ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (PKC)

ΣΥΝΑΡΤΗΣΕΙΣ ΠΑΓΙΔΑΣ (TFT) ΚΑΙ ΕΠΙΘΕΣΕΙΣ RSA

ΜΕΡΟΣ Ι

ΕΙΣΑΓΩΓΗ ΚΑΙ ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

ΕΙΣΑΓΩΓΗ ΣΤΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (PKC)

Τα Κρυπτοσυστήματα Δημοσίου Κλειδιού (Public Key Cryptosystems - PKC) χρησιμοποιούν ένα ζεύγος κλειδιών: ένα δημόσιο κλειδί για την κρυπτογράφηση και ένα ιδιωτικό κλειδί για την αποκρυπτογράφηση. Αυτή η αρχιτεκτονική επιλύει το πρόβλημα της ασφαλούς ανταλλαγής κλειδιών σε μη ασφαλές κανάλι.

Η ΑΣΦΑΛΕΙΑ ΤΩΝ PKC

Η ασφάλεια των PKC βασίζεται σε προβλήματα της Θεωρίας Αριθμών που είναι υπολογιστικά δύσκολα (intractable) για έναν επιτιθέμενο με Πολυωνυμικό Χρόνο (PPT). Τέτοια προβλήματα είναι η Παραγοντοποίηση (Factoring) και ο Διακριτός Λογάριθμος (DLOG).

Η ΕΝΝΟΙΑ ΤΗΣ ΣΥΝΑΡΤΗΣΗΣ ΠΑΓΙΔΑΣ (TRAPDOOR FUNCTION - TDF)

Μία Συνάρτηση Παγίδας (f) είναι μια συνάρτηση που είναι εύκολο να υπολογιστεί (y=f(x)) αλλά δύσκολο να αντιστραφεί ($x=f^{-1}(y)$) χωρίς μια μυστική πληροφορία, την παγίδα (trapdoor). Όλα τα PKC βασίζονται σε μια τέτοια συνάρτηση. Τα πιο γνωστά παραδείγματα TDF προέρχονται από τον RSA (όπου η παγίδα είναι η παραγοντοποίηση του n) και το Rabin. Η TDF του ElGamal βασίζεται στο πρόβλημα DLOG.

ΕΦΑΡΜΟΓΕΣ ΤΩΝ TDF

Τα PKC και οι TDF είναι απαραίτητα για:

- **Ψηφιακές Υπογραφές:** Χρησιμοποιούν το ιδιωτικό κλειδί για την υπογραφή ενός μηνύματος (π.χ., RSA, ElGamal).
- **Υποδομή Δημοσίου Κλειδιού (PKI):** Διαχείριση ψηφιακών πιστοποιητικών (π.χ., SSL/TLS).
- **Blockchain & Bitcoin:** Χρησιμοποιούν ψηφιακές υπογραφές (ECDSA) για την αυθεντικοποίηση συναλλαγών.

ΥΒΡΙΔΙΚΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΚΑΙ ΚΕΜ

Τα PKC είναι αργά για την κρυπτογράφηση μεγάλων μηνυμάτων. Γι' αυτό χρησιμοποιούνται τα Υβριδικά Κρυπτοσυστήματα, όπου το PKC χρησιμοποιείται μόνο για την ανταλλαγή του συμμετρικού κλειδιού συνεδρίας (session key). Ο μηχανισμός αυτός ονομάζεται Key Encapsulation Mechanism (KEM).

ΜΕΡΟΣ ΙΙ

ΒΑΣΙΚΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ RSA - ΒΑΣΙΚΗ ΛΕΙΤΟΥΡΓΙΑ

Το RSA είναι το πιο διαδεδομένο PKC.

- **Δημόσιο Κλειδί:** (n, e)
- **Ιδιωτικό Κλειδί:** (d) ή (p, q)
- **Κρυπτογράφηση:** $c = m^e \pmod{n}$
- **Αποκρυπτογράφηση:** $m = c^d \pmod{n}$

ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ RSA - ΒΑΣΙΚΗ ΛΕΙΤΟΥΡΓΙΑ

Το RSA βασίζεται στη μαθηματική αρχή ότι είναι εύκολο να πολλαπλασιαστούν δύο μεγάλοι πρώτοι αριθμοί, αλλά είναι υπολογιστικά πολύ δύσκολο να παραγοντοποιηθεί το προκύπτον γινόμενο πίσω στους αρχικούς πρώτους αριθμούς. Αυτή η δυσκολία αποτελεί τη βάση της ασφάλειάς του.

RSA: ΔΗΜΙΟΥΡΓΙΑ ΚΛΕΙΔΙΩΝ

1. **Δημιουργία Κλειδιού:**
   - Ο παραλήπτης επιλέγει δύο μεγάλους **πρώτους αριθμούς**, p και q, και υπολογίζει το $n = p \times q$.
   - Στη συνέχεια υπολογίζει το $\phi(n) = (p-1)(q-1)$ (συνάρτηση Όιλερ).
   - Επιλέγει έναν ακέραιο **εκθέτη κρυπτογράφησης** e (τον δημόσιο εκθέτη) τέτοιο ώστε $1 < e < \phi(n)$ και ο e να είναι πρώτος με το $\phi(n)$.
   - Τέλος, υπολογίζει τον **εκθέτη αποκρυπτογράφησης** d (τον ιδιωτικό εκθέτη) έτσι ώστε $d \times e \equiv 1 \pmod{\phi(n)}$.
   - Το **Δημόσιο Κλειδί** είναι το (n, e) και κοινοποιείται σε όλους.
   - Το **Ιδιωτικό Κλειδί** είναι το (n, d) και διατηρείται μυστικό από τον κάτοχο.

RSA: ΔΗΜΙΟΥΡΓΙΑ ΚΛΕΙΔΙΩΝ

2. **Κρυπτογράφηση:**
   - Ο αποστολέας χρησιμοποιεί το **Δημόσιο Κλειδί** του παραλήπτη (n, e) για να κρυπτογραφήσει το μήνυμα (απλό κείμενο M) σε κρυπτογραφημένο κείμενο (C) χρησιμοποιώντας τον τύπο:

$$C \equiv M^e \pmod{n}$$

3. **Αποκρυπτογράφηση:**
   - Ο παραλήπτης χρησιμοποιεί το μυστικό του **Ιδιωτικό Κλειδί** (n, d) για να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο (C) πίσω στο αρχικό μήνυμα (M) χρησιμοποιώντας τον τύπο:

$$M \equiv C^d \pmod{n}$$

ΠΑΡΑΔΕΙΓΜΑ 1: RSA - ΔΗΜΙΟΥΡΓΙΑ ΚΛΕΙΔΙΩΝ

Έστω μικροί πρώτοι: $p = 3$ και $q = 11$.

1. **Μόναχος:** $n = 3 \cdot 11 = 33$.
2. **Συνάρτηση Euler:** $\phi(n) = (3-1)(11-1) = 2 \cdot 10 = 20$.
3. **Δημόσιος Εκθέτης** e**:** Επιλέγουμε $e = 3$ (μικρότερο του 20, $\gcd(3, 20) = 1$).
4. **Ιδιωτικός Εκθέτης** d**:** Πρέπει $3d \equiv 1 \pmod{20}$. Με δοκιμή, $d = 7$ ($3 \cdot 7 = 21 \equiv 1 \pmod{20}$).

- **Δημόσιο Κλειδί:** $(33, 3)$. **Ιδιωτικό Κλειδί:** 7.

ΠΑΡΑΔΕΙΓΜΑ 2: RSA - ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΑΙ ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ

Χρησιμοποιούμε τα κλειδιά από το Παρ. 1: $(n, e) = (33, 3), d = 7$.

1. **Μήνυμα:** $m = 5$.
2. **Κρυπτογράφηση:** $c = 5^3 \pmod{33} = 125 \pmod{33}$. $125 = 3 \cdot 33 + 26$. Άρα $c = 26$.
3. **Αποκρυπτογράφηση:** $m = 26^7 \pmod{33}$. $26^7 \equiv (-7)^7 \pmod{33}$. $(-7)^2 = 49 \equiv 16 \pmod{33}$. $(-7)^4 \equiv 16^2 = 256 \equiv 25 \pmod{33}$. $m \equiv (-7) \cdot 16 \cdot 25 \pmod{33} \equiv -7 \cdot (400) \pmod{33} \equiv -7 \cdot (400 - 12 \cdot 33) \pmod{33} \equiv -7 \cdot (4) \pmod{33} \equiv -28 \equiv 5 \pmod{33}$. Άρα, $m = 5$.

Η ΑΠΟΚΑΛΥΨΗ ΤΟΥ φ(η) ΣΤΟΝ RCA

Η συνάρτηση $f(m)= m^e \pmod n$ είναι η TDF. Είναι εύκολο να υπολογιστεί. Η αντιστροφή της απαιτεί τον υπολογισμό της e-οστής ρίζας modulo n, κάτι που είναι δύσκολο χωρίς την παγίδα (p και q ή d).

Η γνώση του φ(n) αποκαλύπτει την παραγοντοποίηση του n και, κατά συνέπεια, τον ιδιωτικό εκθέτη d. Αυτό συμβαίνει επειδή $\varphi(n)=n-(p+q)+1$, και γνωρίζοντας το φ(n), μπορούμε να λύσουμε ένα τετραγωνικό πολυώνυμο για να βρούμε τα p και q.

ΕΦΑΡΜΟΓΕΣ RSA

Ο RSA χρησιμοποιείται συνήθως για:

- **Ανταλλαγή Κλειδιών:** Ασφαλή ανταλλαγή συμμετρικών κλειδιών (που χρησιμοποιούνται για ταχύτερη μαζική κρυπτογράφηση) μέσω πρωτοκόλλων όπως το TLS/SSL (που χρησιμοποιείται στο HTTPS).
- **Ψηφιακές Υπογραφές:** Επαλήθευση της αυθεντικότητας ενός μηνύματος ή εγγράφου.

Η ασφάλεια του αλγορίθμου RSA βασίζεται στη δυσκολία της παραγοντοποίησης ακεραίων, πράγμα που σημαίνει ότι όσο μεγαλύτερο είναι το μέγεθος του κλειδιού (το μέγεθος του n), τόσο πιο ασφαλής είναι η επικοινωνία.

ΑΝΤΑΛΛΑΓΗ ΚΛΕΙΔΙΟΥ DIFFIE-HELLMAN (DH)

Το πρωτόκολλο DH επιτρέπει σε δύο μέρη να συμφωνήσουν σε ένα κοινό μυστικό κλειδί μέσω μη ασφαλούς καναλιού. Βασίζεται στο Υπολογιστικό Πρόβλημα Diffie-Hellman (CDH).

- **Κοινές παράμετροι:** Πρώτος p, γεννήτορας g.
- **Διαδικασία:** Αλίκη επιλέγει a, στέλνει $A = g^a \pmod{p}$. Μπάμπης επιλέγει b, στέλνει $B = g^b \pmod{p}$.
- **Κοινό Μυστικό:** $K = B^a \pmod{p} = (g^b)^a \pmod{p} = (g^a)^b \pmod{p} = A^b \pmod{p}$.

ΠΑΡΑΔΕΙΓΜΑ 3: ΑΝΤΑΛΛΑΓΗ ΚΛΕΙΔΙΟΥ DIFFIE-HELLMAN

Κοινή $p = 17, g = 3$.

1. **Αλίκη:** Επιλέγει $a = 4$. Στέλνει $A = 3^4 \pmod{17} = **13**$.
2. **Μπάμπης:** Επιλέγει $b = 6$. Στέλνει $B = 3^6 \pmod{17} = **15**$.
3. **Κοινό Μυστικό** K**:** $K = B^a \pmod{17} = 15^4 \pmod{17} = **16**$.

ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ ELGAMAL

Το ElGamal είναι ένα PKC που βασίζεται στο Πρόβλημα Διακριτού Λογαρίθμου (DLOG), στενά συνδεδεμένο με το DH.

- **Δημόσιο Κλειδί:** (p, g, y), όπου $y = g^x \pmod p$.
- **Ιδιωτικό Κλειδί:** x.
- Η κρυπτογράφηση παράγει ένα ζεύγος τιμών (συστοιχία κρυπτοκειμένου).

ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ RABIN

Το Κρυπτοσύστημα Rabin είναι ένα ασύμμετρο σχήμα κρυπτογράφησης δημοσίου κλειδιού του οποίου η ασφάλεια βασίζεται στην υπολογιστική δυσκολία εύρεσης τετραγωνικών ριζών modulo ενός μεγάλου σύνθετου αριθμού, πρόβλημα που είναι αποδεδειγμένα εξίσου δύσκολο με την παραγοντοποίηση ακεραίων.

ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ RABIN

Βασικά Χαρακτηριστικά

- **Ασφάλεια (Security):** Η κρυπτογραφική του ασφάλεια είναι ισοδύναμη με το πρόβλημα της παραγοντοποίησης μεγάλων αριθμών (Integer Factorization Problem). Αυτό είναι ένα ισχυρότερο μαθηματικό πλεονέκτημα σε σχέση με το RSA, όπου η παραγοντοποίηση είναι πιθανώς πιο δύσκολη από την αποκρυπτογράφηση.

ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ RABIN

- **Δημιουργία Κλειδιού (Key Generation):**
  - Επιλέγονται δύο μεγάλοι, διακριτοί πρώτοι αριθμοί p και q.
  - Υπολογίζεται ο **μέγιστος κοινός διαιρέτης** (modulus) $n = p \cdot q$.
  - Το **Δημόσιο Κλειδί** (Public Key) είναι ο αριθμός n.
  - Το **Ιδιωτικό Κλειδί** (Private Key) είναι το ζεύγος (p, q).

ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ RABIN

- **Κρυπτογράφηση (Encryption):** Το μήνυμα m (μετατρεμμένο σε αριθμό) κρυπτογραφείται με **τετραγωνισμό modulo** n:

$$c = m^2 \pmod{n}$$

- **Μειονέκτημα (Ambiguity):** Το βασικό μειονέκτημα είναι ότι η αποκρυπτογράφηση (εύρεση τετραγωνικής ρίζας του c modulo n) δίνει συνήθως **τέσσερις πιθανούς υποψήφιους** για το αρχικό μήνυμα (m). Απαιτείται επιπλέον πληροφορία (π.χ. ειδική μορφοποίηση/padding του μηνύματος) για την αναγνώριση του σωστού μηνύματος.

ΤΟ ΚΡΥΠΤΟΣΥΣΤΗΜΑ RABIN

📝 Σύνοψη Λειτουργίας

1. **Δημόσιο Κλειδί (Public Key):** n
2. **Ιδιωτικό Κλειδί (Private Key):** (p, q)
3. **Κρυπτογράφηση:** $m \to c = m^2 \pmod{n}$
4. **Αποκρυπτογράφηση:** $c \to$ Εύρεση $\sqrt{c} \pmod{n}$ με χρήση των p, q και του **Κινεζικού Θεωρήματος Υπολοίπων** (Chinese Remainder Theorem - CRT). (Δίνει 4 αποτελέσματα, από τα οποία πρέπει να επιλεγεί το σωστό m).

Ο ΚΡΥΠΤΟΓΡΑΦΙΚΟΣ ΑΛΓΟΡΙΘΜΟΣ PAILLIER

🔑 Βασικά Χαρακτηριστικά του Paillier

- **Υπολογιστική Βάση:** Βασίζεται στην υπολογιστική δυσκολία του **προβλήματος σύνθετης υπολειμματικής κλάσης (Composite Residuosity Class Problem)**, το οποίο σχετίζεται στενά με την n**-οστή ρίζα modulo** n^2 .
  - Πιο συγκεκριμένα, η ασφάλειά του εξαρτάται από την υπόθεση ότι είναι δύσκολο να υπολογιστεί η n**-οστή ρίζα** μιας τιμής z modulo n^2 (δηλαδή να βρεθεί m τέτοιο ώστε $m^n \equiv z \pmod{n^2}$) όταν το n είναι το γινόμενο δύο μεγάλων πρώτων αριθμών ($n = pq$).

Ο ΚΡΥΠΤΟΓΡΑΦΙΚΟΣ ΑΛΓΟΡΙΘΜΟΣ PAILLIER

- **Κύρια Ιδιότητα (Ομομορφισμός):** Η πιο σημαντική του ιδιότητα είναι η **Πρόσθετη Ομομορφική Ιδιότητα (Additive Homomorphic Property)**.
  - Αυτό σημαίνει ότι αν έχουμε δύο κρυπτογραφημένα μηνύματα, $E(m_1)$ και $E(m_2)$, μπορούμε να πολλαπλασιάσουμε τις κρυπτογραφημένες τιμές τους, και το αποτέλεσμα θα είναι η κρυπτογραφημένη τιμή του **αθροίσματος** των αρχικών μηνυμάτων:

$$E(m_1) \cdot E(m_2) \equiv E(m_1 + m_2) \pmod{n^2}$$

- Αυτή η ιδιότητα είναι ιδιαίτερα χρήσιμη σε εφαρμογές όπου απαιτείται επεξεργασία δεδομένων **χωρίς αποκρυπτογράφηση** (π.χ., ψηφοφορία, cloud computing).

Ο ΚΡΥΠΤΟΓΡΑΦΙΚΟΣ ΑΛΓΟΡΙΘΜΟΣ PAILLIER

- **Επεκταμένη Ομομορφική Ιδιότητα (Πολλαπλασιασμός με Σταθερά):** Επιπλέον, υποστηρίζει τον πολλαπλασιασμό του κρυπτογραφημένου μηνύματος με μια **σταθερά** k:

$$(E(m_1))^k \equiv E(k \cdot m_1) \pmod{n^2}$$

Ο Paillier είναι ένα κλασικό παράδειγμα **μερικώς ομομορφικής κρυπτογραφίας (Partially Homomorphic Encryption - PHE)**, καθώς υποστηρίζει την πρόσθεση (και τον πολλαπλασιασμό με σταθερά), αλλά όχι τον πολλαπλασιασμό μεταξύ δύο κρυπτογραφημένων μηνυμάτων.

ΠΑΡΑΔΕΙΓΜΑ 4:
ΥΠΟΛΟΓΙΣΜΟΣ ΜΕΣΟΥ ΟΡΟΥ ΣΤΗΝ «ΟΜΙΧΛΗ»

Ας υποθέσουμε ένα σενάριο όπου μια εταιρεία (Α) θέλει να βρει το **συνολικό άθροισμα των πωλήσεων** από δύο πωλητές (Π1 και Π2), χωρίς όμως ο υπολογιστής (Server) που κάνει την πράξη να γνωρίζει τις επιμέρους πωλήσεις για λόγους εμπιστευτικότητας.

1. Τα Αρχικά Δεδομένα (Plaintexts)

- **Πωλητής 1 (m_1):** Πωλήσεις αξίας **10 μονάδων**
- **Πωλητής 2 (m_2):** Πωλήσεις αξίας **5 μονάδων**

Αναμενόμενο Άθροισμα (Μυστικό): $10 + 5 = 15$

ΠΑΡΑΔΕΙΓΜΑ PAILLIER: ΥΠΟΛΟΓΙΣΜΟΣ ΜΕΣΟΥ ΟΡΟΥ ΣΤΗΝ «ΟΜΙΧΛΗ»

2. Η Κρυπτογράφηση (Encryption)

Ο κάθε πωλητής κρυπτογραφεί τα δεδομένα του χρησιμοποιώντας το **Δημόσιο Κλειδί (PK)** του Paillier.

Πωλητής	Μήνυμα (m)	Κρυπτογράφηση ($E(m)$)
Π1	$m_1 = 10$	$E(10) = 45281$
Π2	$m_2 = 5$	$E(5) = 9370$

(Σημείωση: Τα νούμερα 45281 και 9370 είναι υποθετικά κρυπτογραφημένα μηνύματα. Στην πράξη, είναι πολύ μεγαλύτερα και οι πράξεις γίνονται $(\mathrm{mod}\ n^2)$*).*

ΠΑΡΑΔΕΙΓΜΑ PAILLIER: ΥΠΟΛΟΓΙΣΜΟΣ ΜΕΣΟΥ ΟΡΟΥ ΣΤΗΝ «ΟΜΙΧΛΗ»

3. Η Ομομορφική Πράξη (στο Server)

Ο Server λαμβάνει μόνο τα κρυπτογραφημένα μηνύματα 45281 και 9370. **Δεν βλέπει ποτέ τους αριθμούς 10 και 5.**

Για να βρει το άθροισμα των αρχικών μηνυμάτων $(10 + 5)$, ο Server **πολλαπλασιάζει** τα κρυπτογραφημένα μηνύματα:

$$\text{Κρυπτογραφημένο Άθροισμα } (C_{add}) = E(m_1) \cdot E(m_2)$$

$$C_{add} = 45281 \cdot 9370 = 424269970$$

Ο Server ολοκλήρωσε τον υπολογισμό **πάνω σε κρυπτογραφημένα δεδομένα**.

ΠΑΡΑΔΕΙΓΜΑ PAILLIER: ΥΠΟΛΟΓΙΣΜΟΣ ΜΕΣΟΥ ΟΡΟΥ ΣΤΗΝ «ΟΜΙΧΛΗ»

4. Η Αποκρυπτογράφηση (Decryption)

Ο Server στέλνει το τελικό κρυπτογραφημένο αποτέλεσμα ($C_{add} = 424269970$) πίσω στον κάτοχο του **Ιδιωτικού Κλειδιού (SK)** της εταιρείας Α.

Η εταιρεία Α αποκρυπτογραφεί το αποτέλεσμα:

$$D(C_{add}) = D(424269970)$$

Αποτέλεσμα:

$$D(C_{add}) = 15$$

ΠΑΡΑΔΕΙΓΜΑ PAILLIER: ΥΠΟΛΟΓΙΣΜΟΣ ΜΕΣΟΥ ΟΡΟΥ ΣΤΗΝ «ΟΜΙΧΛΗ»

🎯 Συμπέρασμα

Ο Server πέτυχε να υπολογίσει το **15** $(10 + 5)$ χρησιμοποιώντας μόνο τον πολλαπλασιασμό των $E(10)$ και $E(5)$, χωρίς να γνωρίζει τις επιμέρους τιμές 10 και 5.

Αυτή είναι η δύναμη της **Πρόσθετης Ομομορφικής Ιδιότητας** του Paillier: επιτρέπει την εκτέλεση της πράξης της **πρόσθεσης** σε κρυπτογραφημένα δεδομένα.

ΜΕΤΑ-ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ (PQC)

Η Μετα-Κβαντική Κρυπτογραφία (PQC) μελετά κρυπτοσυστήματα που παραμένουν ασφαλή έναντι πιθανής επίθεσης από κβαντικό υπολογιστή. Η Κρυπτογραφία με Ελλειπτικές Καμπύλες (ECC) θεωρείται PQC, αλλά ο αλγόριθμος του Shor θα μπορούσε να σπάσει το πρόβλημα DLOG στις καμπύλες. Ως εκ τούτου, η έρευνα στρέφεται σε συστήματα που βασίζονται σε Πλέγματα (Lattices).

ΓΙΑΤΙ ΕΙΝΑΙ ΣΗΜΑΝΤΙΚΗ Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΒΑΣΙΣΜΕΝΗ ΣΕ ΠΛΕΓΜΑΤΑ (LATTICE-BASED CRYPTOGRAPHY)

Τα πλέγματα αποτελούν τη βάση για τη λεγόμενη **Μετα-Κβαντική Κρυπτογραφία (PQC)**.

- **Κβαντική Αντοχή:** Τα κρυπτοσυστήματα που βασίζονται σε πλέγματα (όπως το **CRYSTALS-Kyber** για την ανταλλαγή κλειδιών και το **CRYSTALS-Dilithium** για ψηφιακές υπογραφές – που επιλέχθηκαν από το NIST) θεωρούνται ανθεκτικά σε επιθέσεις από έναν κβαντικό υπολογιστή (σε αντίθεση με το RSA και το ECC που καταρρίπτονται από τον αλγόριθμο του Shor).
- **Υποκείμενη Δυσκολία:** Η ασφάλεια αυτών των συστημάτων βασίζεται στη δυσκολία επίλυσης των προβλημάτων SVP και CVP σε **υψηλές διαστάσεις**, κάτι που θεωρείται δύσκολο ακόμα και για τους κβαντικούς υπολογιστές.
- **Απόδοση:** Πολλά σχήματα πλέγματος είναι γρήγορα και έχουν μικρό μέγεθος κλειδιού, καθιστώντας τα πρακτικά για εφαρμογές στο διαδίκτυο.

ΜΕΡΟΣ ΙΙΙ

ΕΠΙΘΕΣΕΙΣ ΣΤΟΝ RSA

ΕΠΙΣΚΟΠΗΣΗ ΕΠΙΘΕΣΕΩΝ ΣΤΟΝ RSA

Οι επιθέσεις στο RSA αποσκοπούν είτε στην παραγοντοποίηση του *n* είτε στην εύρεση του ιδιωτικού κλειδιού *d*. Συχνά εκμεταλλεύονται την κακή επιλογή των κρυπτογραφικών παραμέτρων.

Η ΕΠΙΘΕΣΗ ΤΟΥ WIENER

- Πρόκειται για έναν τύπο κρυπτογραφικής επίθεσης που στρέφεται κατά του κρυπτοσυστήματος **RSA**.
- Ονομάστηκε έτσι από τον κρυπτολόγο **Μάικλ Τζ. Βίνερ** (Michael J. Wiener).
- Η επίθεση χρησιμοποιεί τη μέθοδο των **συνεχών κλασμάτων** για τον εντοπισμό του ιδιωτικού κλειδιού d, όταν αυτό είναι **αρκετά μικρό** (συγκεκριμένα, όταν $d < \frac{1}{3}N^{1/4}$, όπου N είναι ο RSA πολλαπλασιαστής).

Ουσιαστικά, εκμεταλλεύεται το γεγονός ότι αν το ιδιωτικό κλειδί d είναι μικρό, τότε ο λόγος k/d αποτελεί μια καλή προσέγγιση του $e/\phi(N)$ (όπου e είναι το δημόσιο κλειδί και $\phi(N)$ η συνάρτηση Euler), η οποία μπορεί να βρεθεί αποτελεσματικά μέσω των συνεχών κλασμάτων του e/N.

Η ΕΠΙΘΕΣΗ ΤΟΥ WIENER

1. Η Σχέση του RSA

Στο κρυπτοσύστημα RSA, το δημόσιο κλειδί e και το ιδιωτικό κλειδί d συνδέονται με την εξής σχέση:

$$e \cdot d \equiv 1 \pmod{\phi(N)}$$

Όπου:

- N είναι ο RSA πολλαπλασιαστής.
- $\phi(N)$ είναι η συνάρτηση Euler του N.

Αυτή η ισοτιμία σημαίνει ότι υπάρχει ένας ακέραιος k τέτοιος ώστε:

$$e \cdot d - k \cdot \phi(N) = 1$$

Η ΕΠΙΘΕΣΗ ΤΟΥ WIENER

2. Η Προσέγγιση με Συνεχή Κλάσματα

Αναδιατάσσοντας την παραπάνω εξίσωση και διαιρώντας με $d \cdot \phi(N)$, παίρνουμε:

$$\frac{e}{\phi(N)} - \frac{k}{d} = \frac{1}{d \cdot \phi(N)}$$

Αυτό σημαίνει ότι το κλάσμα $\frac{k}{d}$ είναι μια **πολύ καλή προσέγγιση** του $\frac{e}{\phi(N)}$.

Η ΕΠΙΘΕΣΗ ΤΟΥ WIENER

3. Η Αδυναμία

Το πρόβλημα είναι ότι ο επιτιθέμενος δεν γνωρίζει το $\phi(N)$, παρά μόνο το N. Ωστόσο, για μεγάλους πρώτους αριθμούς p και q, ισχύει ότι:

$$\phi(N) = (p-1)(q-1) = pq - p - q + 1 = N - (p+q) + 1$$

Εφόσον το $p+q$ είναι σχετικά μικρό σε σχέση με το N, το $\phi(N)$ είναι **πολύ κοντά** στο N.

Επομένως, το $\frac{e}{N}$ είναι μια καλή προσέγγιση του $\frac{e}{\phi(N)}$, άρα και του $\frac{k}{d}$.

$$\frac{k}{d} \approx \frac{e}{\phi(N)} \approx \frac{e}{N}$$

Η ΕΠΙΘΕΣΗ ΤΟΥ WIENER

4. Η Εφαρμογή της Επίθεσης

Το θεώρημα των συνεχών κλασμάτων λέει ότι αν ένα κλάσμα $\frac{k}{d}$ προσεγγίζει ένα πραγματικό αριθμό α με μεγάλη ακρίβεια, τότε το $\frac{k}{d}$ είναι ένας από τους **αναγωγούς** (convergents) της ανάπτυξης του α σε συνεχές κλάσμα.

Στην επίθεση του Βίνερ, ο επιτιθέμενος:

1. Υπολογίζει την ανάπτυξη του $\frac{e}{N}$ σε **συνεχές κλάσμα**.
2. Εξετάζει όλους τους **αναγωγούς** $\frac{k}{d_{δοκιμής}}$ που προκύπτουν.
3. Για κάθε αναγωγό, χρησιμοποιεί τον παρονομαστή $d_{δοκιμής}$ ως υποψήφιο ιδιωτικό κλειδί d και ελέγχει αν ικανοποιεί τη σχέση του RSA.

Η ΕΠΙΘΕΣΗ ΤΟΥ WIENER

Η Προϋπόθεση του Βίνερ

Η επιτυχία της επίθεσης βασίζεται στο **Θεώρημα του Βίνερ**, το οποίο εγγυάται ότι αν το ιδιωτικό κλειδί d είναι μικρό:

$$d < \frac{1}{3} N^{1/4}$$

τότε η προσέγγιση είναι τόσο καλή που το k/d **σίγουρα** θα είναι ένας από τους αναγωγούς του e/N, επιτρέποντας στον επιτιθέμενο να βρει το d σε πολυωνυμικό χρόνο.

Η ΕΠΙΘΕΣΗ ΤΟΥ WIENER

Αντιμετώπιση

Για να αποφευχθεί η επίθεση του Βίνερ, ο σχεδιασμός του RSA απαιτεί:

1. **Μεγάλο ιδιωτικό κλειδί** d: Το d πρέπει να είναι αρκετά μεγάλο ώστε να μην ικανοποιείται η συνθήκη $d < \frac{1}{3}N^{1/4}$.
2. **Μεγάλο δημόσιο κλειδί** e: Αν και δεν σταματά την επίθεση, ένα μεγάλο e βοηθά στο να διασφαλιστεί ότι το d είναι μεγάλο.

Στην πράξη, οι τυπικές τιμές των κλειδιών στο RSA διασφαλίζουν ότι το d είναι μεγάλο και η επίθεση του Βίνερ δεν λειτουργεί.

ΕΠΙΘΕΣΕΙΣ ΒΑΣΙΣΜΕΝΕΣ ΣΕ ΠΛΕΓΜΑΤΑ (LATTICES)

Είναι σημαντικό να κατανοήσουμε ότι τα πλέγματα έχουν δύο βασικούς, αντιφατικούς ρόλους στην κρυπτογραφία:

1. **Ως Εργαλείο Κρυπτανάλυσης (Επιθέσεις):** Χρησιμοποιούνται για να επιτεθούν σε **παραδοσιακά** κρυπτοσυστήματα (όπως το RSA ή το κρυπτοσύστημα με σακίδιο).
2. **Ως Βάση Ασφάλειας (Μετα-Κβαντική Κρυπτογραφία):** Χρησιμοποιούνται για την κατασκευή **νέων** κρυπτοσυστημάτων (όπως το Kyber και το Dilithium), τα οποία θεωρούνται ανθεκτικά ακόμη και σε κβαντικούς υπολογιστές.

ΕΠΙΘΕΣΕΙΣ ΒΑΣΙΣΜΕΝΕΣ ΣΕ ΠΛΕΓΜΑΤΑ (LATTICES)

Στις κρυπταναλυτικές επιθέσεις, ο επιτιθέμενος "μεταφράζει" το πρόβλημα του σπασίματος του κώδικα σε ένα **υπολογιστικό πρόβλημα πλέγματος**.

Το βασικό ιδέα είναι:

1. **Μετατροπή:** Οι πληροφορίες του κρυπτοσυστήματος (π.χ., το δημόσιο κλειδί και τυχόν διαρρέουσες πληροφορίες) κωδικοποιούνται ως μια **βάση** ενός πλέγματος L.
2. **Πρόβλημα Πλέγματος:** Το κλειδί ή το καθαρό μήνυμα που αναζητείται αντιστοιχεί σε ένα **μικρό διάνυσμα** v σε αυτό το πλέγμα.

ΕΠΙΘΕΣΕΙΣ ΒΑΣΙΣΜΕΝΕΣ ΣΕ ΠΛΕΓΜΑΤΑ (LATTICES)

3. **Επίλυση:** Ο επιτιθέμενος χρησιμοποιεί αλγορίθμους (όπως ο **LLL** – Lenstra-Lenstra-Lovász) για να βρει αυτό το μικρό διάνυσμα, επιλύοντας ένα από τα "δύσκολα" προβλήματα πλέγματος:
   - **SVP (Shortest Vector Problem - Πρόβλημα Συντομότερου Διανύσματος):** Εύρεση του μικρότερου μη-μηδενικού διανύσματος στο πλέγμα.
   - **CVP (Closest Vector Problem - Πρόβλημα Πλησιέστερου Διανύσματος):** Εύρεση του διανύσματος του πλέγματος που βρίσκεται πλησιέστερα σε ένα δοθέν σημείο εκτός του πλέγματος.

ΕΠΙΘΕΣΕΙΣ ΒΑΣΙΣΜΕΝΕΣ ΣΕ ΠΛΕΓΜΑΤΑ (LATTICES)

- Παράδειγμα: Επίθεση Coppersmith στο RSA

Η πιο γνωστή εφαρμογή είναι η **Επίθεση Coppersmith** (η οποία αποτελεί επέκταση της επίθεσης του Βίνερ) κατά του RSA. Αυτή η επίθεση χρησιμοποιεί πλέγματα για να παραγοντοποιήσει τον RSA πολλαπλασιαστή N ή να ανακτήσει το ιδιωτικό κλειδί d αν γνωρίζει κανείς μερικά από τα κρυφά bits του d ή αν το d είναι μικρό.

ΕΠΙΘΕΣΗ ΣΕ ΜΙΚΡΑ ΜΗΝΥΜΑΤΑ (SMALL MESSAGE ATTACK)

Αν ο δημόσιος εκθέτης e είναι μικρός (π.χ., $e = 3$) και το μήνυμα m είναι μικρό ώστε $m^e < n$, τότε το κρυπτογραφημένο μήνυμα $c = m^e \pmod{n}$ είναι απλά $c = m^e$ στους ακέραιους. Ένας επιτιθέμενος μπορεί να βρει το m υπολογίζοντας την e-οστή ρίζα του c στους πραγματικούς.

ΠΑΡΑΔΕΙΓΜΑ 5: ΕΠΙΘΕΣΗ SMALL MESSAGE RSA (e=3)

Δημόσιο κλειδί $(n, e) = (1000000, 3)$.

1. **Μήνυμα:** $m = 50$.
2. **Κρυπτογράφηση:** $c = 50^3 \pmod{1000000} = **125000**$.
3. **Επίθεση:** Επειδή $c < n$, ο επιτιθέμενος υπολογίζει $m = \sqrt[3]{125000} = **50**$.

- **Συμπέρασμα:** Αποκάλυψη του m χωρίς το ιδιωτικό κλειδί.

CRT ΚΑΙ RSA
(ΚΙΝΕΖΙΚΟ ΘΕΩΡΗΜΑ ΥΠΟΛΟΙΠΩΝ)

Το **Κινέζικο Θεώρημα Υπολοίπων (CRT)** χρησιμοποιείται για την **ταχύτερη αποκρυπτογράφηση** στο RSA. Αντί να υπολογιστεί $m = c^d \pmod{n}$, υπολογίζονται m_p και m_q και στη συνέχεια συνδυάζονται για να βρεθεί το m.

ΣΥΜΠΕΡΑΣΜΑΤΑ ΕΠΙΘΕΣΕΩΝ

Η σωστή επιλογή παραμέτρων είναι επιβεβλημένη για την ασφάλεια του RSA:

- **Οι πρώτοι p , q πρέπει να είναι τυχαίοι και μεγάλοι.**
- **Ο ιδιωτικός εκθέτης d δεν πρέπει να είναι μικρός.**

ΣΥΝΟΨΗ & ΣΥΜΠΕΡΑΣΜΑΤΑ

PKC	Χρησιμοποιούν δημόσιο/ιδιωτικό κλειδί για εμπιστευτικότητα και αυθεντικοποίηση.
TDF	Η κεντρική μαθηματική δομή των PKC. Εύκολη μονόδρομη λειτουργία, δύσκολη αντιστροφή χωρίς παγίδα.
RSA / Rabin	Βασίζονται στην υπολογιστική δυσκολία της **Παραγοντοποίησης**.
ElGamal / DH	Βασίζονται στην υπολογιστική δυσκολία του **Διακριτού Λογαρίθμου**.
Επιθέσεις RSA	Οι επιθέσεις του Wiener και Coppersmith εκμεταλλεύονται την κακή επιλογή παραμέτρων (μικρός d, γνωστά bits του p).
PQC	Η έρευνα στρέφεται σε συστήματα βασισμένα σε **Πλέγματα** για αντοχή σε κβαντικούς υπολογιστές.

ΕΡΩΤΗΣΕΙΣ ΠΡΟΣ ΣΥΖΗΤΗΣΗ

- Εξηγήστε αναλυτικά γιατί η γνώση της τιμής φ(n) σε ένα κρυπτοσύστημα RSA καθιστά άμεσα δυνατή την παραγοντοποίηση του μονάχου n=pq και, κατά συνέπεια, την εύρεση του ιδιωτικού κλειδιού d.
- Ποια είναι η διαφορά μεταξύ του Υπολογιστικού Προβλήματος Diffie-Hellman (CDH) και του Προβλήματος Απόφασης Diffie-Hellman (DDH); Ποιο από τα δύο προβλήματα αποτελεί την ισχυρότερη υπόθεση ασφαλείας;

ΕΡΩΤΗΣΕΙΣ ΠΡΟΣ ΣΥΖΗΤΗΣΗ

- Περιγράψτε τη βασική ιδέα της Επίθεσης του Wiener στο RSA. Ποιες παραμέτρους του συστήματος εκμεταλλεύεται και ποιο μαθηματικό εργαλείο χρησιμοποιεί για να επιτύχει την επίθεση;
- Επεξηγήστε την έννοια της Πρόσθετης Ομομορφικής Ιδιότητας του κρυπτοσυστήματος Paillier. Δώστε ένα παράδειγμα πρακτικής εφαρμογής αυτής της ιδιότητας.
- Συγκρίνετε το κρυπτοσύστημα RSA με το κρυπτοσύστημα Rabin. Πώς συνδέεται η ασφάλεια του καθενός με το πρόβλημα της παραγοντοποίησης και ποιες είναι οι διαφορές στην αποκρυπτογράφηση;

ΠΡΟΒΛΗΜΑΤΑ ΕΞΑΣΚΗΣΗΣ

1. **RSA - Δημιουργία Κλειδιών:** Δίνονται οι πρώτοι $p = 13$ και $q = 17$.
   - Να υπολογίσετε τον μονάχο n και το $\phi(n)$.
   - Αν επιλεγεί $e = 35$, να βρείτε τον ιδιωτικό εκθέτη d.
2. **Diffie-Hellman - Υπολογισμός Κλειδιού:** Στο $\mathbb{Z}_{29}^*$ με γεννήτορα $g = 2$.
   - Η Αλίκη επιλέγει $a = 5$. Να υπολογίσετε το A.
   - Ο Μπάμπης λαμβάνει το A και υπολογίζει το κοινό μυστικό κλειδί K, αν γνωρίζει ότι το δικό του ιδιωτικό κλειδί είναι $b = 12$.

ΠΡΟΒΛΗΜΑΤΑ ΕΞΑΣΚΗΣΗΣ

3. **RSA - Small Message Attack:** Δημόσιο κλειδί $(n, e) = (5600000000, 5)$. Το κρυπτοκείμενο είναι $c = 3200000$. Να βρεθεί το αρχικό μήνυμα m.
4. **CRT και RSA (Εφαρμογή):** Δίνονται τα υπολογιστικά αποτελέσματα $x \equiv 2 \pmod 3$ και $x \equiv 3 \pmod 5$. Να βρεθεί η τιμή του $x \pmod{15}$ χρησιμοποιώντας το Κινέζικο Θεώρημα Υπολοίπων.
5. **Rabin - Υπολογισμός Κρυπτοκειμένου:** Δίνεται ο μόναχος $n = 21$ και το μήνυμα $m = 5$. Να υπολογιστεί το κρυπτοκείμενο c του κρυπτοσυστήματος Rabin.