ΚΡΥΠΤΟΓΡΑΦΙΑ

Ψηφιακή ασφάλεια και ιδιωτικότητα

Γεώργιος Σπαθούλας

Msc Πληροφορική και υπολογιστική βιοιατρική

Πανεπιστήμιο Θεσσαλίας

ΙΔΙΟΤΗΤΕΣ ΑΣΦΑΛΕΙΑΣ

ΙΔΙΟΤΗΤΕΣ ΑΣΦΑΛΕΙΑΣ ΑΓΑΘΩΝ

- **Εμπιστευτικότητα (Confidentiality) :** Αποφυγή αποκάλυψης πληροφοριών χωρίς την άδεια του ιδιοκτήτη τους
- **Εγκυρότητα (Integrity) :** Απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας
- **Διαθεσιμότητα (Availability) :** Αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας σε εξουσιοδοτημένους χρήστες
- **Ανιχνευσιμότητα (Accountability) :** Η δυνατότητα ανίχνευσης συμβάντων και των υπευθύνων τους

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

- **Η πληροφορία δεν γίνεται γνωστή σε μη εξουσιοδοτημένες οντότητες**
- Η έννοια της εμπιστευτικότητας προϋποθέτει την ύπαρξη μίας πολιτικής ελέγχου πρόσβασης που καθορίζει ποιος ή τι μπορεί να έχει πρόσβαση σε κάποια δεδομένα
- Παράδειγμα : Ιατρικά δεδομένα υποψηφίων για μία θέση γίνονται γνωστά στον εργοδότη ή μία εταιρεία αποκτά πρόσβαση στα σχέδια ενός μελλοντικού προϊόντος μίας ανταγωνίστριας της

ΕΓΚΥΡΟΤΗΤΑ

- **Τα δεδομένα δεν έχουν αλλάξει**
- Η εγκυρότητα των δεδομένων απαιτεί αυτά να μην έχουν αλλοιωθεί κατά οποιονδήποτε τρόπο από κάποιον που δεν έχει τα απαραίτητα δικαιώματα
- Παράδειγμα : Ένα ηλεκτρονικό σύστημα πληρωμών αλλάζει το ποσό μίας πληρωμής από 100 σε 1000 ευρώ

ΔΙΑΘΕΣΙΜΟΤΗΤΑ

- **Δεδομένα ή υπηρεσίες είναι διαθέσιμα πάντα όταν πρέπει**
- Η διαθεσιμότητα μπορεί να πληγεί από ποικίλες αιτίες όπως φυσικές καταστροφές, διακοπή ρεύματος αλλά κυρίως από ηθελημένες επιθέσεις
- Συνήθως η διαθεσιμότητα παραβιάζεται μέσω επιθέσεων που προσπαθούν να εξαντλήσουν τους πόρους ενός συστήματος
- Παράδειγμα : Οι Denial of service επιθέσεις σε διάφορες on-line υπηρεσίες

ΑΝΙΧΝΕΥΣΙΜΟΤΗΤΑ

- **Όλες οι δραστηριότητες καταγράφονται και μπορούν στην συνέχεια να αποδοθούν στους υπευθύνους τους**
- Όταν όλα τα μέσα προστασίας αποτυγχάνουν και παραβιάζεται η ασφάλεια ενός συστήματος πρέπει τουλάχιστον να είναι δυνατή η ανίχνευση του υπευθύνου για το συμβάν
- Η διατήρηση αρχείων καταγραφής στο ίδιο το σύστημα δεν είναι συνήθως αρκετά ασφαλής για αυτό και επιλέγεται η διατήρηση τους σε ανεξάρτητη υποδομή
- Παράδειγμα : Ένας επιτιθέμενος πού αποκτά πρόσβαση σε ένα server στην συνέχεια σβήνει τα αρχεία καταγραφής

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

ΒΑΣΙΚΟΙ ΟΡΟΙ

Με τον όρο **κρυπτογραφία** εννοούμε τη μελέτη μαθηματικών τεχνικών που στοχεύουν στην εξασφάλιση θεμάτων που άπτονται της ασφάλειας μετάδοσης της πληροφορίας, όπως εμπιστευτικότητα, πιστοποίηση ταυτότητας του αποστολέα και διασφάλιση του αδιάβλητου της πληροφορίας.

- **Plaintext (απλό κείμενο):** Το αρχικό κομμάτι πληροφορίας
- **Ciphertext (κρυπτόγραμμα):** Το κρυπτογραφημένο μήνυμα
- **Encryption :** Η διαδικασία της κρυπτογράφησης ενός μηνύματος
- **Decryption :** Η διαδικασία αποκρυπτογράφησης του κρυπτογραφημένου μηνύματος

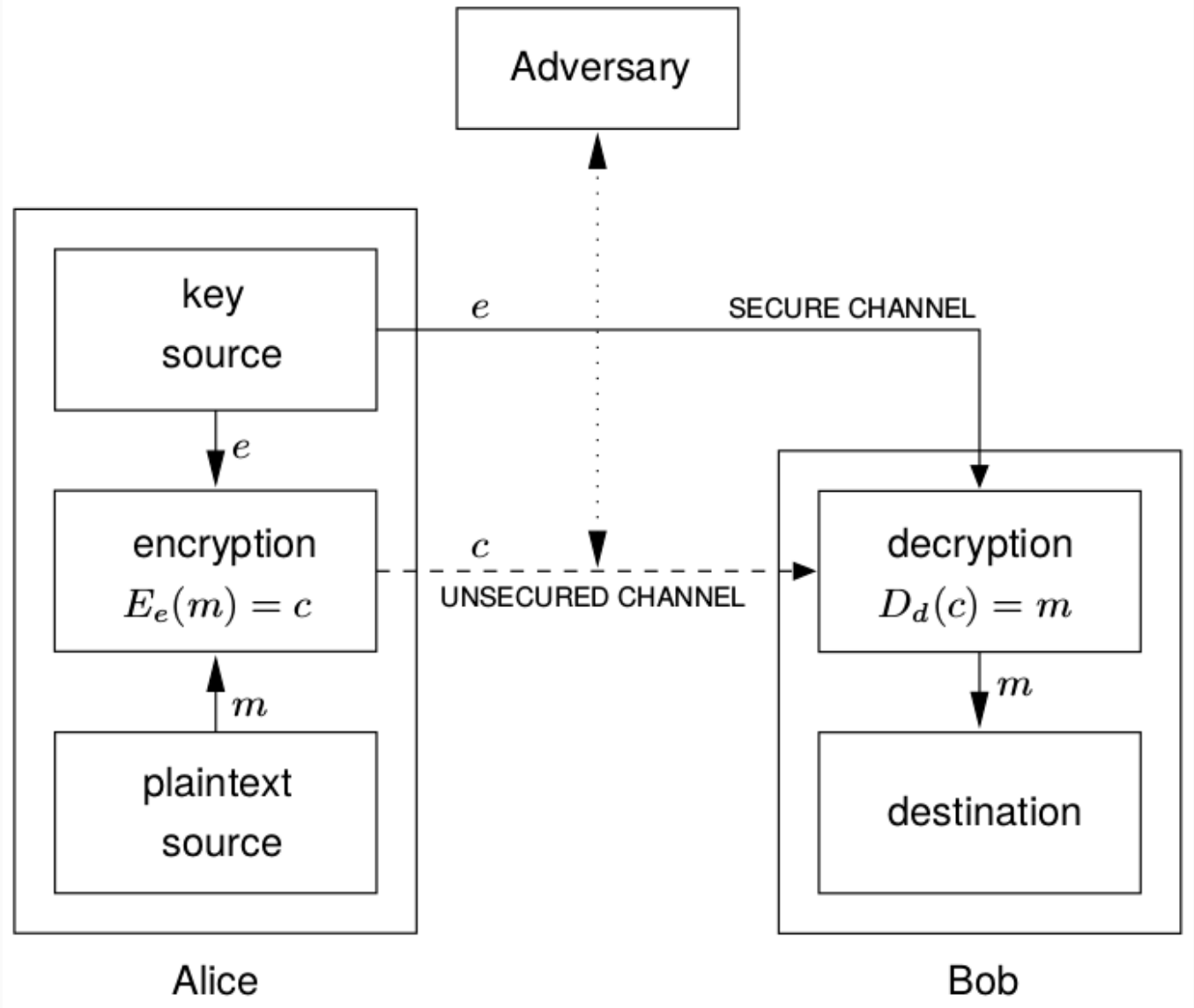
ΑΛΓΟΡΙΘΜΟΙ ΜΕ ΚΛΕΙΔΙΑ

- Αλγόριθμοι κρυπτογράφησης που χρησιμοποιούν ένα ή περισσότερα κλειδιά (keys)
- Η ασφάλεια έγκειται στο ότι **δεν είναι γνωστό το κλειδί**
- Οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης μπορούν να είναι ευρέως γνωστοί (αρχή του Kerchoff)
- **Κρυπτανάλυση** είναι η μελέτη μαθηματικών τεχνικών που στοχεύουν στην ακύρωση των κρυπτογραφικών μεθόδων, καθιστώντας τις έτσι μη κατάλληλες για κρυπτογραφικούς σκοπούς
- Ένας αλγόριθμος θεωρείται μη ασφαλής αν είναι δυνατή η ανάκτηση του **αρχικού μηνύματος** ή του **κλειδιού** από το **κρυπτόγραμμα**, ή αν είναι δυνατή η ανάκτηση του **κλειδιού** από **ζευγάρια plaintext - ciphertext**

ΚΑΤΗΓΟΡΙΕΣ ΑΛΓΟΡΙΘΜΩΝ

- **Αλγόριθμοι συμμετρικού (ή κρυφού) κλειδιού (symmetric key algorithms)** Χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση
- **Αλγόριθμοι ασύμμετρου (ή δημοσίου) κλειδιού (Asymmetric (or public key) algorithms)** Χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση

ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ



ΠΕΡΙΓΡΑΦΗ ΔΙΑΔΙΚΑΣΙΑΣ

- Το απλό κείμενο εισάγεται μαζί με το κλειδί στον αλγόριθμο κρυπτογράφησης
- Το αποτέλεσμα του αλγόριθμου κρυπτογράφησης είναι το κρυπτοκείμενο. Για δεδομένο απλό κείμενο, δύο διαφορετικά κλειδιά παράγουν δύο διαφορετικά κρυπτοκείμενα
- Ο αλγόριθμος αποκρυπτογράφησης δέχεται ως είσοδο το κρυπτοκείμενο και το κλειδί το οποίο είναι το ίδιο με αυτό του αλγόριθμου κρυπτογράφησης
- Ο αλγόριθμος αποκρυπτογράφησης εφαρμόζει τους αντίστροφους μετασχηματισμούς από αυτούς του αλγόριθμου κρυπτογράφησης και επαναφέρει το κείμενο στην αρχική του μορφή, αυτήν του απλού κειμένου

Απαίτηση για ασφαλές κανάλι επικοινωνίας

Ένα **ασφαλές κανάλι επικοινωνίας** πρέπει να υπάρχει για την επικοινωνία των δύο κόμβων, προκειμένου να ενημερώσει ο ένας τον άλλον για τον κλειδί. Η απαίτηση αυτή μπορεί υπό συγκεκριμένες συνθήκες να αποτελέσει ένα μεγάλο πρόβλημα για την επικοινωνία δύο κόμβων με συμμετρική κρυπτογράφηση.

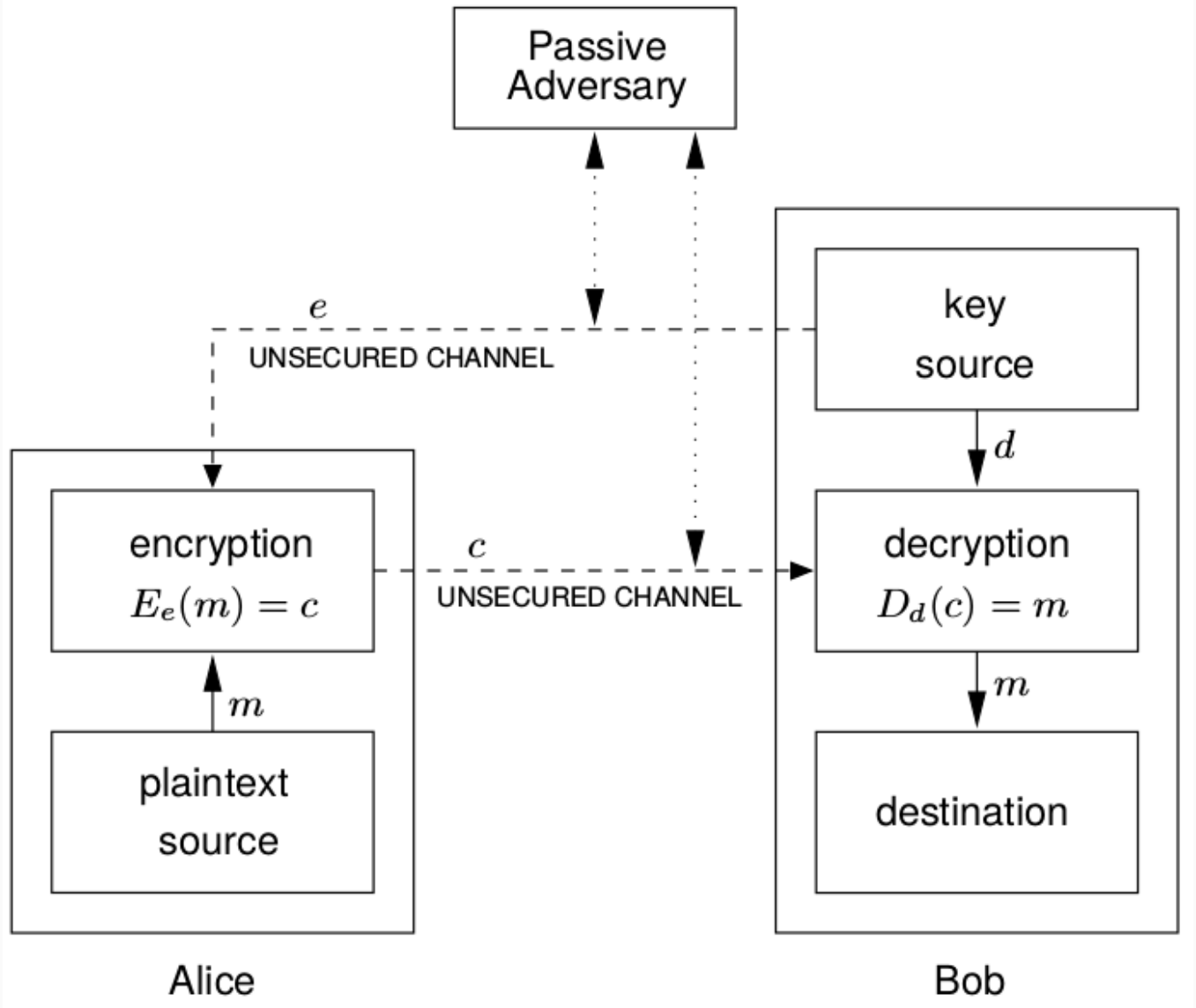
Το πρόβλημα του τετραγώνου

Εάν **n μέλη** επικοινωνούν μεταξύ τους με συμμετρική κρυπτογραφία συνολικά θα πρέπει να μοιραστούν **n(n-1)/2 κλειδιά**. Ο αριθμός αυτός είναι ανάλογος με το τετράγωνο του αριθμού των κόμβων, οπότε για μεγάλο αριθμό κόμβων η συμμετρική κρυπτογράφηση είναι ακατάλληλη λύση.

ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ

- Ένα κρυπτοσύστημα ονομάζεται ασύμμετρο, όταν χρησιμοποιούνται δύο διαφορετικά κλειδιά, το ένα για την κρυπτογράφηση και το άλλο για την αποκρυπτογράφηση
- **Τα κλειδιά δημιουργούνται στον παραλήπτη**, ο οποίος είναι ο μόνος που μπορεί να παράγει και να συσχετίσει ένα ζευγάρι ασύμμετρων κλειδιών
- Το κλειδί για την κρυπτογράφηση ονομάζεται **δημόσιο κλειδί** γιατί μπορεί να διατεθεί ελεύθερα χωρίς να απαιτείται ασφαλές κανάλι για τη μετάδοσή του
- Το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση είναι το **ιδιωτικό κλειδί** και παραμένει υπό την κατοχή του παραλήπτη

ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ



ΔΙΑΔΙΚΑΣΙΑ

- Η διαδικασία της ασύμμετρης κρυπτογράφησης έχει ως εξής :
  - Ο αποστολέας ζητάει από τον παραλήπτη το δημόσιο κλειδί K_e
  - Ο παραλήπτης στέλνει το δημόσιο κλειδί μέσω του μη ασφαλούς καναλιού επικοινωνίας
  - Ο αποστολέας κρυπτογραφεί το μήνυμα P με το δημόσιο κλειδί του παραλήπτη και στέλνει το κρυπτοκείμενο στον παραλήπτη C
  - Ο παραλήπτης αποκρυπτογραφεί το κρυπτοκείμενο χρησιμοποιώντας το ιδιωτικό κλειδί K_d
- Τα δημόσιο κλειδιά των κόμβων επικοινωνίας μπορεί να είναι δημοσιευμένα εξ αρχής οπότε σε αυτή την περίπτωση δεν χρειάζονται τα δύο πρώτα βήματα
- Στην ασύμμετρη κρυπτογράφηση δεν χρειάζεται ασφαλές κανάλι επικοινωνίας
- Ο αριθμός των κλειδιών που απαιτούνται για επικοινωνίας n κόμβων είναι 2n

ΑΛΓΟΡΙΘΜΟΣ RSA

ΑΛΓΟΡΙΘΜΟΣ RSA

- Ανακλύφθηκε το 1977 από τους Rivest, Shamir, Adleman
- Η ασφάλειά του βασίζεται στο δύσκολο πρόβλημα της παραγοντοποίησης ενός σύνθετου ακεραίου σε γινόμενο πρώτων παραγόντων

ΛΕΙΤΟΥΡΓΙΑ RSA

1. Ο χρήστης διαλέγει δύο πολύ μεγάλους πρώτους αριθμούς p, q
2. Υπολογίζει το γινόμενό τους $N = p * q$
3. Υπολογίζει την συνάρτηση Euler $\Phi(N) = (p-1)(q-1)$
4. Διαλέγει ένα τυχαίο αριθμό e με $e < \Phi(N)$ και $\gcd(e, \Phi(N)) = 1$. Ο αριθμός e δημοσιοποιείται.
5. Με τον αλγόριθμο του Ευκλείδη ο χρήστης υπολογίζει μοναδικό ακέραιο d ώστε $1 < d < \Phi(N)$ και $e * d \bmod(\Phi(N)) = 1$ (ο d είναι ο αντίστροφος του e ως προς $\bmod(\Phi(N))$)
6. Το δημόσιο κλειδί είναι το (N, e) και
7. Το ιδιωτικό είναι το (N, d)

Η κρυπτογράφηση γίνεται με την σχέση $c = m^e \bmod N$

Η αποκρυπτογράφηση γίνεται με την σχέση $m = c^d \bmod N$

- Ο αποστολέας πρέπει να κάνει τα εξής:
  1. Παραλαμβλανει το σημόσιο κλειδί του παραλήπτη (N, e)
  2. Εκφράζει το μύνημα που θα στείλει με έναν αριθμό στο διάστημα $[0, n - 1]$
  3. Υπολογίζει το κρυπτόγραμμα με την σχέση $c = m^e \mod N$
  4. Στέλνει το κρυπτογραμμα στον παραλήπτη
- Ο παραλήπτης παραλαμβάνει το κρυπτοκείμενο και το αποκρυπτογραφεί με το ιδιωτικό του κλειδί (N, d), με την σχέση $m = c^d \mod N$

ΠΑΡΑΔΕΙΓΜΑ RSA

- Ο χρήστης επιλέγει δύο τυχαίους πρώτους αριθμούς $p = 3, q = 11$
- Υπολογίζει $N = p * q = 33$
- Υπολογίζει $\Phi(N) = (p - 1)(q - 1) = 20$
- Επιλέγει αριθμό e που να μην έχει κοινούς διαιρέτες με το $\Phi(N), e = 7$
- Με τον αλγόριθμο του Ευκλείδη $d = 3$
- Η κρυπτογράφηση γίνεται με την σχέση $c = m^7 mod 33$
- Η αποκρυπτογράφηση γίνεται με την σχέση $m = c^3 mod 33$

ΑΛΓΟΡΙΘΜΟΣ PAILLIER

ΑΛΓΟΡΙΘΜΟΣ PAILLIER

- Το κρυπτοσύστημα Paillier δημιουργήθηκε το 1999
- Σχεδιάστηκε από τον Γάλλο ερευνητή Pascal Paillier
- Είναι ένας αλγόριθμος δημοσίου κλειδιού
- Αναλύονται :
    - η δημιουργία των κλειδιών
    - η πράξη της κρυπτογράφησης
    - και η πράξη της αποκρυπτογράφησης

ΔΗΜΙΟΥΡΓΙΑ ΚΛΕΙΔΙΩΝ

- Επιλέγονται δύο μεγάλοι τυχαίοι πρώτοι αριθμοί p,q
- Υπολογίζεται το γινόμενο τους $n = p * q$
- Επιλέγεται ένας ακέραιο αριθμό $g \in Z^*_{n^2}$ (δηλαδή, ο g αντιστρέφεται ως προς modulo n^2)
- τέτοιος ώστε το n και το $L(g^{\lambda} mod n^2)$ είναι σχετικώς πρώτοι :

$$gcd(n, L(g^{\lambda} mod n^2)) = 1 \tag{1}$$

- Το L αναπαριστά την συνάρτηση $L : Z_{n^2} \to Z_n$:

$$u \to \frac{u-1}{n} \tag{2}$$

- Το λ αναπαριστά την συνάρτηση Carmichael

$$\lambda(p * q) = lcm(p-1, q-1) \tag{3}$$

- lcm = ελάχιστο κοινό πολλαπλάσιο
- Δημόσιο κλειδί : **(n,g)**
- Ιδιωτικό κλειδί : **(p,q)**

- Κατά την διαδικασία της κρυπτογράφησης του **απλού κειμένου** $m \in Z_n$ επιλέγεται ένας **τυχαίος ακέραιος** $r \in Z_n^*$
- Με την χρήση του **τυχαίου** r ο αλγόριθμος αποκτά μία ιδιότητα που λέγεται **probabilistic encryption**, και πρακτικά για το ίδιο απλό κείμενο, δύο κρυπτογραφήσεις παράγουν διαφορετικά κρυπτοκείμενα
- Το αποτέλεσμα είναι το **κρυπτοκείμενο** $c \in Z_n^2$ που υπολογίζεται από την σχέση :

$$c = g^m * r^n mod n^2 \tag{4}$$

ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ

- Κατά την διαδικασία της αποκρυπτογράφησης του **κρυπτοκειμένου c** χρησιμοποιείται το **ιδιωτικό κλειδί** του αλγόριθμου **(p,q)**
- Υπολογίζεται από την σχέση :

$$m = \frac{L(c^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \tag{5}$$

ΑΠΛΟΠΟΙΗΜΕΝΗ ΕΚΔΟΧΗ

- g=n+1
- $\lambda = \Phi(N)$
- $\mu = \Phi(N)^{-1} \mathrm{mod} n$
- Κρυπτογράφηση $c = g^m * r^n \mathrm{mod} n^2$
- Αποκρυπτογράφηση $= L(c^{\lambda} \mathrm{mod} n^2)\mu \mathrm{mod} n$