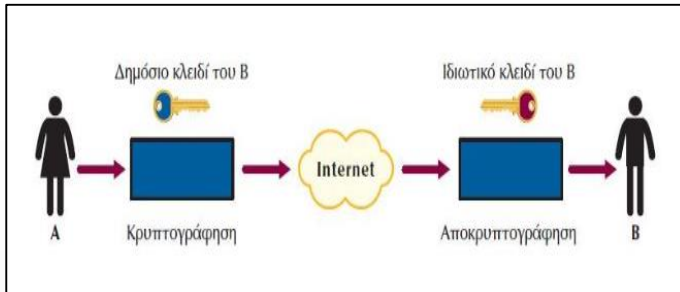


- › **Κρυπτογράφηση**
- › **Ανωνυμοποίηση**
- › **Ψευδωνυμοποίηση**

Τετάρτη 20 Ιουνίου, 2018

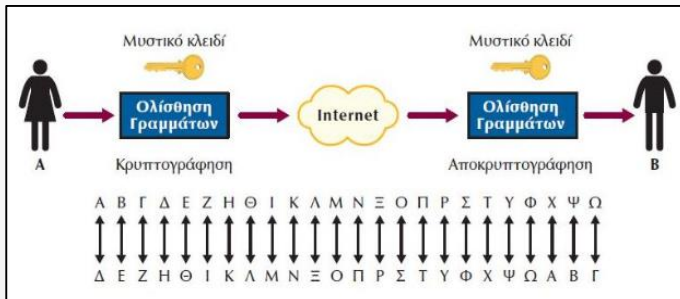


- **Τι είναι:** Κρυπτογράφηση είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να διαβαστεί χωρίς τη γνώση της σωστής ακολουθίας bit. Η ακολουθία bit καλείται "κλειδί" και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο / συνάρτηση. Η αντίστροφη διαδικασία είναι η αποκρυπτογράφηση και απαιτεί γνώση του κλειδιού.
- **Διασφαλίζει την:** Εμπιστευτικότητα, Ακεραιότητα, Πιστοποίηση Ταυτότητας, Πιστοποίηση Μηνύματος, Μη απάρνηση



## Ασύμμετρα (Public Key Cryptography): Χρήση Ζεύγους Κλειδιών

- Η υπολογιστική ισχύς που απαιτείται για κρυπτογραφία δημόσιου κλειδιού είναι πολύ μεγαλύτερη
- Μικρότερη ταχύτητα



## Συμμετρική (Symmetric Cryptography): Χρήση Κοινού Κλειδιού

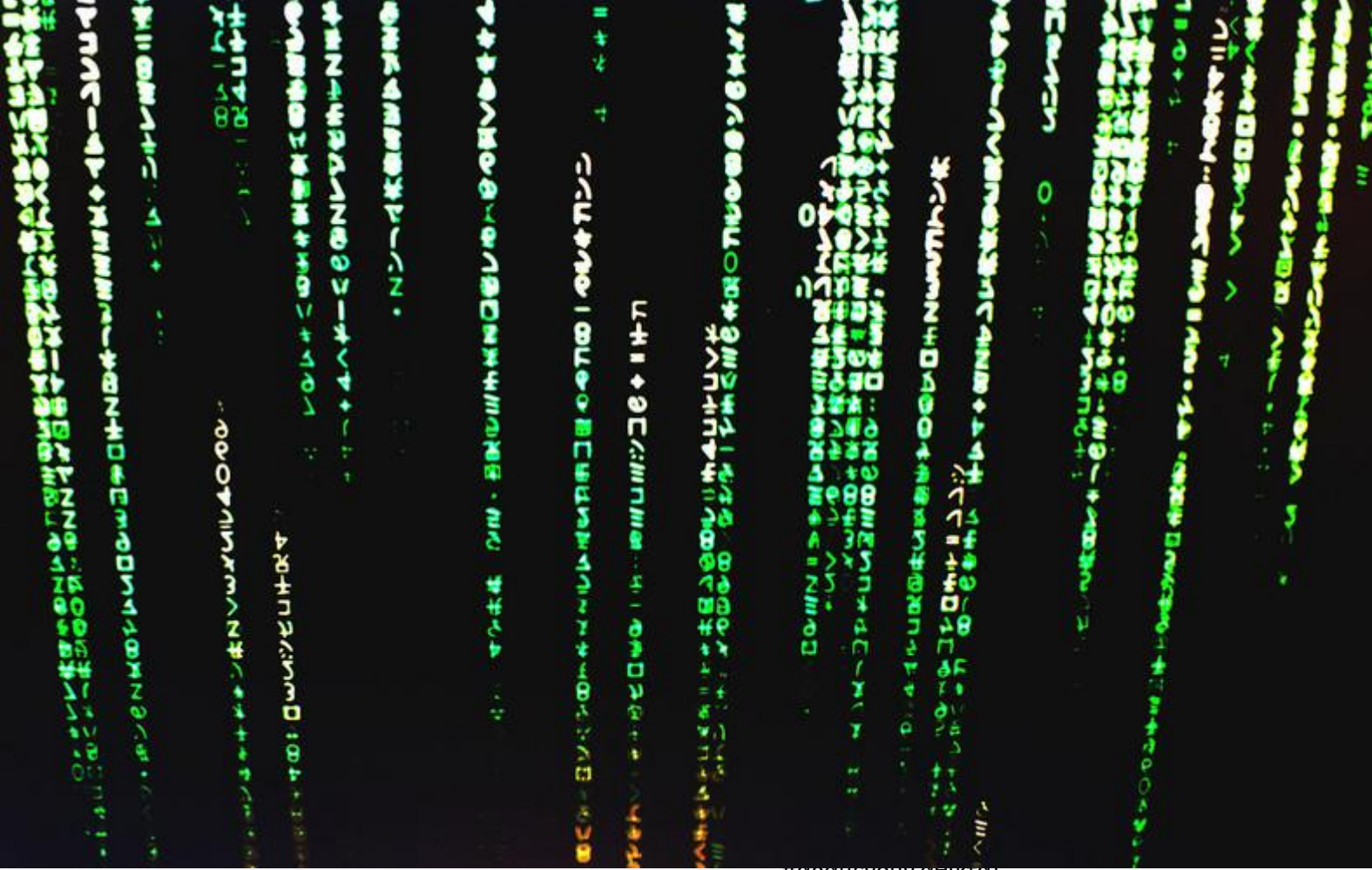
- Αποδοτική όσον αφορά τους πόρους που απαιτούνται
- Σημαντικά ταχύτερη μέθοδος
- Προϋποθέτει ότι το κλειδί είτε έχει ανταλλαχθεί μέσω ενός ασφαλούς διαύλου επικοινωνίας είτε μέσα από τη φυσική παρουσία των προσώπων

## Διεθνής Χρήση:

- Ασφάλεια συναλλαγών σε τράπεζες
- Κινητή και σταθερή τηλεφωνία
- Στρατιωτικά δίκτυα
- Ηλεκτρονικές επιχειρήσεις(ηλεκτρονικό εμπόριο)
- Διαδίκτυο
- Έξυπνες κάρτες
- VPN-ιδιωτικά δίκτυα
- Ασύρματα δίκτυα
- Τηλεδιασκέψεις
- Συναγερμοί κτλ.

## Χρήση εντός Interamerican:

- Εταιρικά laptop (hard disks)
- Εταιρικές κινητές συσκευές υπαλλήλων (σε εξέλιξη τα κινητά των διαμεσολαβητών)
- Καθημερινή κρυπτογράφηση δεδομένων backup
- Αποστολή συγκεκριμένων email μέσω Secure Email (McAfee) ανάλογα με την έγκριση/απόφαση των αιτημάτων από τον Data Traffic Controller
- Σε εξέλιξη η υλοποίηση Secure Email από συγκεκριμένα τμήματα που αποστέλλουν καθημερινά email με πολλά προσωπικά δεδομένα (xls, pdfs etc).
- Πραγματοποιήθηκαν εκτενείς έλεγχοι απόδοσης (performance tests) κρυπτογράφησης παραγωγικών βάσεων, ωστόσο η αποδοτικότητα ήταν μειωμένη σε σχέση με το αναμενόμενο.



παραμένουν ασκικά).

# TERAMERICAN

ό πρόσωπο, προκειμένου

ρούσαν με  
ωπο.

ές, όπως η  
σκοπό την  
τικών κλπ

απόκρυψης  
δομένου ότι

ης)  
όν με μη  
"), ωστόσο  
ληθούν από  
μερομηνίες

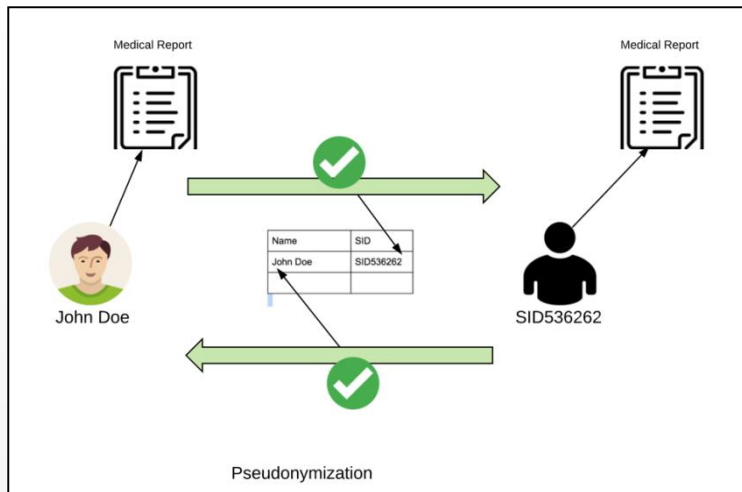
## Διεθνής Χρήση:

- Για χρήση δεδομένων για ιστορικούς, επιστημονικούς και στατιστικούς σκοπούς
- Από εξειδικευμένους στον τομέα marketing
- Επιχειρήσεις που επεξεργάζονται προσωπικά/ευαίσθητα δεδομένα

## Χρήση εντός INTERAMERICAN:

- Δεν γίνεται χρήση

- **Τι είναι:** Ως ψευδωνυμοποίηση ορίζεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα.
- **Διασφαλίζει την:** Εμπιστευτικότητα, μη ταυτοποίηση



## Data Masking

Μια τεχνική κάλυψης η οποία επιτρέπει να καλυφθεί ένα μέρος των δεδομένων με τυχαίους χαρακτήρες ή άλλα δεδομένα.

Παράδειγμα: 5500 000 000 0004 → xxxx xxx xxxx 0004

## Κρυπτογράφηση

Καθιστά τα αρχικά δεδομένα ακατάληπτα και η διαδικασία δε μπορεί να αντιστραφεί εάν δεν υπάρχει πρόσβαση στα κλειδιά.

## Ανακάτεμα (Scrambling)

Ανάμειξη γραμμάτων. Μπορεί να είναι μη αντιστρέψιμη. Παράδειγμα: Προστασία → Σραπιστοα

## Tokenization

Γίνεται αντικατάσταση των ευαίσθητων/προσωπικών δεδομένων με μη-ευαίσθητα/προσωπικά τα οποία λέγονται "tokens". Τα tokens δεν έχουν καμία ιδιαίτερη ή εκμεταλλεύσιμη αξία. Η διαδικασία αυτή δεν τροποποιεί τον τύπο και το μήκος δεδομένων.

## Θόλωση (Blurring)

Η διαδικασία αυτή χρησιμοποιεί προσεγγιστικές τιμές των δεδομένων ώστε να καταστήσει αδύνατη την ταυτοποίηση του προσώπου.

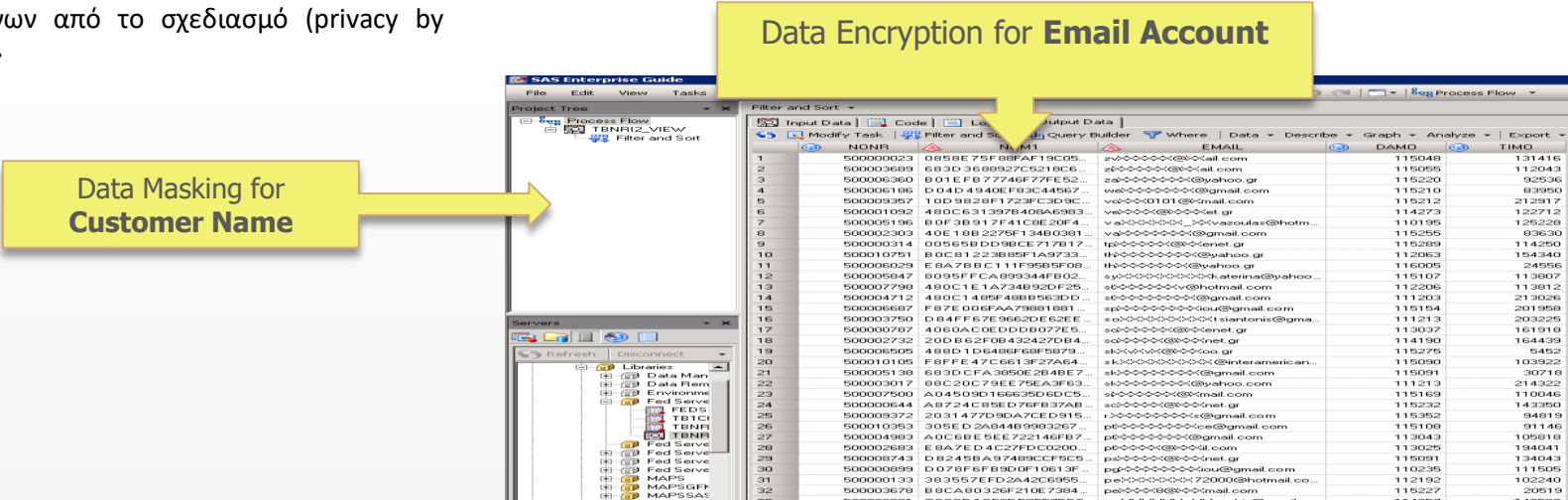
Παράδειγμα: θόλωση προσώπου σε φωτογραφία.

## Διεθνής Χρήση:

- Για χρήση δεδομένων για ιστορικούς, επιστημονικούς και στατιστικούς σκοπούς
- Βασικό χαρακτηριστικό της «προστασίας δεδομένων από το σχεδιασμό (privacy by design)»

## Χρήση εντός Interamerican:

**Data Masking:** υλοποίηση σε όλο το μη παραγωγικό περιβάλλον με σκοπό τη βέλτιστη προσέγγιση test αποτελεσμάτων χωρίς τη χρήση δεδομένων ταυτοποίησης.



The screenshot shows the SAS Enterprise Guide interface. A yellow callout box labeled "Data Masking for Customer Name" points to the first column of a data table, where customer names have been replaced with alphanumeric strings. Another yellow callout box labeled "Data Encryption for Email Account" points to the second column, where email addresses have been replaced with alphanumeric strings. The data table has columns for ID, NAME, EMAIL, and TIMO. The data is as follows:

ID	NAME	EMAIL	TIMO
1	500000023	0858E75F8BFA13C05...	115048
2	500003689	6B3D3688927C5218C6...	115056
3	500006360	B01E7F7746F77FE52...	115220
4	500006186	D04D4940EF93C44567...	115210
5	500009357	10D982BF1723FC3D9C...	115212
6	500001092	480CE31397B406A8393...	114273
7	500005196	B0F3B917F41C8E20F4...	110196
8	500002303	40E1982275F134B0381...	115255
9	500000314	00565BDD98CE717B17...	115289
10	500010761	B0C81223B88F1A3733...	112063
11	500006029	E8A7B8C111F958F08...	115205
12	500009847	8095FFCA993044B02...	115107
13	500007788	480C1E1A794B92DF28...	112306
14	500004712	480C1485F48B8563DD...	111203
15	500006687	F67E006FAA79881881...	115154
16	500003760	D84FF67E36620E62EE...	203226
17	500000767	4060AC0EDDD8077E5...	113037
18	500002732	20DB62F08432427DB4...	114190
19	500006006	488D1D448E68F8579...	115276
20	500010106	F8FFE47C6613F27A64...	115090
21	500005138	6B3DCFA3850E284BE7...	115091
22	500003017	69C20C791EE75EA3F63...	111213
23	500007600	A04509D166635D6DC5...	115169
24	500006644	A8724C85ED76FB37A8...	115232
25	500009372	2031477D90A76E915...	115362
26	500010353	305ED2A844B9983267...	115108
27	500004983	40C6BE5EE722146FB7...	113043
28	500002683	E9A7E44227DC0200...	113025
29	500008743	B245BA97485CCF5C5...	115091
30	500000899	D078F5FB9D0F10613F...	110235
31	500000133	363557ED2A420595...	112192
32	500003678	B8CA88328F210E7884...	115227