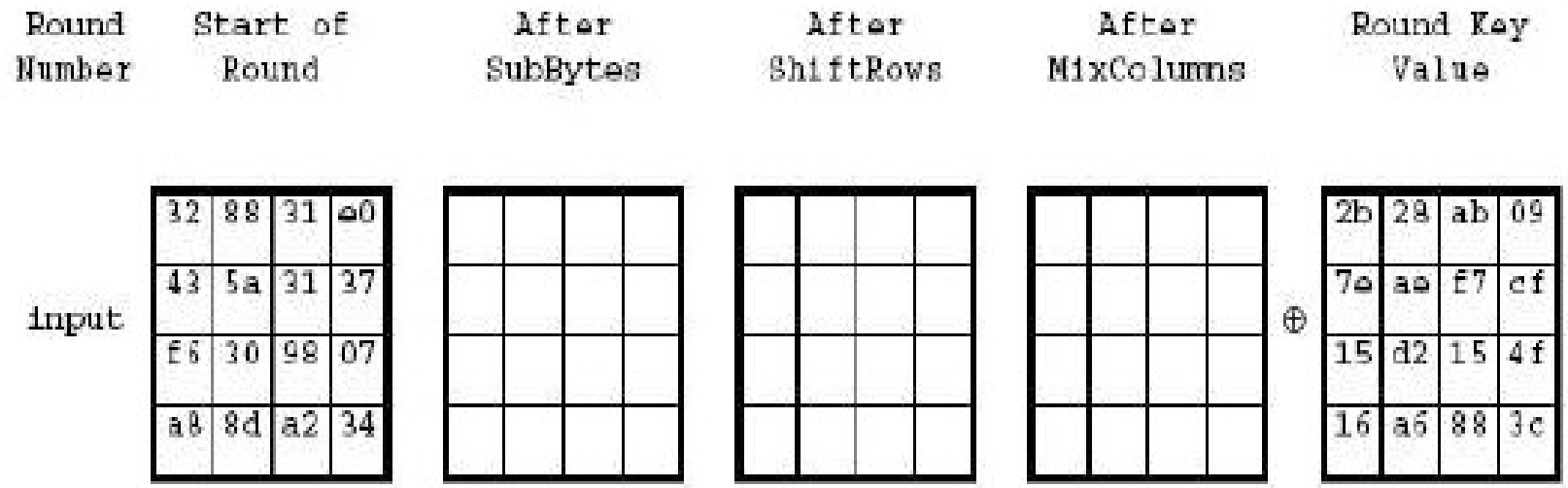
- Όλες οι λειτουργίες που επιτελεί ο αλγόριθμος γίνονται πάνω σε ένα δισδιάστατο πίνακα που αποκαλείται Κατάσταση (State)
- Αφού 1 byte είναι 8 bits, το μέγεθος του block των 128 bits είναι 128/8 = 16 bytes.
- Ο AES λειτουργεί σε έναν πίνακα 4×4 bytes
- Ο αλγόριθμος βασίζεται σε συνεχείς αλλαγές των bytes του κειμένου βασισμένες στο κλειδί και στη συνέχεια η αποκρυπτογράφηση βασίζεται πάλι στο ίδιο κλειδί.
- Στη διαδικασία κρυπτογράφησης υπάρχουν τέσσερις κυκλικές συναρτήσεις:
  - SubByte
  - ShiftRow
  - MixColumns
  - AddRound Key

Η λειτουργία του Αλγόριθμου AES (6).

- Ο πίνακας αυτός περιλαμβάνει τέσσερις γραμμές από bytes, τόσες στήλες (**Nb**) το οποίο ισούται με το μήκος του block (block length) διαιρούμενο με το 32
- Ένας άλλος τρόπος να δει κάποιος τα περιεχόμενα της State είναι σαν 32-bit λέξεις (words) αντί για bytes.
- Η μεταβλητή **Nk** συμβολίζει τον αριθμό των 32-bit λέξεων που μπορεί να περιλαμβάνει ένα κλειδί και κατά συνέπεια μπορεί να πάρει τις τιμές 4, 6 και 8
- Η μεταβλητή **Nr** χρησιμοποιείται για να δηλώσει το πλήθος των γύρων
  - AES-128 Nr=10
  - AES-192 Nr=12
  - AES-256 Nr=14

Η λειτουργία του Αλγόριθμου AES (7).

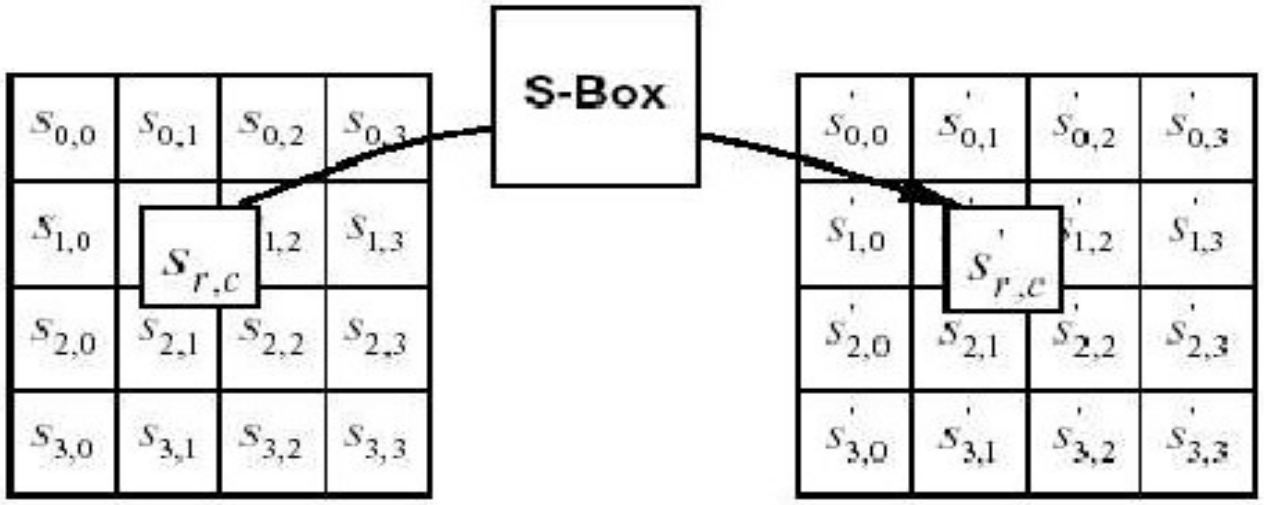
1. Πριν το πρώτο γύρο ένα block εισόδου αντιγράφεται στην State και στη συνέχεια εφαρμόζεται μία πρόσθεση κλειδιού (AddRound Key). Σε αυτή τη λειτουργία, ένα κλειδί Γύρου προστίθεται στην State με την χρήση μίας απλής XOR.



Η λειτουργία του Αλγόριθμου AES (8).

2. Ο Μετασχηματισμός SubBytes

Ο μετασχηματισμός SubBytes() είναι μια μη γραμμική αντικατάσταση οκτάδων που λειτουργεί ανεξάρτητα σε κάθε οκτάδα της κατάστασης χρησιμοποιώντας έναν πίνακα αντικατάστασης (s-box)



Η λειτουργία του Αλγόριθμου AES (9).

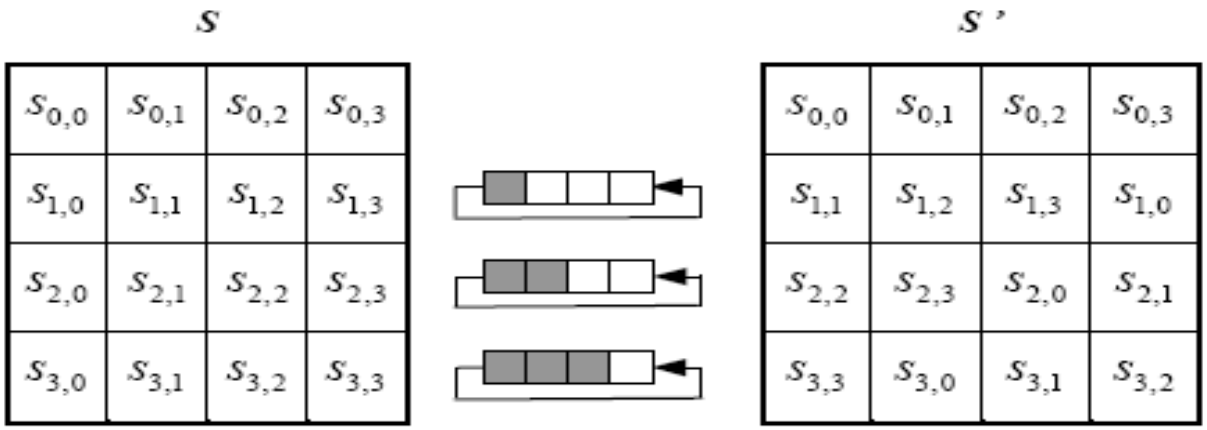
- Ο πίνακας S-Box *τυπικά* δεν υπολογίζεται κατά την διαδικασία της κρυπτογράφησης, αλλά οι τιμές του έχουν προϋπολογιστεί.

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Η λειτουργία του Αλγόριθμου AES (10).

3. Ο Μετασχηματισμός ShiftRows

Στο μετασχηματισμό ShiftRows(), οι ψηφιολέξεις στις τελευταίες τρεις σειρές της State μετατοπίζονται κυκλικά πέρα από τους διαφορετικούς αριθμούς ψηφιολέξεων. Η πρώτη σειρά, r = 0, δεν μετατοπίζεται.



Η λειτουργία του Αλγόριθμου AES (11).

4. Ο Μετασχηματισμός MixColumns

Στο μετασχηματισμό MixColumns πολλαπλασιάζεται κάθε στήλη με ένα πολυώνυμο c(x) modulo $x^4 + 1$.

5. *Ο Μετασχηματισμός AddRoundKey*

Σε αυτή τη λειτουργία, ένα κλειδί Γύρου προστίθεται στην State με την χρήση μίας απλής XOR.

Το ενδιάμεσο κλειδί ή Κλειδί Γύρου προκύπτει από το αρχικό Κλειδί Κρυπτογράφησης (ή μυστικό κλειδί) με τη μέθοδο Key Schedule. Το μήκος του είναι ίσο με το μήκος του Block (Nb).

Η ασφάλεια του Αλγόριθμου AES (1).

- Μέχρι το 2006, οι μοναδικές περιπτώσεις επιτυχών επιθέσεων στον AES είχαν να κάνουν με τις επιθέσεις με «έμμεσο τρόπο» (side-channel attacks).
- Στις επιθέσεις αυτές ο επιτιθέμενος δε προσπαθεί να βρει το μυστικό κλειδί με μαθηματικά ή επιλύοντας τον αλγόριθμο δοκιμάζοντας διάφορα κλειδιά, όπως στην εξαντλητική αναζήτηση.
- Αντίθετα εδώ, οι πληροφορίες ανακτώνται μετά από μελέτη κυρίως της φυσικής υλοποίησης του αλγορίθμου.
- Για παράδειγμα, πληροφορίες σχετικά με το χρόνο κρυπτογράφησης και την υπολογιστική δύναμη που καταναλώθηκε θα μπορούσαν να δώσουν χρήσιμες πληροφορίες που να οδηγήσουν στην εύρεση του κλειδιού και την αποκρυπτογράφηση δε δεδομένων.

Η ασφάλεια του Αλγόριθμου AES (2).

- Επιθέσεις στον AES με έμμεσο τρόπο:
- **Επίθεση με χρονομέτρηση (timing attack):** Παρακολουθεί και χρονομετρεί την είσοδο και έξοδο των δεδομένων σε έναν επεξεργαστή ή στη μνήμη στα οποία τρέχει ο αλγόριθμος. Επίσης, μπορεί να μετράει το χρόνο που χρειάζεται για να γίνει η κρυπτογράφηση σε διαφορετικά κείμενα. Έτσι, μπορεί να υπολογιστεί το μήκος του κλειδιού.
- **Επίθεση με παρακολούθηση της υπολογιστικής δύναμης (power monitoring attack):** Παρακολουθεί και καταγράφει την υπολογιστική δύναμη, κυρίως του επεξεργαστή που χρησιμοποιείται για την κρυπτογράφηση. Πολλές δοκιμές σε διαφορετικούς επεξεργαστές και με διαφορετικά κρυπτογραφημένα δεδομένα μπορούν να μας οδηγήσουν στην εύρεση του κλειδιού.
- **Επίθεση με θερμική απεικόνιση:** Είναι μια πολύ καινούργια μέθοδος του Shamir με την οποία οι θερμικές αλλαγές της επιφάνειας του επεξεργαστή απεικονίζονται σαν εικόνες στην οθόνη και μας δείχνουν έτσι πως λειτουργεί ο επεξεργαστής κατά τη διάρκεια της εφαρμογής του αλγορίθμου.

Η ασφάλεια του Αλγόριθμου AES (3).

- Το 2003, η NSA (National Security Agency) ανακοίνωσε ότι ο AES είναι αρκετά ασφαλής και μπορεί να χρησιμοποιηθεί από την κυβέρνηση των Η.Π.Α. για την προστασία μη-εμπιστευτικών δεδομένων. Συγκεκριμένα εκδόθηκε η εξής ανακοίνωση:
- *«Ο σχεδιασμός και η ισχύς όλων των κλειδιών του AES είναι αρκετά για να προστατεύσουν εμπιστευτικές πληροφορίες μέχρι το επίπεδο του «ΑΠΟΡΡΗΤΟΥ». Εμπιστευτικές πληροφορίες του επιπέδου «ΑΚΡΩΣ ΑΠΟΡΡΗΤΟ» απαιτούν κλειδιά μήκους 192 ή 256 bits. Οι διάφορες υλοποιήσεις του AES μπορούν να προστατεύσουν τα εθνικά συστήματα ασφαλείας, αρκεί να πιστοποιηθούν πρώτα από την NSA».*
- Ο AES, με μήκος κλειδιού 128-bit, έχει ήδη σπάσει, αφού χρειάστηκαν 2^{120} δοκιμές κλειδιών. Το 2005, ο D. J. Bernstein ανακοίνωσε το σπάσιμο ενός εξυπηρέτη που χρησιμοποιούσε κρυπτογράφηση AES. Η επίθεση έγινε με τη μέθοδο της χρονομέτρησης και χρειάστηκαν 200 εκατομμύρια επιλεγμένα κείμενα να χρονομετρηθούν για να βρεθεί το κλειδί. Παρόλα αυτά, μέσα στο διαδίκτυο τα πράγματα είναι αρκετά διαφορετικά και δεν είναι τόσο εύκολη μια τέτοιου είδους επίθεση.
- Την ίδια χρονιά ο Shamir κατάφερε να ανακτήσει το μυστικό κλειδί του AES με την ίδια μέθοδο και μετά από 800 δοκιμές μέσα σε 65 milliseconds. Όμως, οι δοκιμές έγιναν στο ίδιο υπολογιστικό σύστημα που έτρεχε ο αλγόριθμος.

Συμπεράσματα σχετικά με τους αλγόριθμους συμμετρικής κρυπτογράφησης

Λειτουργικότητα	Επαρκής επικοινωνία μεταξύ των συμμετεχόντων σε ένα κλειστό περιβάλλον
Υπολογιστική ικανότητα	Γρήγορη κρυπτογράφηση και αποκρυπτογράφηση με τη χρήση πιο απλών μαθηματικών
Μέγεθος κλειδιού	Συνήθως 128-bit, αλλά για μεγαλύτερη ασφάλεια γίνεται χρήση και 192-bit ή 256-bit
Υλικό	Απλό υλικό που χρησιμοποιούμε και στη χρήση απλών υπολογιστικών συστημάτων και όχι αρκετά ακριβό
Ασφάλεια	Η ασφάλεια εξαρτάται από το είδος της εφαρμογής, από το μήκος κλειδιού που θα χρησιμοποιήσουμε και τα μαθηματικά που χρησιμοποιεί ο αλγόριθμος

Χρήση των αλγόριθμων συμμετρικής κρυπτογράφησης

Είδος Εφαρμογής και Περίπτωση	Ναι / Όχι
Ηλεκτρονικό Εμπόριο	Όχι
Όταν έχουμε μετακίνηση κλειδιών	Όχι
Υπογραφές	Όχι
Ασφάλεια	Ναι / Όχι (Ανάλογα το κλειδί και τον αλγόριθμο)
Ταχύτητα Επεξεργασίας του αλγορίθμου	Ναι
Μήκους κλειδιού μικρό	Ναι
Κρυπτογράφηση σε ένα μόνο τερματικό	Ναι
Κρυπτογράφηση σε smart-cards	Ναι
Κρυπτογράφηση σε δίσκο (κυρίως USB)	Ναι
Οικονομία σε πλικό	Ναι

Ο αλγόριθμος ανταλλαγής κλειδιών Diffie-Hellman.

- Στην ασύμμετρη κρυπτογραφία απαιτείται η ασφαλής ανταλλαγή των κλειδιών μεταξύ των 2 συμμετεχόντων.
- Το πιο γνωστό πρωτόκολλο ανταλλαγής κλειδιών είναι αυτό του Diffie και Hellman (Diffie-Hellman key exchange protocol).
- Το πρωτόκολλο δημοσιεύτηκε το 1976 από τους Diffie W. και Hellman M., λίγο πριν την εμφάνιση του αλγορίθμου RSA που σήμανε και την έναρξη ουσιαστικά της κρυπτογραφίας δημοσίου κλειδιού.
- Παρόλα αυτά ο ίδιος ο Hellman αναφέρει το 2002 ότι ο Merkle R. πολύ νωρίτερα είχε ασχοληθεί με το θέμα και για αυτόν τον λόγο και ο αλγόριθμος θα έπρεπε να ονομαστεί “Diffie-Hellman-Merkle key exchange protocol”.

Περιγραφή του Αλγόριθμου Diffie-Hellman.

- Έστω, η Alice και ο Bob θέλουν να ανταλλάξουν ένα κλειδί και να το ξέρουν μόνο αυτοί.

1. Συμφωνούν και διαλέγουν ένα πεπερασμένο σώμα αριθμών G και τον γεννήτορα g.
2. Η Alice επιλέγει έναν τυχαίο αριθμό a και στέλνει στον Bob τον g^a.
3. Ο Bob επιλέγει έναν τυχαίο αριθμό b και στέλνει στον Bob τον g^b.
4. Η Alice υπολογίζει το κλειδί $(g^b)^a$.
5. Ο Bob υπολογίζει το κλειδί $(g^a)^b$.

Παράδειγμα του Αλγόριθμου Diffie-Hellman.

- Έστω την ώρα που ο Bob στέλνει το κλειδί στην Alice η Eve προσπαθεί να το κλέψει. Έστω έχουμε:

1. s = 2, το μυστικό κλειδί που πρέπει να μεταφερθεί κρυφά
2. a = 6, το ιδιωτικό κλειδί της Alice
3. b = 15, το ιδιωτικό κλειδί του Bob
4. g = 5, ο γεννήτορας (βάση) του σώματος
5. p = 23, ένας πρώτος αριθμός

Alice	
γνωστό	άγνωστο
p = 23	b = 15
g = 5	
a = 6	
$5^6 \bmod 23 = 8$	
$5^b \bmod 23 = 19$	
$19^6 \bmod 23 = 2$	
$8^b \bmod 23 = 2$	
$19^6 \bmod 23 = 8^b \bmod 23$	
s = 2	

Bob	
γνωστό	άγνωστο
p = 23	a = 6
base g = 5	
b = 15	
$5^{15} \bmod 23 = 19$	
$5^a \bmod 23 = 8$	
$8^{15} \bmod 23 = 2$	
$19^a \bmod 23 = 2$	
$8^{15} \bmod 23 = 19^a \bmod 23$	
s = 2	

Eve	
γνωστό	άγνωστο
p = 23	a = 6
g = 5	b = 15
	s = 2
$5^a \bmod 23 = 8$	
$5^b \bmod 23 = 19$	
$19^a \bmod 23 = s$	
$8^b \bmod 23 = s$	
$19^a \bmod 23 = 8^b \bmod 23$	

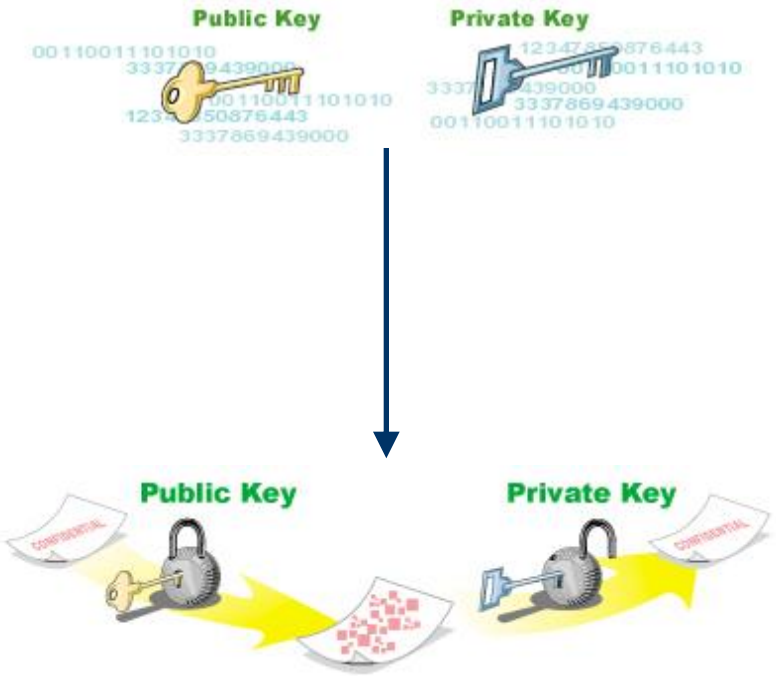
Ασφάλεια του Αλγόριθμου Diffie-Hellman.

- Η ασφάλεια του αλγορίθμου καταρρίπτεται μόνο αν ο υποκλοπέας ανακτήσει το g^{ab}.
- Αυτό όμως είναι αρκετά δύσκολο αφού τα G και g είναι πάρα πολύ μεγάλα και η εύρεση του διακριτού λογαρίθμου είναι δύσκολη διαδικασία.
- Παρόλα αυτά ο αλγόριθμος δεν παρέχει πιστοποίηση από μόνος του.
- Αν κάποιος καταφέρει να αποκτήσει ταυτόχρονη επικοινωνία και με τους δυο συμμετέχοντες (Bob και Alice), κάνοντας να πιστέψουν ότι ο Bob είναι η Alice και αντίστροφα, θα μπορέσει να βρει το κλειδί.
- Για αυτό το λόγο, συνήθως ο αλγόριθμος λειτούργει παράλληλα με ένα σύστημα πιστοποίησης και όχι μόνος του.

Η Ιστορία του Αλγόριθμου RSA (1)

- Το 1977, ένα χρόνο μετά τη δημοσίευση του πρωτοκόλλου του Diffie-Hellman, τρεις ερευνητές από το Massachusetts Institute of Technology (MIT), δημιούργησαν μια πρακτική μέθοδο χρησιμοποιώντας υπάρχουσες προτεινόμενες ιδέες.
- Αυτή η μέθοδος οδήγησε στη δημιουργία του αλγορίθμου RSA, που πήρε το όνομα του από τα αρχικά των τριών δημιουργών του, Rivest R., Shamir A. και Adelman L.
- Ο RSA αποτέλεσε πιθανόν τον πιο πολυχρησιμοποιημένο αλγόριθμο στην κρυπτογραφία δημοσίου κλειδιού.
- Επίσημα, χρησιμοποιήθηκε στις Η.Π.Α. το 1983, όταν και υιοθετήθηκε σαν επίσημος αλγόριθμος κρυπτογραφίας στη συγκεκριμένη χώρα.
- Το 2000 εκδόθηκε επίσημα στις Η.Π.Α η ανάλυση και η περιγραφή του και έτσι έγινε πια γνωστός σε όλους.

Η Περιγραφή του Αλγόριθμου RSA (1)



Η Περιγραφή του Αλγόριθμου RSA (2).

- Ο αλγόριθμος RSA λειτουργεί ως εξής:
  - Εύρεση ***μεγάλου*** ακεραίου, ως γινόμενο δύο ***πρώτων*** αριθμών
  - Κατασκευή ***μυστικού - ιδιωτικού*** κλειδιού και ***δημόσιου*** κλειδιού (θεωρία αριθμών)
  - Όποιος επιθυμεί να στείλει κωδικοποιημένο μήνυμα, το κάνει με το ***δημόσιο*** κλειδί
  - ***Μόνο*** όποιος έχει το αντίστοιχο ***μυστικό*** κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα.
  - ***Ανακάλυψη*** (δύσκολο!) των δύο πρώτων αριθμών ⇒ υποκλοπή μηνυμάτων εύκολη!

Η Περιγραφή του Αλγόριθμου RSA (3).

Παράδειγμα κρυπτογράφησης με το RSA.

- **<u>Βήμα 1ο:</u>** Επιλέγουμε δύο πρώτους αριθμούς p και q.Το γινόμενό τους είναι p*q=N. Τα p και q είναι γνωστά μόνο σε εμάς και άγνωστα για όλους τους άλλους. Αντιθέτως το N είναι γνωστό στο ευρύ κοινό.

Π.χ. Διαλέγω για p=3 και q=11 (πρώτοι)

Το γινόμενό τους είναι ίσο με:

N=p*q=33 (αυτό είναι το **δημόσιο κλειδί**, το οποίο δημοσιεύεται είτε στο Internet, είτε σε έναν κατάλογο δημοσίων κλειδιών)

Τα p και q είναι άγνωστα στο ευρύ κοινό και αποτελούν το **ιδιωτικό κλειδί**.

Η Περιγραφή του Αλγόριθμου RSA (4).

Βήμα 2ο:

Υπολογίζω την συνάρτηση

$$\varphi(n)=(p-1)*(q-1)$$

Στο συγκεκριμένο παράδειγμα

$$\varphi(n)=(3-1)*(11-1)=2*10=20$$

Στη συνέχεια επιλέγω έναν αριθμό που να μη δίνει υπόλοιπο μηδέν (σχετικά πρώτοι), όταν διαιρείται με το φ(n).

Στο παράδειγμά μας το φ(n) είναι ίσο με 20.Έστω ότι διαλέγω τον αριθμό 13,τον οποίο τον ονομάζω e και είναι το **κλειδί της κρυπτογράφησης**.

Η Περιγραφή του Αλγόριθμου RSA (5).

Βήμα 3ο:

Εφαρμόζω τον εκτεταμένο αλγόριθμο του Ευκλείδη με διαιρέτη τον e και διαιρετέο το φ(n).

Εκτεταμένος Αλγόριθμος του Ευκλείδη → Για 2 αριθμούς a, b που είναι σχετικά πρώτοι μεταξύ τους ισχύει:

gcd(a, b)= a*x + b*y

Επαλήθευση:13*(-3)+20*2=-39+40=1

Στη συνέχεια υπολογίζω τον αριθμό d,

ο οποίος είναι ίσος με d=20+(-3)=17

Ο αριθμός d είναι **το κλειδί αποκρυπτογράφησης** και θα χρησιμοποιηθεί αργότερα.

Η Περιγραφή του Αλγόριθμου RSA (6).

Βήμα 4ο:

Αντικαθιστώ κάθε γράμμα του αλφάβητου μ' έναν αριθμό:

A 10	B 11	C 12	D 13	E 14
F 15	G 16	H 17	I 18	J 19
K 20	L 21	M 22	N 23	O 24
P 25	Q 26	R 27	S 28	T 29
U 30	V 31	W 32		
X 33	Y 34	Z 35		

Η Περιγραφή του Αλγόριθμου RSA (7).

Έστω ότι θέλουμε να κρυπτογραφήσουμε τη αγγλική λέξη

JUPITER

Έχοντας αντιστοιχήσει κάθε γράμμα της αλφαβήτου με έναν αριθμό, η λέξη JUPITER αντιστοιχίζεται ως εξής:

J U P I T E R

19 30 25 18 24 14 27

Στη συνέχεια ενώνω τους παραπάνω αριθμούς σ' ένα string.

Η Περιγραφή του Αλγόριθμου RSA (8).

Οπότε θα προκύψει το εξής string:

19302518241427

Το παραπάνω string θα το χωρίσω σε μπλοκ, τα οποία αριθμητικά θα είναι μικρότερα του N (N=33).

Δηλαδή το string θα χωριστεί ως εξής :

19-30-25-18-24-14-27

Στο κάθε μπλοκ εφαρμόζεται η συνάρτηση κρυπτογράφησης η οποία είναι η εξής:

$$\mathrm{E}(b) = b^{e} \bmod n$$

Η Περιγραφή του Αλγόριθμου RSA (9).

Άρα τα μπλοκ

19 30 25 18 24 14 27

που αντιστοιχούν στα γράμματα

J-U-P-I-T-E-R

θα μετατραπούν σύμφωνα με την παραπάνω συνάρτηση σε:

$$19^{13} \bmod 33 = 28$$
$$30^{13} \bmod 33 = 6$$
$$25^{13} \bmod 33 = 16$$
$$18^{13} \bmod 33 = 24$$
$$29^{13} \bmod 33 = 2$$
$$14^{13} \bmod 33 = 5$$
$$27^{13} \bmod 33 = 15$$

Η Περιγραφή του Αλγόριθμου RSA (10).

- Η αποκρυπτογράφηση θα γίνει ως εξής:

Στο κάθε κρυπτογραφημένο μπλοκ εφαρμόζεται η συνάρτηση αποκρυπτογράφησης η οποία είναι η εξής:

α: το κρυπτογραφημένο μπλοκ.

d:κλειδί αποκρυπτογράφησης

$$D(a) = a^{d} \bmod n$$

$$28^{17} \bmod 33 = 19$$
$$6^{17} \bmod 33 = 30$$
$$16^{17} \bmod 33 = 25$$
$$24^{17} \bmod 33 = 18$$
$$2^{17} \bmod 33 = 29$$
$$5^{17} \bmod 33 = 14$$
$$15^{17} \bmod 33 = 27$$

Η Περιγραφή του Αλγόριθμου RSA (11).

- Η πιο κομψή πτυχή του κρυπτογράμματος RSA είναι ότι αν και το N είναι γνωστό, τα p και q είναι εξαιρετικά δύσκολο να βρεθούν, καθώς είναι δύσκολη η παραγοντοποίηση του N σε δύο πρώτους αριθμούς.
- Τα p και q είναι ένα ζευγάρι πρώτων αριθμών, οι οποίοι αποτελούνται από 100-200 ψηφία, ίσως και περισσότερα.

Η Περιγραφή του Αλγόριθμου RSA (12).

- **Μέθοδος Λειτουργίας του RSA**

1. Εύρεση ***μεγάλου*** ακεραίου, ως γινόμενο δύο ***πρώτων*** αριθμών
2. Κατασκευή ***μυστικού - ιδιωτικού*** κλειδιού και ***δημόσιου*** κλειδιού (θεωρία αριθμών!)
3. Όποιος επιθυμεί να στείλει κωδικοποιημένο μήνυμα, το κάνει με το ***δημόσιο*** κλειδί
4. ***Μόνο*** όποιος έχει το αντίστοιχο ***μυστικό*** κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα!
5. ***Ανακάλυψη*** (δύσκολο!) των δύο πρώτων αριθμών ⇒ υποκλοπή μηνυμάτων εύκολη!

- Πολλαπλασιασμός ακεραίων: *εύκολο!*
  - 122 X 831 = ? (? = 1013812)
- Εύρεση πρώτων αριθμών που πολλαπλασιαζόμενοι δίνουν έναν δοσμένο ακέραιο: *δύσκολο!* (το περίφημο πρόβλημα της παραγοντοποίησης)
  - 415711= ? X ? (? = 199, ? = 2089)

Η Περιγραφή του Αλγόριθμου RSA (13).

Ποιο συγκεκριμένα, πως γίνεται η κρυπτογράφηση:

- Διαλέγω τυχαία 2 πρώτος αριθμούς: p=11 και q=19 $n = 11 \times 19 = 319$
- Για δημόσιο κλειδί διαλέγουμε k_e=101 και υπολογίζουμε το ιδιωτικό κλειδί k_d :

$$k_d k_e \equiv 1 (\mathrm{mod} \phi(n)) \Rightarrow k_d \cdot 101 \equiv 1 (\mathrm{mod} 180)$$

- Η παραπάνω modular γραμμική εξίσωση έχει μόνο μία λύση αφού gcd(α,n)=gcd(101,180)=1

Η Περιγραφή του Αλγόριθμου RSA (14).

- Εφαρμόζοντας τον εκτεταμένο αλγόριθμο του Ευκλείδη2(α,n) για α=101, n=180 και έχοντας b=1 έχουμε:

n=180=α+79	79=n-α
a=101=79+22	22=α-(n-α)=2α-n
79=3*22+13	13=n-α-3(2α-n)=-7α+4n
22=13+9	9=2α-n+7a-4n=9α-5n
13=9+4	4=-7α+4n-9α+5n=-16α+9n
9=2*4+1	1=9α-5n-2(-16α+9n)=9α-5n+32α-18n=
4=4*1+0	=41α-23n

Η Περιγραφή του Αλγόριθμου RSA (15).

- Ευκλείδης2(101,180) → (d,x',y')=(1,41,-23)

$$d = 101 \cdot 41 + 180 \cdot (-23) = 1$$

Ke Kd

- Άρα k_d=41

Η Περιγραφή του Αλγόριθμου RSA (16).

- Αφού έχουμε τα 2 κλειδιά έστω ότι θέλουμε να κρυπτογραφήσουμε τη λέξη [ρέμα]
- Αντιστοιχούμε το Α→10, Β→11, Γ→12,.....Ω→33 έτσι ώστε όλα τα σύμβολα απλού κειμένου να κωδικοποιούνται με σταθερό πλήθος ψηφίων (2)
- Έτσι το [ρέμα] → [26 14 21 10]
- Ομαδοποιούμε τα ψηφία ώστε οι αριθμοί που δημιουργούνται να είναι μικρότεροι του δημόσιου modulus (319) και έχουμε:
- [ρέμα] → [261, 42, 110]
- Μετά την κρυπτογραφική πράξη (εκτελείται 3 φορές) θα έχουμε:
  - $261^{101}=261 \bmod 319$
  - $42^{101}=196 \bmod 319$
  - $110^{101}=132 \bmod 319$

Η Ασφάλεια του Αλγόριθμου RSA (1).

- Το σχήμα του RSA βασίζεται στο ότι αν και το N είναι γνωστό, τα p και q είναι εξαιρετικά δύσκολο να βρεθούν, καθώς είναι δύσκολη η παραγοντοποίηση του N σε δύο πρώτους αριθμούς.
- Το γεγονός αυτό καθιστά το κρυπτόγραμμα RSA δύσκολο και αρκετά χρονοβόρο στο να αποκρυπτογραφηθεί.
- Το μεγάλο πλεονέκτημα της κρυπτογραφίας δημόσιου κλειδιού που εφαρμόζει ο RSA είναι ότι καταργεί όλα τα προβλήματα που συνδεόταν με τα παραδοσιακά κρυπτογράμματα και τις μεθόδους ανταλλαγής κλειδιών.

Η Ασφάλεια του Αλγόριθμου RSA (2).

- Ο **RSA** είναι πολύ πιο αργός από τον DES και άλλα συμμετρικά κρυπτοσυστήματα.
- Ο Kocher περιέγραψε ένα νέο είδος επίθεσης στον **RSA** το 1995: Αν ο επιτιθέμενος γνωρίζει το hardware με απόλυτη ακρίβεια του ατόμου που κάνει την κρυπτογράφηση μπορεί να μετρήσει τον χρόνο που κάνει το μηχάνημα να κρυπτογραφήσει διάφορα κρυπτοκείμενα. Έτσι, υπολογίζει το ιδιωτικό κλειδί.
- Λύση: Για όλα τα κρυπτοκείμενα → ίσος αριθμός χρόνου κρυπτογράφησης.
- Όμως, έτσι μειώνεται η απόδοση του αλγορίθμου.
- Χρήση της τεχνικής Blinding για τον αποπροσανατολισμό και τη δημιουργία ενός random αλγόριθμου του χρόνου κρυπτογράφησης των μηνυμάτων.
- Η ασφάλεια που προσφέρει ένα κλειδί μεγέθους 1024-bit είναι αρκετά καλή. Η RSA Laboratories προτείνει τη χρήση κλειδιών 2048-bit. Για συνηθισμένη χρήση, συνήθως προτείνεται κλειδί μήκους 768-bit, το οποίος όμως σπάει εύκολα με διάφορες τεχνικές. Η RSA Laboratories το 1995 ανέφερε ότι ένα κλειδί μήκους 512-bit μπορεί να σπάσει σε 8 μήνες με κόστος 1 εκατομμύριο δολάρια. Και πράγματι, το 1999, σε διαγωνισμό που προκήρυξε η RSA ένα κλειδί 512-bit έσπασε σε 7 μήνες. Επίσης, πρέπει να σημειωθεί ότι διπλασιάζοντας τον αριθμό modulo τετραπλασιάζεται ο χρόνος κρυπτογράφησης, το οποίο είναι εντελώς ασύμφορο.

7. Η Συνάρτηση Κατακερματισμού (Hashing) (1)

- Μια πολύ πρακτική μέθοδος κρυπτογράφησης είναι η συνάρτηση κατακερματισμού ή κατατεμαχισμού (**one way hash**).
- Για κάθε μήνυμα δημιουργείται μια σύνοψή του, που είναι μια σειρά από bits με συγκεκριμένο πλήθος, για παράδειγμα 128 bits. Η σύνοψη του μηνύματος, που είναι γνωστή με τον όρο **fingerprint ή message digest**, αποτελεί ψηφιακή αναπαράσταση του μηνύματος και είναι μοναδική για το μήνυμα που αντιπροσωπεύει. Αν αλλάξουμε έστω και μια τελεία στο μήνυμα, θα αλλάξει και η σύνοψή του, ενώ είναι πρακτικά αδύνατο δύο διαφορετικά μηνύματα να δώσουν την ίδια σύνοψη. Είναι επίσης πρακτικά αδύνατο να ανακτήσουμε το αρχικό μήνυμα αν γνωρίζουμε τη σύνοψή του.

7. Η Συνάρτηση Κατακερματισμού (Hashing) (2)

- **Πως λειτουργεί:**
  1. Ο αποστολέας δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να αποστείλει, χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού και έτσι δημιουργείται μια σειρά από bits με συγκεκριμένο μήκος.
  2. Ο αποστολέας κρυπτογραφεί μετά με το ιδιωτικό του κλειδί τη σύνοψη που έχει δημιουργηθεί.
  3. Η κρυπτογραφημένη σύνοψη προσαρτάται στο αρχικό κείμενο και μεταδίδεται μαζί του, χωρίς να είναι απαραίτητη και η κρυπτογράφηση του αρχικού κειμένου.
  4. Στη λήψη, ο παραλήπτης αποσπά από το μήνυμα την κρυπτογραφημένη σύνοψη και εφαρμόζει στο κανονικό κείμενο τον ίδιο αλγόριθμο κατακερματισμού, ώστε να δημιουργήσει μια δική του σύνοψη.
  5. Μετά αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα την κρυπτογραφημένη σύνοψη του μηνύματος και συγκρίνει τις δύο συνόψεις.
  6. Αν οι δύο αυτές συνόψεις βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο, ενώ αν βρεθούν διαφορετικές, θα σημαίνει ότι το μήνυμα αλλοιώθηκε κατά τη μετάδοσή του.

Κρυπτοσύστημα ELGAMAL (1)

- Ο Taher ElGamal είναι ο εφευρέτης του ομώνυμου κρυπτοσυστήματος. Θεωρείται ως μια από τις πιο διακεκριμένες μορφές στην κρυπτογραφία και στη βιομηχανία της ασφάλειας πληροφοριών.
- Διετέλεσε ως βασικό επιστημονικό στέλεχος της Netscape Communications, όπου αποδείχτηκε πρωτοπόρος στις τεχνολογίες ασφάλειας του Διαδικτύου, όπως το SSL, που αποτελεί το πρότυπο για την ασφάλεια στο Internet. Ανέπτυξε επίσης έναν αριθμό από τρόπους πληρωμής μέσω Internet.
- Διετέλεσε επίσης διευθυντής στην εταιρεία RSA Data Security, όπου παρήγαγε εργαλεία κρυπτογράφησης με τον RSA.
- Η καριέρα του στην κρυπτογραφία ξεκίνησε με ένα διδακτορικό στο Stanford υπό την επίβλεψη του Martin Hellman και του Whitfield Diffie, οι οποίοι και έθεσαν τις βάσεις της κρυπτογραφίας δημόσιου κλειδιού.
- Το 1985 εφηύρε το ομώνυμο κρυπτοσύστημα, ενώ το 1994 η κυβέρνηση των ΗΠΑ υιοθέτησε το πρότυπο ψηφιακής υπογραφής (Digital Signature Standard, DSS), το οποίο βασίζεται στο κρυπτοσύστημα του ElGamal.

Κρυπτοσύστημα ELGAMAL (2)

- Το κρυπτοσύστημα του ElGamal βασίζεται στο Πρόβλημα του Διακριτού Λογαρίθμου (DLP).
- Το πρόβλημα DLP διατυπώνεται ως εξής: Δοθέντος ενός στοιχείου g, που ανήκει σε ένα ορισμένο σύνολο G και ενός στοιχείου h,όπου το h ανήκει στο σύνολο G αναζητούμε έναν ακέραιο x τέτοιο ώστε : g^x = h
- Δοθέντων των ακεραίων g και n με g < n, ο διακριτός λογάριθμος ενός ακεραίου y με βάση g είναι ένας ακέραιος x, έτσι ώστε g^x ισοδυναμεί με h mod n.
- Παράδειγμα:Ψάχνουμε έναν ακέραιο x,τέτοιον ώστε 3^x να ισοδυναμεί με 13(mod17).
- Η λύση στο πρόβλημα αυτό είναι x=4, αφού 3^4=81 και 81 ισοδυναμεί με 13(mod17).

Κρυπτοσύστημα ELGAMAL (3)

- Έστω p ένας μεγάλος πρώτος αριθμός και g ένας generator του Z^*_p, όπου g ανήκει στο [0, p -1].
- Έστω A και B δύο άτομα που θέλουν να επικοινωνήσουν στέλνοντας ο ένας στον άλλον ένα κρυπτογραφημένο μήνυμα.
- Οι A και B έχουν δημιουργήσει ήδη το λεγόμενο disposable key (διαθέσιμο κλειδί) βάσει του key agreement protocol.

Κρυπτοσύστημα ELGAMAL (4)

- Όταν ο Α θελήσει να στείλει μήνυμα στον Β υπολογίζει το α **= g^k mod p** και μετά προχωρά στη διαδικασία της κρυπτογράφησης με αυτό το κλειδί.
- Σχηματίζει το **My^k mod p**, ισοδυναμεί με M(**g^b mod p)^k mod p**,όπου **g^b mod p** είναι το δημόσιο κλειδί του Β.
- Το κρυπτογραφημένο μήνυμα που τελικά λαμβάνει ο Β είναι το (α,b) ,όπου

  α = g^k mod p

  b = My^k mod p

Κρυπτοσύστημα ELGAMAL (5)

- **ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ**
  - Ο Β λαμβάνει το κρυπτογραφημένο μήνυμα και για να προχωρήσει στην αποκρυπτογράφηση χρησιμοποιεί το δημόσιο κλειδί του και πραγματοποιεί την πράξη:

b/ α^b mod p ⇔ b * (α^b mod p)^(-1)

⇔ M(g^b mod p)^k mod p * ((g^k mod p) ^b mod p)^(-1) ⇔ M,

Όπου M = plaintext (το αρχικό μήνυμα)

Κρυπτοσύστημα ELGAMAL (6)

- Ο ElGamal αλγόριθμος δημιουργεί κρυπτογραφημένο κείμενο σχεδόν 2 φορές το αρχικό κείμενο. Επομένως, απαιτεί μεγάλες αποθηκεύτηκες ικανότητες και επίσης μεγαλύτερο χρόνο για την αποκρυπτογράφηση του κειμένου.
- Είναι πιο αργός από τον RSA και φυσικά από τους DES και AES.

Κρυπτοσύστημα ELGAMAL (7)

- Η ασφάλεια του αλγορίθμου βασίζεται στο σώμα G που θα επιλέξουμε. Όσο μεγαλύτερο είναι τόσο μεγαλύτερη είναι και η ασφάλεια του κρυπτοσυστήματος.
- Η επίλυση του βλήματος DLP είναι πολύ πιο δύσκολη από την παραγοντοποίηση ακεραίων και έτσι δίνει μεγαλύτερη ασφάλεια από τον RSA.

Κρυπτογραφία με ελλειπτικές καμπύλες. (1)

- Το 1985, μια παραλλαγή του DLP (Discrete Logarithm Problem) προτάθηκε από τους Miller και Koblitz που όριζε το πρόβλημα στο σύνολο των σημείων μιας ελλειπτικής καμπύλης, δηλαδή σε ένα σύνολο που αποτελείται από σημεία (x, y) στο δισδιάστατο χώρο. Το πρόβλημα ονομάσθηκε **ECDLP (Elliptic Curve Discrete Logarithm Problem),** δηλαδή **πρόβλημα διακριτού λογαρίθμου σε ελλειπτικές καμπύλες**.
- Η ισχύς ανά bit κλειδιού είναι πολύ μεγαλύτερη σε συστήματα ελλειπτικών καμπυλών παρά σε συμβατικά συστήματα διακριτού λογαρίθμου. Έτσι μικρότερες παράμετροι μπορούν να χρησιμοποιηθούν σε κρυπτογραφικά συστήματα ελλειπτικών καμπυλών παρέχοντας την ίδια ασφάλεια με τα συστήματα διακριτού λογάριθμου.
- Για παράδειγμα ένα κλειδί 160 bits σε συστήματα ελλειπτικών καμπυλών προσφέρει την ίδια ασφάλεια, με ένα κλειδί 1024 bits στο RSA.
- Αποτέλεσμα: Μεγαλύτερη ταχύτητα, μικρότερη κατανάλωση ισχύος, μικρότερος απαιτούμενος χώρος αποθήκευσης και μικρότερη υπολογιστική ισχύς.
- Τα κυριότερα πρωτόκολλα στο χώρο της κρυπτογραφίας έχουν και τα ανάλογα τους στις ελλειπτικές καμπύλες.

Κρυπτογραφία με ελλειπτικές καμπύλες. (2)

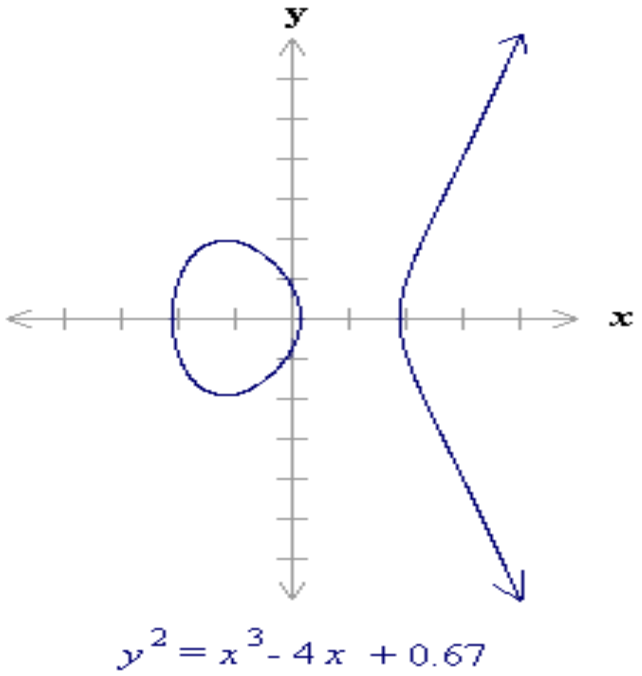
- Τα συστήματα ελλειπτικών καμπυλών εφαρμοσμένα στη κρυπτογραφία προτάθηκαν για πρώτη φορά το 1985 παράλληλα από τον Neal Koblitz (πανεπιστήμιο της Ουάσιγκτον) και από τον Victor Miller, που εργαζόταν για την IBM Yorktown Heights.
- Πολλά κρυπτοσυστήματα απαιτούν τη χρήση αλγεβρικών ομάδων. Οι ελλειπτικές καμπύλες μπορούν να χρησιμοποιηθούν για το σχηματισμό ομάδων ελλειπτικών καμπυλών.
- Οι ελλειπτικές καμπύλες αρχικά εξετάζονται πάνω στους πραγματικούς αριθμούς, ώστε να διευκρινιστούν οι γεωμετρικές τους ιδιότητες. Κατόπιν, οι ομάδες ελλειπτικών καμπυλών εξετάζονται στα υποκείμενα σώματα F_p (όπου το p είναι ένας πρώτος αριθμός) και F_2m (μια δυαδική αναπαράσταση με 2^m στοιχεία).

Κρυπτογραφία με ελλειπτικές καμπύλες. (3)

- **Σώμα** ονομάζεται ένα σύνολο από στοιχεία με δύο ορισμένες αριθμητικές πράξεις μέσα σε αυτό: πιο συχνά είναι, η πρόσθεση και ο πολλαπλασιασμός.
- Τα στοιχεία του σώματος είναι μια προσθετική αβελιανή ομάδα, και τα μη μηδενικά στοιχεία του σώματος αποτελούν μια πολλαπλασιαστική αβελιανή ομάδα.
- Όλα τα στοιχεία του σώματος έχουν αντίθετο, και όλα τα μη μηδενικά στοιχεία της ομάδας έχουν πολλαπλασιαστικό αντίστροφο.
- Ένα σώμα ονομάζεται **πεπερασμένο** όταν έχει ένα πεπερασμένο αριθμό στοιχείων. Τα πιο γνωστά πεπερασμένα σώματα δεδομένης τάξης, που χρησιμοποιούνται στην κρυπτογραφία είναι τα σώματα F_p (όπου p ένας πρώτος αριθμός) και F_2m.

Κρυπτογραφία με ελλειπτικές καμπύλες. (4)

- Μια ελλειπτική καμπύλη με πραγματικούς αριθμούς ορίζεται από το σύνολο των σημείων (x, y) που ικανοποιούν την εξίσωση της μορφής: $y^2 = x^3 + ax + b$, όπου x, y, a και b είναι πραγματικοί αριθμοί.
- Για κάποιον συνδυασμό των a και b, η εξίσωση της ελλειπτικής καμπύλης δεν έχει πολλαπλές (ίδιες) ρίζες (για y=0). Τότε η $x^3 + ax + b$ περιέχει μη συνεχόμενους παράγοντες, ή ισοδύναμα ισχύει $4a^3 + 27b^2 \neq 0$, τότε η $y^2 = x^3 + ax + b$ μπορεί να χρησιμοποιηθεί για το σχηματισμό μιας ομάδας.
- Μια ομάδα ελλειπτικής καμπύλης με πραγματικούς αριθμούς αποτελείται από σημεία της αντίστοιχης ελλειπτικής καμπύλης, μαζί με το ειδικό σημείο Ο που ονομάζεται σημείο στο άπειρο.

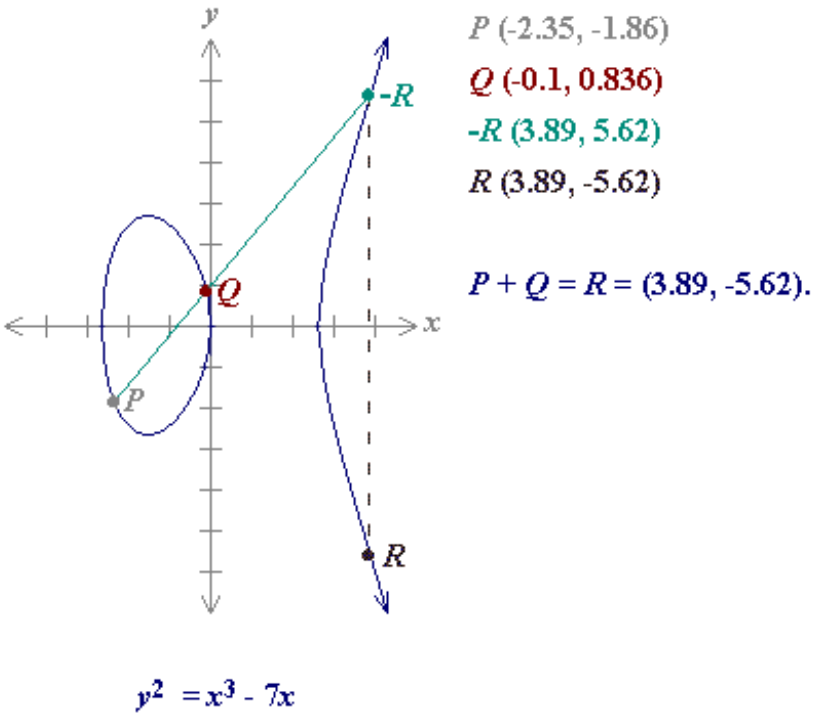


Παράδειγμα ελλειπτικής καμπύλης.

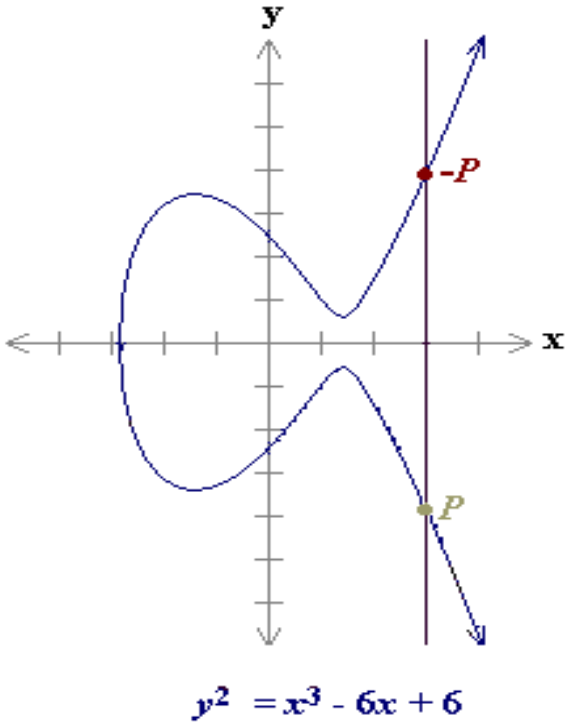
Κρυπτογραφία με ελλειπτικές καμπύλες. (5)

- Αν μία ευθεία τέμνει την ελλειπτική καμπύλη σε 2 σημεία, σίγουρα θα την τέμνει και σε ένα 3ο ή θα πηγαίνει προς το άπειρο.
- Για 3 σημεία (P, Q, (-R)): P + Q + (-R) = O
- Έτσι ορίζεται η πρόσθεση: P + Q = R είναι η προσθετική ιδιότητα που ορίζεται γεωμετρικά στην ελλειπτική καμπύλη.
- Το αρνητικό ενός σημείου $P = (x_P, y_P)$ είναι το συμμετρικό του ως προς τον άξονα των x: το σημείο –P είναι το $(x_P, -y_P)$.
- Για να προστεθούν τα σημεία P και Q, μια γραμμή σχεδιάζεται μεταξύ των δυο σημείων.
- Η γραμμή αυτή τέμνει την ελλειπτική καμπύλη σε ακόμα ένα σημείο, το –R. Το –R έχει το συμμετρικό του στον άξονα των x στο σημείο R.
- Οι ομάδες ελλειπτικών καμπυλών είναι προσθετικές ομάδες.
- Το άθροισμα δύο σημείων είναι σημείο της ελλειπτικής καμπύλης.
- Η πρόσθεση είναι προσεταιριστική πράξη.
- Το σημείο στο άπειρο είναι το ουδέτερο στοιχείο.
- Ορίζεται ο αντίστροφος ενός σημείου (το άλλο σημείο της καμπύλης που έχει την ίδια x - συντεταγμένη).
- Η πρόσθεση είναι αντιμεταθετική πράξη.

Κρυπτογραφία με ελλειπτικές καμπύλες. (6)

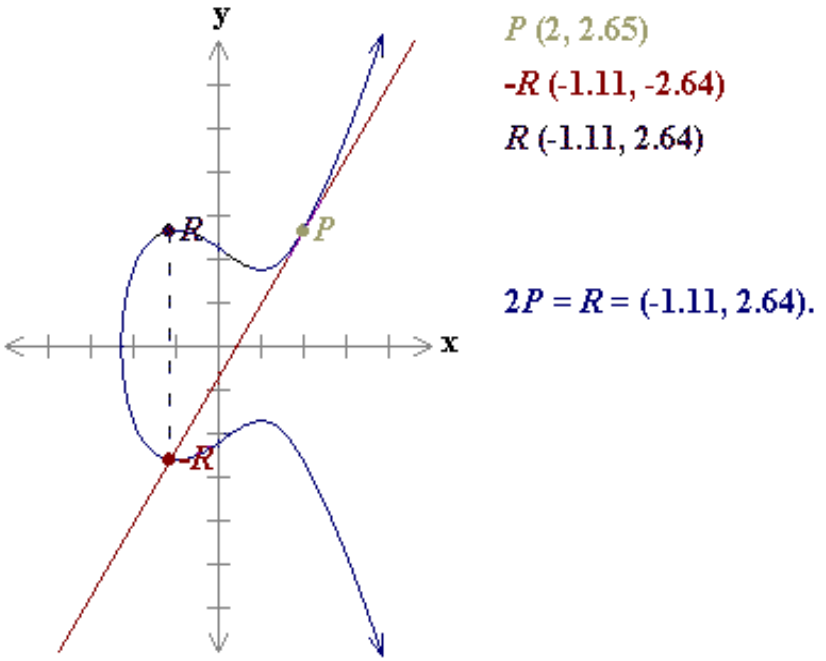


Προσθέτοντας ξεχωριστά σημεία P και Q.



Προσθέτοντας τα σημεία P και -P.

Κρυπτογραφία με ελλειπτικές καμπύλες. (7)



P (2, 2.65)

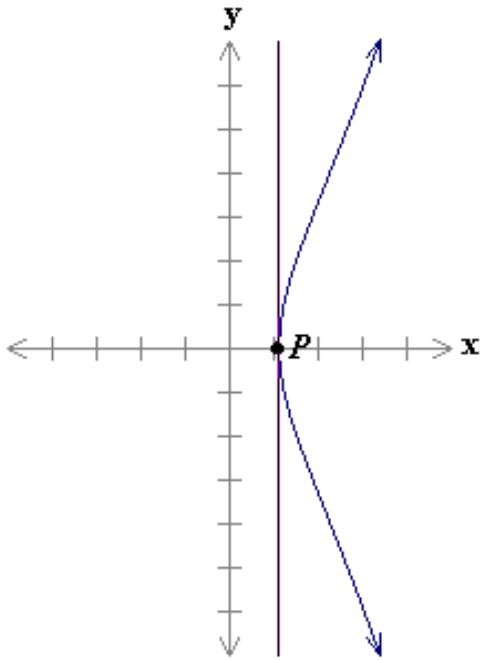
$-R$ (-1.11, -2.64)

R (-1.11, 2.64)

$2P = R = (-1.11, 2.64)$.

$y^2 = x^3 - 3x + 5$

Διπλασιάζοντας το σημείο P.



P (1.1,0)

Since $y_P = 0$, $2P = O$, the point at infinity.

$y^2 = x^3 + 5x - 7$

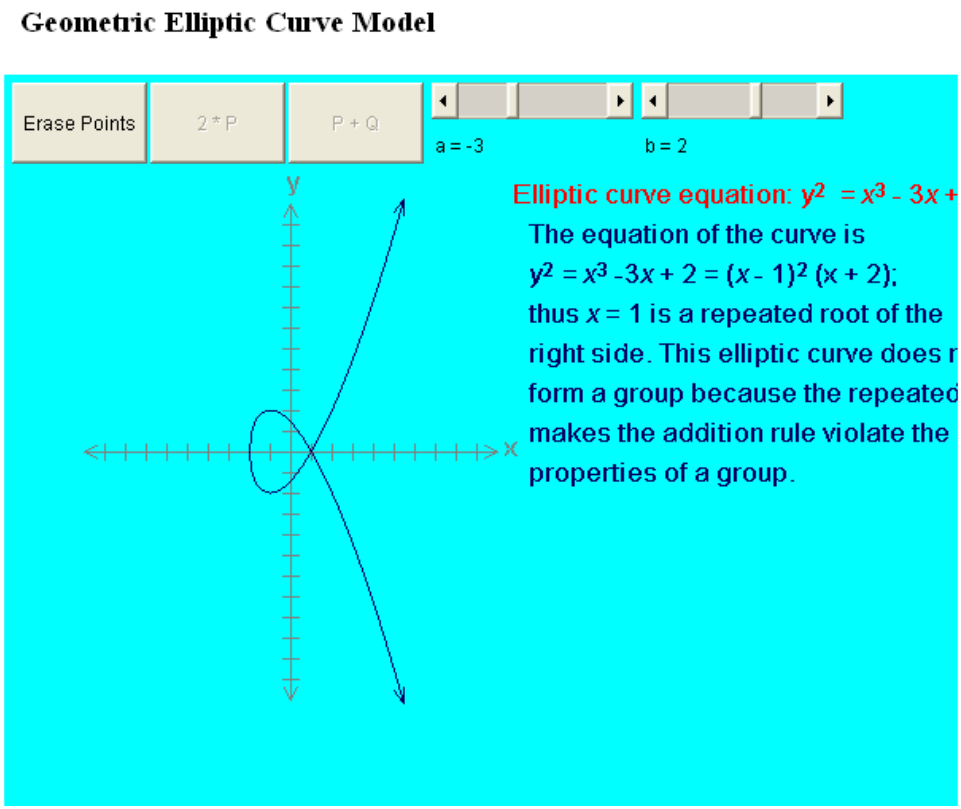
Διπλασιάζοντας το σημείο P, αν $y_P = 0$.

Κρυπτογραφία με ελλειπτικές καμπύλες. (8)

- Όταν τα $P = (x_P, y_P)$ και $Q = (x_Q, y_Q)$ δεν είναι αρνητικά μεταξύ τους, $P + Q = R$ όπου
  $s = (y_P - y_Q) / (x_P - x_Q)$, $x_R = s^2 - x_P - x_Q$ και
  $y_R = -y_P + s(x_P - x_R)$.
- Όταν το y_P δεν είναι 0, $2P = R$ όπου
  $s = (3x_P^2 + a) / (2y_P)$
  $x_R = s^2 - 2x_P$ και $y_R = -y_P + s(x_P - x_R)$
- Το a είναι μία από τις παραμέτρους της ελλειπτικής καμπύλης και το s είναι η κλίση της ευθείας που ενώνει τα σημεία P και Q.

Κρυπτογραφία με ελλειπτικές καμπύλες. (9)

- Αν δοκιμάσουμε για a = -3 και b = 2, θα δούμε ότι επειδή για x = 1 υπάρχει διπλή ρίζα στην ελλειπτική καμπύλη, αυτή δεν αποτελεί ομάδα διότι παραβιάζονται οι ιδιότητες της ομάδας εξαιτίας αυτού του γεγονότος.

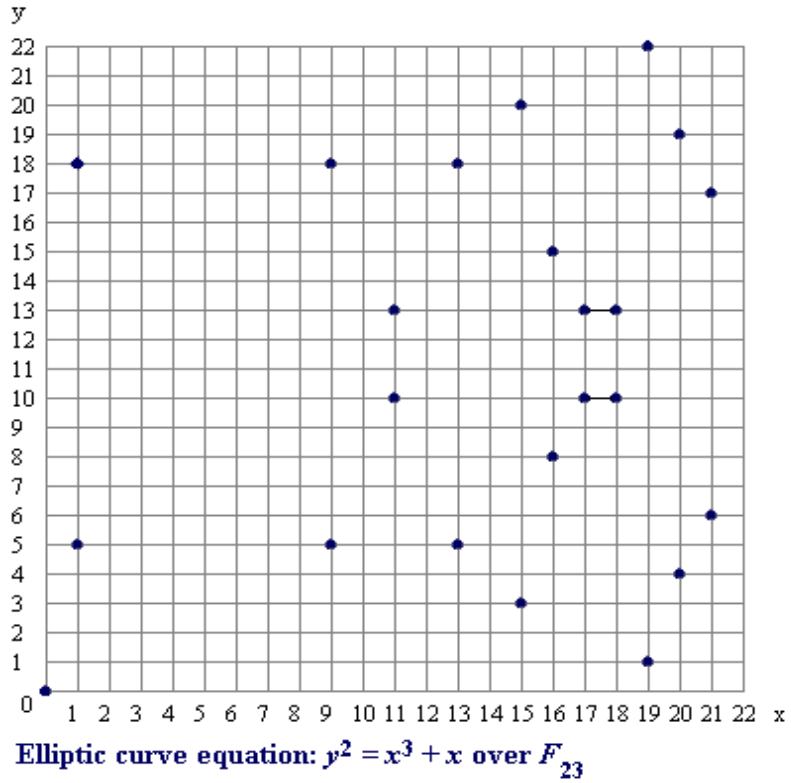


Κρυπτογραφία με ελλειπτικές καμπύλες. (10)

- Οι υπολογισμοί με πραγματικούς αριθμούς είναι αργοί και ανακριβείς εξαιτίας του λάθους λόγω στρογγυλοποίησης.
- Οι κρυπτογραφικές εφαρμογές απαιτούν γρήγορη και ακριβής αριθμητική.
- Οι ομάδα σωμάτων F_p ελλειπτικών καμπυλών χρησιμοποιείται συχνότερα.
- Το σώμα F_p χρησιμοποιεί αριθμούς από 0 έως p–1, και οι υπολογισμοί έχουν αποτέλεσμα το υπόλοιπο της διαίρεσης με το p.

Κρυπτογραφία με ελλειπτικές καμπύλες. (11)

- Η εξίσωση της ελλειπτικής καμπύλης είναι $y^2 = x^3 + x$ στο F_{23}, με a = 1 και b = 0.
- Τα 23 σημεία που ικανοποιούν την εξίσωση φαίνονται στο σχήμα.
- Σημειώστε ότι υπάρχουν δύο σημεία για κάθε τιμή x.
- Υπάρχει συμμετρία στο y = 11,5.

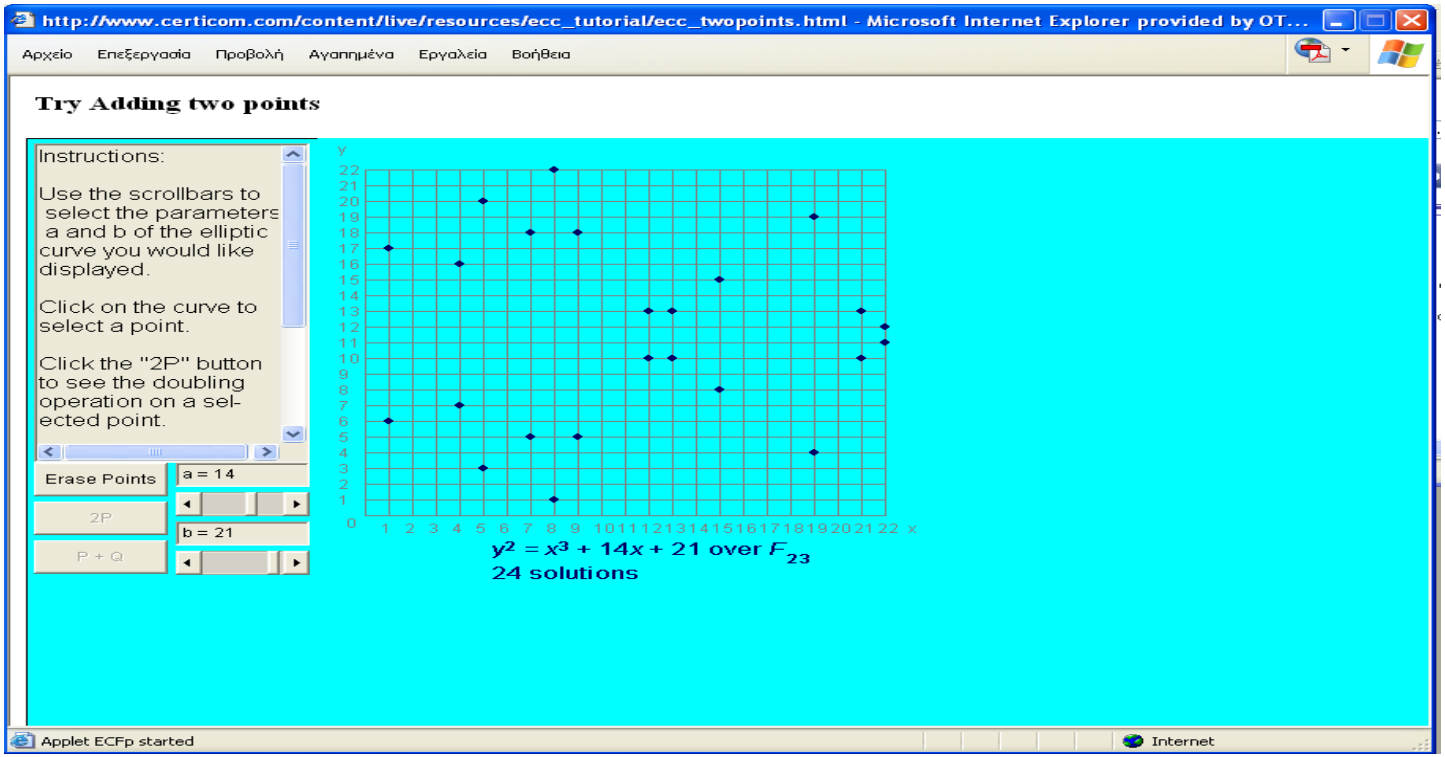


Elliptic curve equation: $y^2 = x^3 + x$ over F_{23}

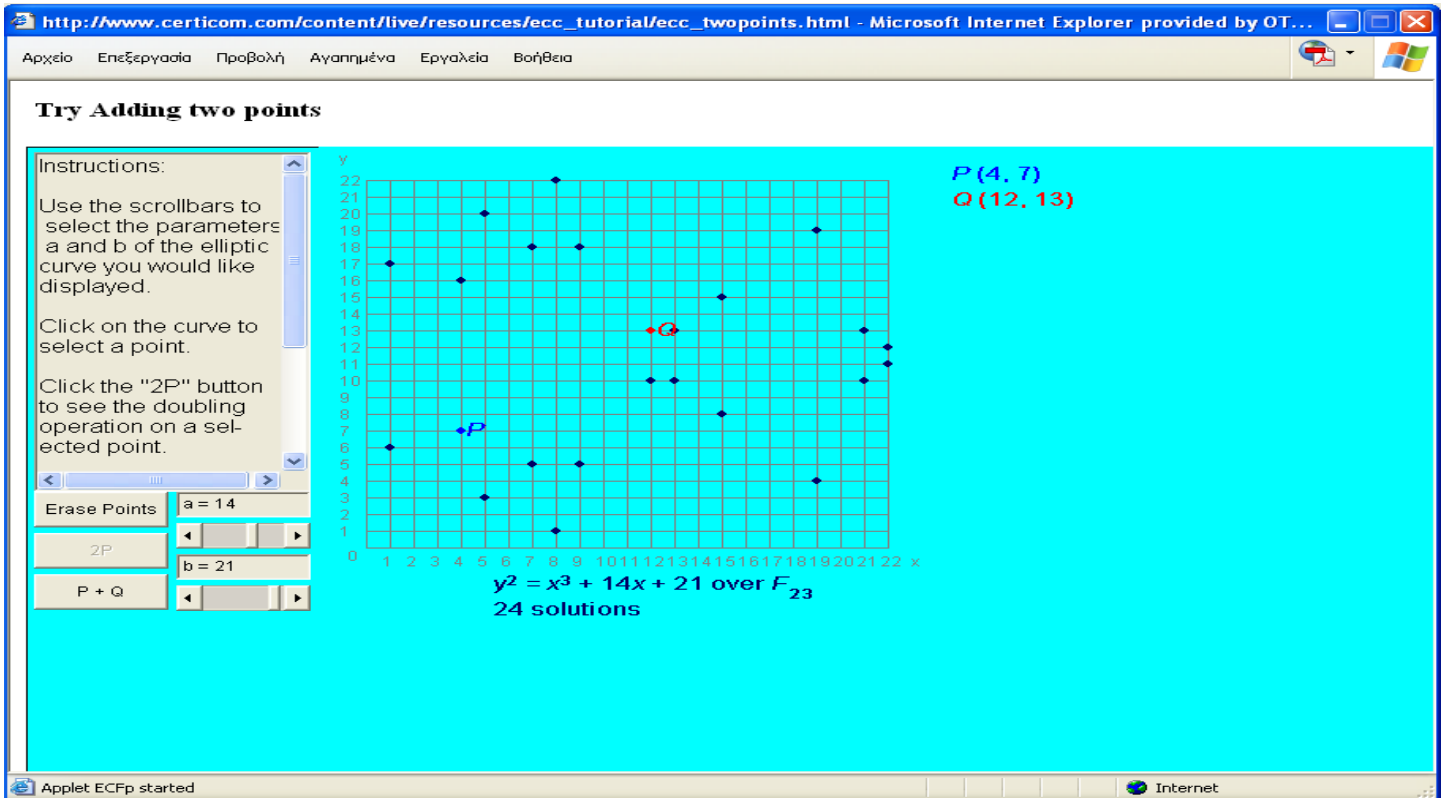
Κρυπτογραφία με ελλειπτικές καμπύλες. (12)

- Υπάρχουν αρκετές σημαντικές διαφορές ανάμεσα στις ομάδες ελλειπτικών καμπυλών F_p και σ' αυτές των πραγματικών αριθμών.
- Οι ομάδες ελλειπτικής καμπύλης στο F_p έχουν πεπερασμένο πλήθος σημείων, τα οποία αποτελούν απαραίτητη προϋπόθεση για κρυπτογραφική χρήση.
- Δεν είναι ξεκάθαρο πώς πρέπει να εφαρμοστούν οι γεωμετρικές σχέσεις.
- Όμως, οι κανόνες άλγεβρας για την αριθμητική μπορούν να υιοθετηθούν για τις ελλειπτικές καμπύλες στο F_p.
- Αντίθετα με τις ελλειπτικές καμπύλες με πραγματικούς αριθμούς, οι υπολογισμοί στο F_p δεν εμπλέκουν το λάθος της στρογγυλοποίησης, μια σημαντική ιδιότητα που απαιτείται από ένα κρυπτοσύστημα.

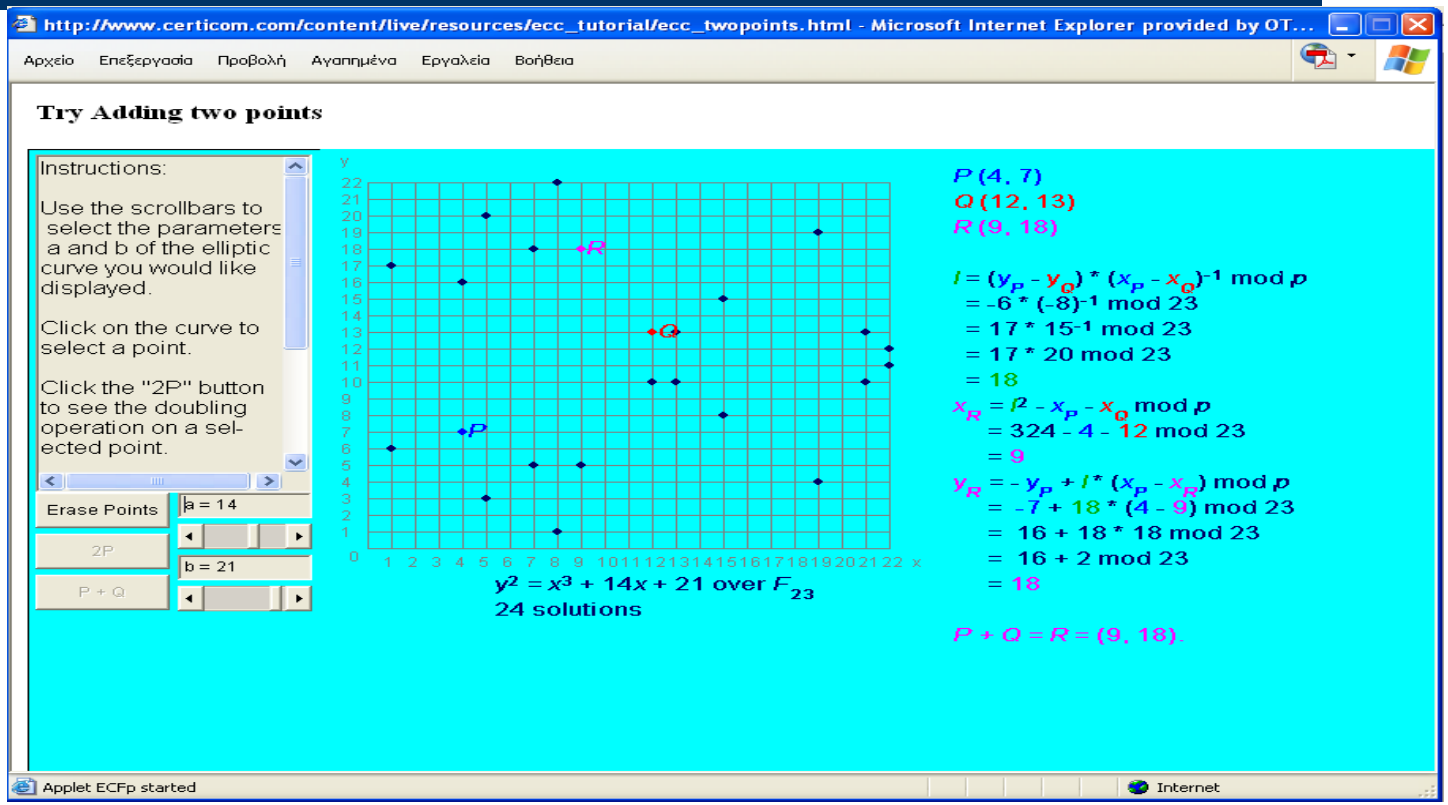
Κρυπτογραφία με ελλειπτικές καμπύλες. (13)



Κρυπτογραφία με ελλειπτικές καμπύλες. (14)



Κρυπτογραφία με ελλειπτικές καμπύλες. (15)

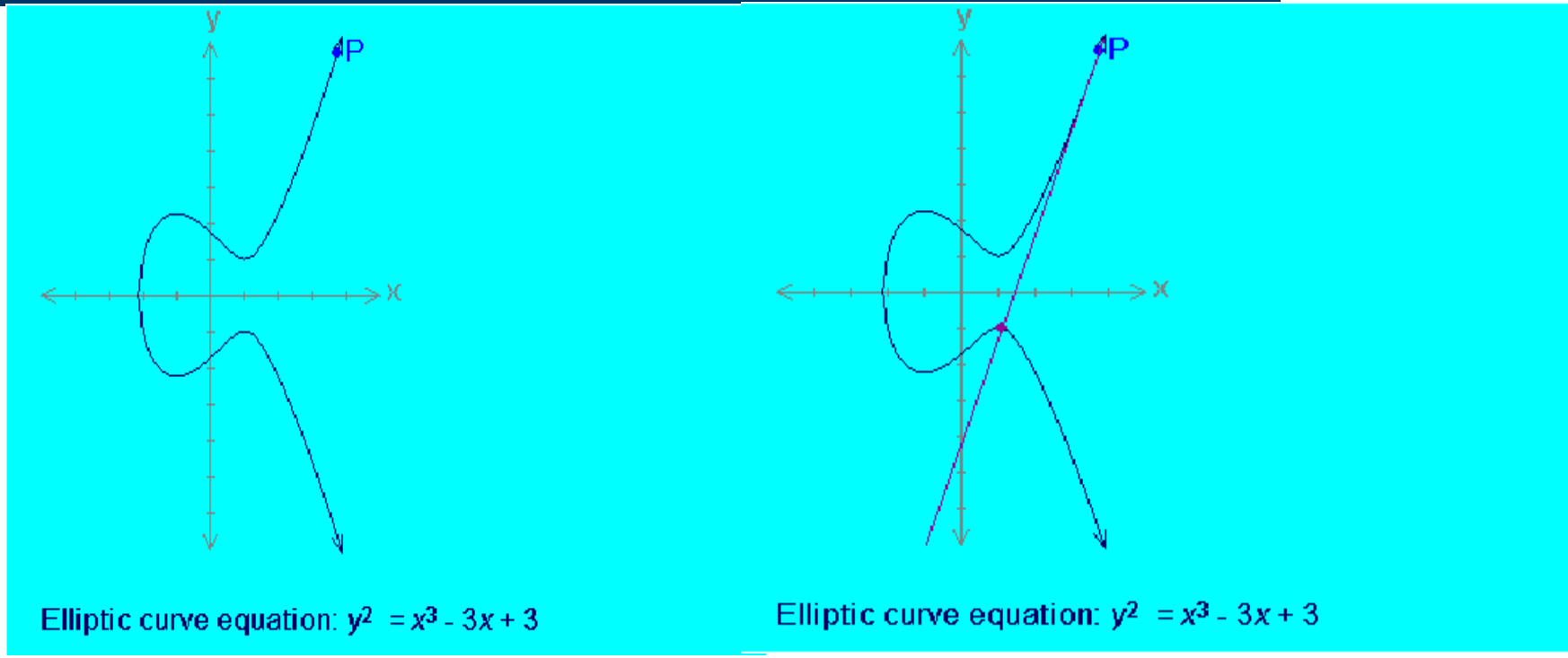


Κρυπτογραφία με ελλειπτικές καμπύλες. (16)

- **Το πρόβλημα του διακριτού λογαρίθμου (DLP, Discrete Logarithm Problem) στις ελλειπτικές καμπύλες**
  - Είναι η βάση για την ασφάλεια πολλών κρυπτοσυστημάτων συμπεριλαμβανομένου του Κρυπτοσυστήματος των Ελλειπτικών Καμπυλών.
  - Η ECC (Elliptic Curve Cryptography) βασίζεται στη δυσκολία του Προβλήματος του Διακριτού Λογαρίθμου στις Ελλειπτικές Καμπύλες ECDLP (Elliptic Curve Discrete Logarithm Problem).
  - Επιλέγοντας ένα σημείο P από μια ομάδα ελλειπτικής καμπύλης, μπορούμε να βρούμε το διπλάσιο του παίρνοντας το σημείο 2P. Μετά μπορούμε να προσθέσουμε ξανά το σημείο P στο σημείο 2P και να πάρουμε το σημείο 3P. Ο καθορισμός του σημείου nP με αυτό τον τρόπο αναφέρεται ως Βαθμωτός Πολλαπλασιασμός ενός σημείου.
  - Ο πολλαπλασιασμός είναι σαν να πολλαπλασιάζουμε μαζί k αντίγραφα του σημείου P, παίρνοντας το σημείο

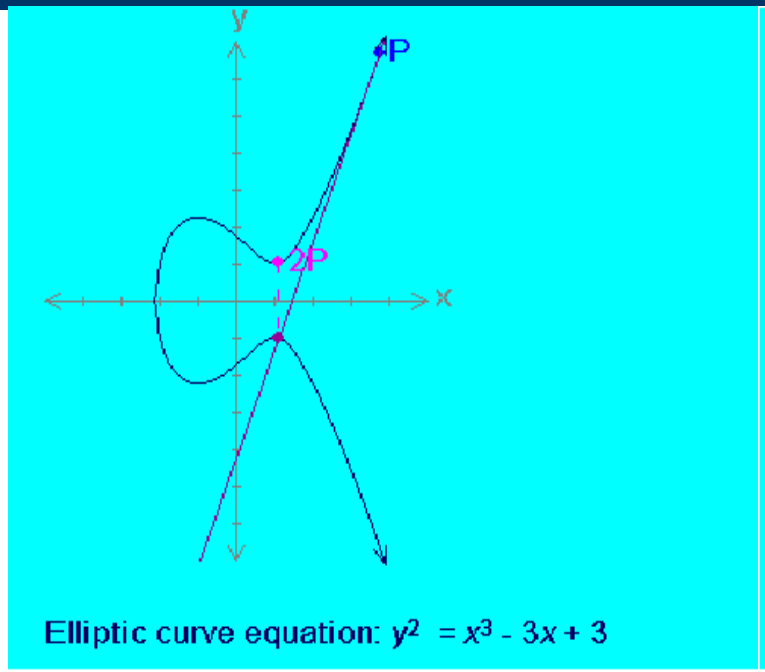
$$P \cdot P \cdot P \cdot P \cdot .... \cdot P = Pk$$

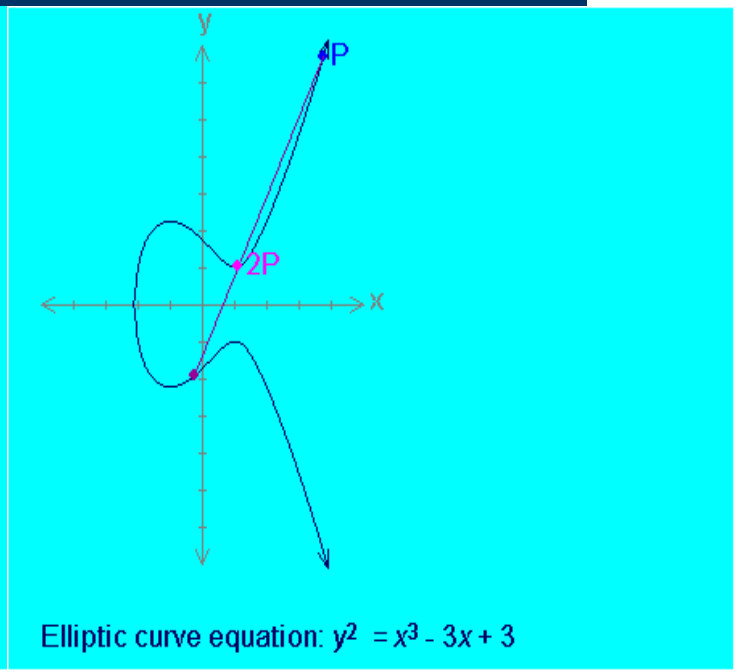
Κρυπτογραφία με ελλειπτικές καμπύλες. (17)



Παίρνουμε ένα σημείο P στην ελλειπτική καμπύλη και φέρουμε την εφαπτόμενη στο σημείο αυτό.

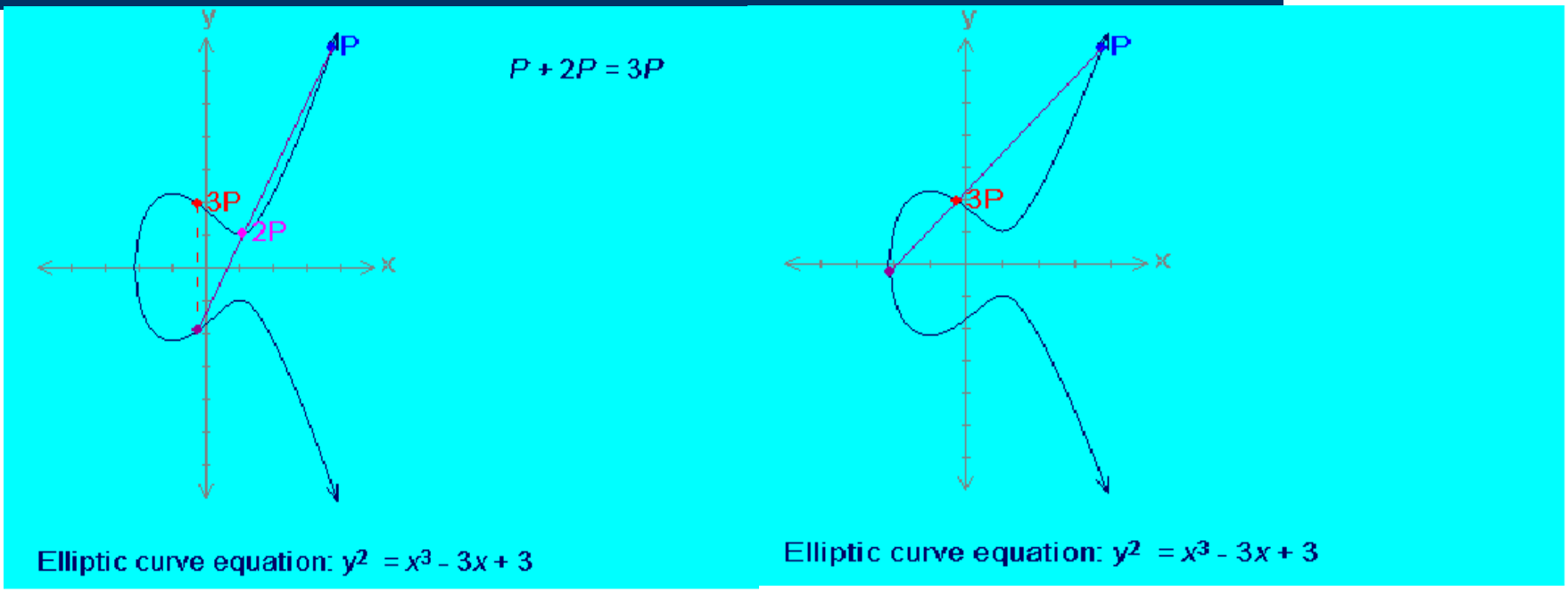
Κρυπτογραφία με ελλειπτικές καμπύλες. (18)





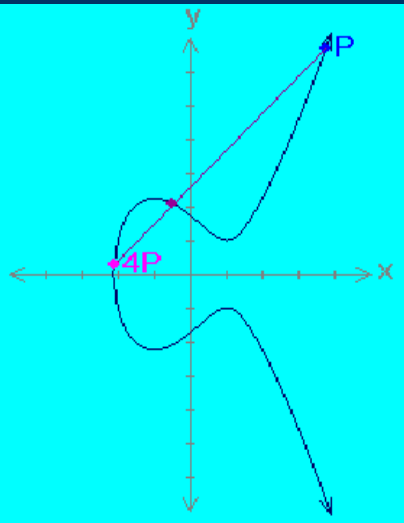
Προκύπτει το σημείο 2P. Φέρνουμε την ευθεία που τέμνει το 2P με το P. Η προέκτασή της τέμνει την EC σε ένα τρίτο σημείο.

Κρυπτογραφία με ελλειπτικές καμπύλες. (19)

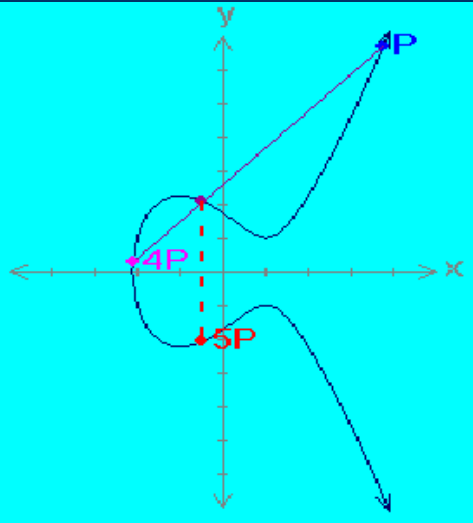


Έτσι, βρίσκουμε το σημείο 3P.

Κρυπτογραφία με ελλειπτικές καμπύλες. (20)



Elliptic curve equation: $y^2 = x^3 - 3x + 3$



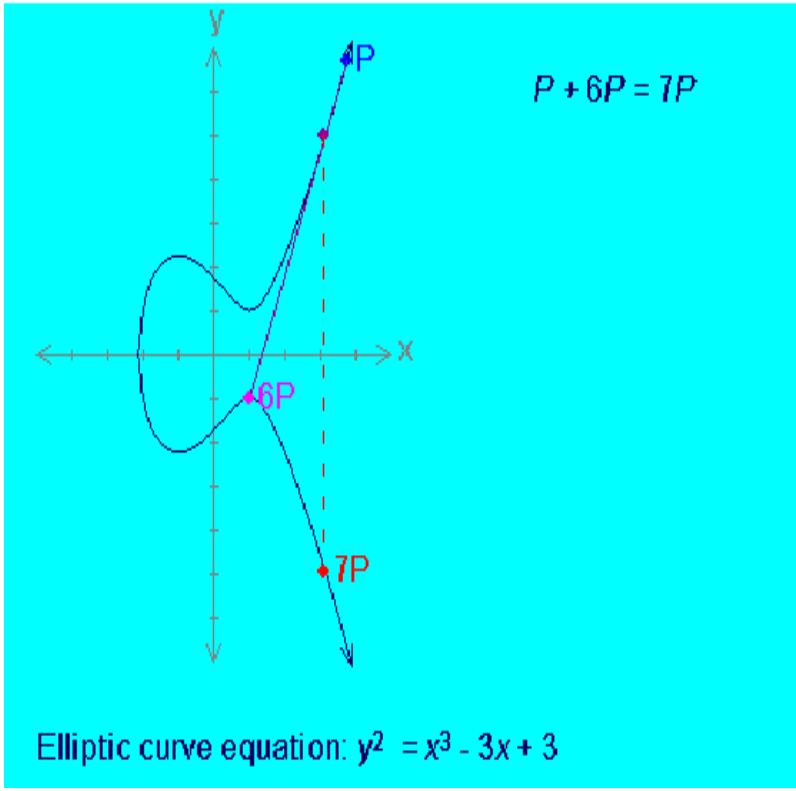
$P + 4P = 5P$

Elliptic curve equation: $y^2 = x^3 - 3x + 3$

Με παρόμοιο τρόπο στα επόμενα σχήματα βρίσκουμε τα 4P, 5P, 6P και 7P αντίστοιχα.

Κρυπτογραφία με ελλειπτικές καμπύλες. (21)

- Στην πολλαπλασιαστική ομάδα Z_p^*, το πρόβλημα του διακριτού λογαρίθμου είναι: Δοσμένων των στοιχείων r και q της ομάδας, και p ένας πρώτος αριθμός, να βρεθεί ο αριθμός k τέτοιος ώστε $r = qk \bmod p$.
- Αν οι ομάδες ελλειπτικών καμπυλών περιγράφονται με τη πράξη του συμβόλου του πολλαπλασιασμού τότε το πρόβλημα του διακριτού λογαρίθμου θα είναι: Δοσμένων των σημείων P και Q σε μια ομάδα, να βρεθεί ένας αριθμός τέτοιος ώστε $Pk = Q$. Ο k λέγεται διακριτός λογάριθμος του Q με βάση το P.
- Όταν η ομάδα ελλειπτικής καμπύλης περιγράφεται από τη πράξη της πρόσθεσης, το πρόβλημα του διακριτού λογαρίθμου είναι: Δοσμένων των σημείων P και Q σε μια ομάδα να βρεθεί ο αριθμός k τέτοιος ώστε $kP = Q$.



Κρυπτογραφία με ελλειπτικές καμπύλες. (22)

- Ο κύριος λόγος για τον οποίο οι διακριτοί λογάριθμοι χρησιμοποιούνται στην κρυπτογραφία είναι ότι έχουν τις ιδιότητες μιας συνάρτησης μοναδικής κατεύθυνσης (one-way).
- Είναι πολύ εύκολο να υπολογιστεί το $y = g^x$ από τα g και x, ενώ είναι πολύ δύσκολο να υπολογιστεί το $\log_g y$.
- Η πιο απλή εφαρμογή του DLP αφορά την απόδειξη της γνησιότητας του χρήστη (user authentication).
  - Αντί να αποθηκεύεται ένα password x_i για κάθε χρήστη i, επιλέγεται ένα πεπερασμένο σώμα F_q και ένα στοιχείο g και στο αρχείο αποθηκεύονται οι τιμές $g^{xi}=y_i$ για κάθε χρήστη i και συγκρίνεται το αποτέλεσμα με κάποιο άλλο αρχείο. Ακόμα και αν κάποιος αποκτήσει πρόσβαση στο αρχείο, θα πρέπει πρώτα να λύσει το DLP για να βρει τα x_i.

Κρυπτογραφία με ελλειπτικές καμπύλες. (23)

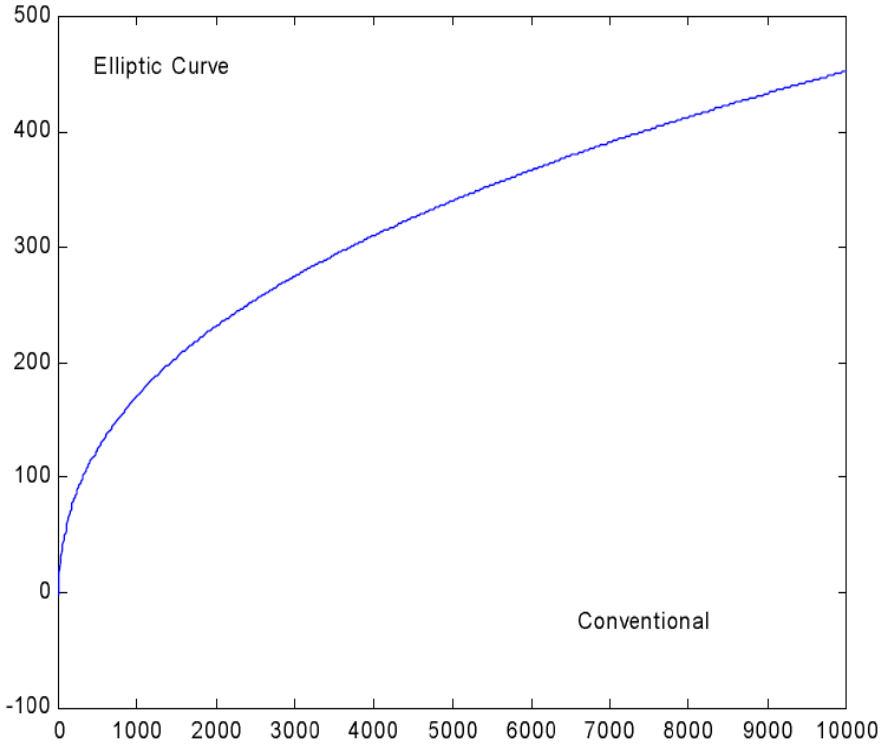
- Άλλη εφαρμογή είναι η ανταλλαγή κλειδιών μεταξύ δύο χρηστών.
  - Ένας ασφαλής αλγόριθμος για ανταλλαγή κλειδιών είναι ο αλγόριθμος των Diffie και Hellman.
  - Επιλέγεται ένα πεπερασμένο σώμα F_q και ένα στοιχείο g τα οποία είναι γνωστά και στους δύο χρήστες. Κάθε χρήστης επιλέγει ένα ιδιωτικό κλειδί x_i. Και οι δύο μπορούν να μοιράζονται το ίδιο κλειδί υψώνοντας ο καθένας το δημόσιο κλειδί του άλλου σε δύναμη ίση με το ιδιωτικό τους κλειδί.
- Οι διακριτοί λογάριθμοι χρησιμοποιούνται επίσης στην κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων.
- Τέλος, μία εφαρμογή του DLP βρίσκεται σε έναν αλγόριθμο για δημιουργία ψηφιακών υπογραφών.
  - Οι ψηφιακές υπογραφές ενσωματώνονται στα μηνύματα που στέλνει ένας χρήστης Α, για να επιβεβαιώσουν τον χρήστη Β πως πράγματι τα μηνύματα στέλνονται από τον Α και όχι από κάποιον που προσποιείται ότι είναι ο Α.

Κρυπτογραφία με ελλειπτικές καμπύλες. (24)

- Οι καλύτεροι γνωστοί γενικοί αλγόριθμοι για το ECDLP έχουν πολυπλοκότητα ανάλογη με: $C_{EC}(n) = 2^{n/2} = q^{1/2}$
- Διακριτοί λογάριθμοι στο F_p έχουν πολυπλοκότητα: $C_{CONV}(N) = \exp(c_0 N^{1/3} (\log(N \log 2))^{2/3})$
- Εξισώνοντας το C_{EC} και το C_{CONV} (και παραλείποντας πάλι τους σταθερούς όρους), αποδεικνύεται ότι για παρόμοια επίπεδα ασφαλείας, πρέπει να ισχύει: $n = \beta N^{1/3} (\log(N \log 2))^{2/3}$
- Οι παράμετροι n και N μπορούν να ερμηνευτούν σαν τα μεγέθη των κλειδιών, σε bits, για τα αντίστοιχα κρυπτογραφικά συστήματα (ελλειπτικών καμπυλών και συμβατικών).

Κρυπτογραφία με ελλειπτικές καμπύλες. (25)

- Αυτό που παρατηρείται είναι ότι το μέγεθος κλειδιού σε ένα σύστημα ελλειπτικών καμπυλών αυξάνεται με ρυθμό ελαφρώς γρηγορότερο από την κυβική ρίζα του αντίστοιχου μεγέθους κλειδιού για τα συμβατικά συστήματα, για την επίτευξη περίπου ισοδύναμης κρυπτογραφικής ισχύς.
- Π.χ. κλειδιά μεγέθους 1024 και 4096 bits (μεγέθη που χρησιμοποιούνται πολύ συχνά στον RSA) αντιστοιχούν σε κλειδιά μεγέθους 173 και 313 bits αντίστοιχα, για συστήματα ελλειπτικών καμπυλών.



Οι κυριότερες εφαρμογές των Ελλειπτικών Καμπυλών στην Κρυπτογραφία (ECC) και οι αλγόριθμοί τους.

- **Ψηφιακές Υπογραφές**
  - ECDSA: Elliptic Curve Digital Signature Algorithm
  - ECPVS: Elliptic Curve Pintsov Vanstone Signatures
  - ECNR: Elliptic Curve Nyberg Rueppel
- **Ανταλλαγή Κλειδιού**
  - ECDH: Elliptic Curve Diffie - Hellman
  - ECMQV: Elliptic Curve Menezes – Qu - Vanstone
- **Κρυπτογράφηση – Αποκρυπτογράφηση**
  - ECIES: Elliptic Curve Integrated Encryption Scheme

Ο αλγόριθμος δημιουργίας ψηφιακής υπογραφής με τη χρήση ελλειπτικών καμπυλών (ECDSA) (1).

- Μία κατηγορία ψηφιακών υπογραφών που χρησιμοποιούνται είναι εκείνες που κατασκευάζονται με τη χρήση ελλειπτικών καμπυλών.
- Όπως γνωρίζουμε η κρυπτογράφηση γίνεται με τη βοήθεια του δημοσίου κλειδιού και η αποκρυπτογράφηση γίνεται μόνον από αυτόν που γνωρίζει το ιδιωτικό κλειδί. Αντίθετα, στις ψηφιακές υπογραφές αυτός που υπογράφει έχει το μυστικό κλειδί και αυτός που επικυρώνει την υπογραφή πρέπει να έχει το δημόσιο.
- Ο ECDSA αλγόριθμος έχει να κάνει με μη συμμετρικές υπογραφές με παράρτημα (asymmetric digital signature with appendix). Υπογραφή με παράρτημα είναι αυτή που δεν εφαρμόζεται απευθείας στο μήνυμα αλλά στην έξοδο μιας hash συνάρτησης που έχει σαν είσοδο το μήνυμα αυτό.
- Όπως θα δούμε παρακάτω εφαρμόζοντας τον αλγόριθμο, η ασφάλεια των ψηφιακών υπογραφών βασίζεται στην δυσκολία επίλυσης του προβλήματος του διακριτού λογαρίθμου (ECDLP).

Ο αλγόριθμος δημιουργίας ψηφιακής υπογραφής με τη χρήση ελλειπτικών καμπυλών (ECDSA) (2).

- **1.** Παράμετροι Ελλειπτικής Καμπύλης:
  Έστω έχουμε το πεπερασμένο σώμα F_{23} και την ελλειπτική καμπύλη $y^2 = x^3 + x + 1$. Επιλέγεται το $G = (x_G, y_G) = (13, 7)$. Αφού $7G = 0$, το σημείο G έχει τάξη $n = 7$.
- Οι παράμετροι της ελλειπτικής καμπύλης θα είναι:
  - Το σώμα F_{23}
  - Η ελλειπτική καμπύλη E
  - Το βασικό σημείο G
  - Η τάξη του G $n = 7$
  - Ο παράγων $h = 4$.

Ο αλγόριθμος δημιουργίας ψηφιακής υπογραφής με τη χρήση ελλειπτικών καμπυλών (ECDSA) (3).

2. Δημιουργία κλειδιού.

Ο Α εκτελεί τα παρακάτω:

1. Επιλέγει έναν τυχαίο ακέραιο d = 3 μεταξύ των [1, n - 1] = [1, 6].
2. Ο Α δημοσιοποιεί το σημείο Q. Υπολογίζει το σημείο Q = dG = 3(13, 7) = (17, 3)
3. Το ιδιωτικό κλειδί του Α είναι το d = 3.

Ο αλγόριθμος δημιουργίας ψηφιακής υπογραφής με τη χρήση ελλειπτικών καμπυλών (ECDSA) (4).

- **3.** Δημιουργία Υπογραφής.
  Ο Α υπογράφει το μήνυμα M = 1110001101010111100. Υποθέτουμε η δεκαδική αναπαράσταση του μηνύματος μετά την εφαρμογή της συνάρτησης κατακερματισμού hash modulo 7 είναι e = 6.
  Ο Α:

1. Επιλέγει τυχαία έναν ακέραιο k = 4 μεταξύ των [1, n - 1] = [1, 6].
2. Υπολογίζει:
   $(x_1, y_1) = kG = 4(13, 7) = (17, 20)$.
3. Αναπαριστά τη συντεταγμένη x_1 με τον ακέραιο $x_1 = 17$.
4. Υπολογίζουμε το $r = x_1 \bmod n = 17 \bmod 7 = 3$.Αν το r=0 πάμε πίσω στο βήμα 2.
5. Υπολογίζει:
   $s = k^{-1}(e + dr) \bmod n = 4^{-1}(6 + 3 \cdot 3) \bmod 7 = 2(15) \bmod 7 = 2$.
   Η υπογραφή στο μήνυμα M είναι τι ζευγάρι (r, s) = (3, 2).

Ο αλγόριθμος δημιουργίας ψηφιακής υπογραφής με τη χρήση ελλειπτικών καμπυλών (ECDSA) (5).

- **4.** Επικύρωση της υπογραφής.
  Ο Β επικυρώνει την υπογραφή (r`, s`) = (3, 2) στο M:

1. Ανακτά το δημόσιο κλειδί του A, Q = (17, 3).
2. Υπολογίζει το e = 6, με τη βοήθεια της συνάρτησης κατακερματισμού hash, εφαρμόζοντάς την στο M.
3. Υπολογίζει το:
   $c = (s`)^{-1} \bmod n = 2^{-1} \bmod 7 = 4$.
4. Υπολογίζει τα:
   $u_1 = e\ c \bmod n = 6 \cdot 4 \bmod 7 = 3$
   και
   $u_2 = r`\ c \bmod n = 3 \cdot 4 \bmod 7 = 5$.
5. Υπολογίζει το σημείο:
   $(x_1, y_1) = u_1G + u_2Q = 3G + 5Q = 3(13, 7) + 5(17, 3) = (17, 20)$.
6. Αναπαριστά τη συντεταγμένη x_1 με τον ακέραιο $x_1 = 17$.
7. Υπολογίζει το $v = x_1 \bmod n = 17 \bmod 7 = 3$.
8. Δέχεται την υπογραφή εφόσον είναι: $v = r` = 3$.

ΕΥΧΑΡΙΣΤΩ ΓΙΑ ΤΗ ΠΡΟΣΟΧΗ ΣΑΣ !