Ασφάλεια Υπολογιστικών Συστημάτων

7ο Εξάμηνο

Ασφάλεια Ηλεκτρονικού Ταχυδρομείου

Διδάσκων : Δρ. Παρασκευάς Κίτσος, Καθηγητής
https://ecsalab.ece.uop.gr/

Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών (ECSA Lab.)
e-mail: kitsos@go.uop.gr

ΔΙΑΡΘΡΩΣΗ ΕΝΟΤΗΤΑΣ

1. Pretty Good Privacy (PGP) and OpenPGP
2. S/MIME
3. Kerberos

PRETTY GOOD PRIVACY

- Το παρέχει την υπηρεσία εξασφάλισης απορρήτου και πιστοποίησης αυθεντικότητας
- Χρησιμοποιείται σε εφαρμογές ηλεκτρονικού ταχυδρομείου και αποθήκευσης αρχείων

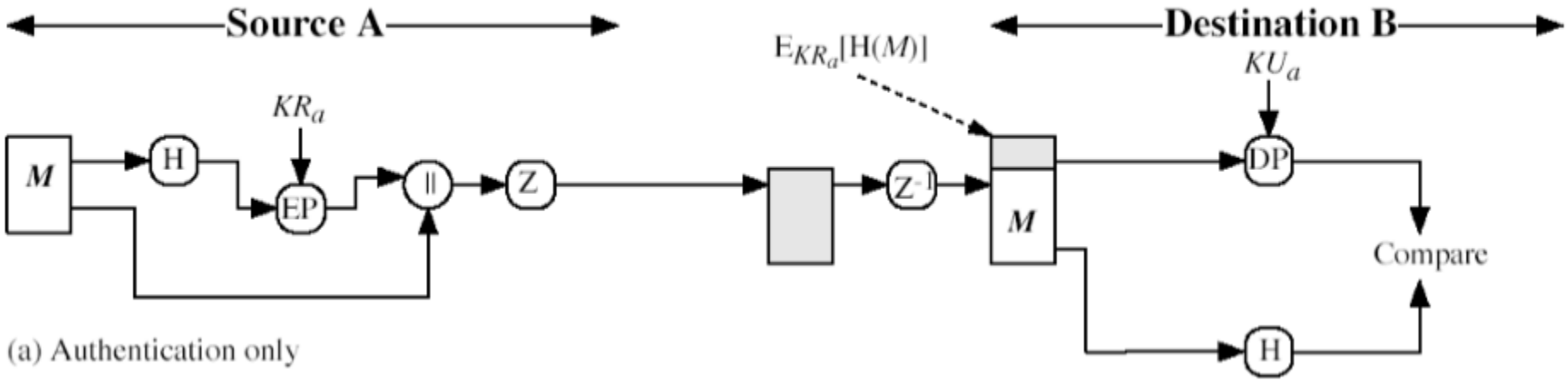
ΟΙ ΛΟΓΟΙ ΑΠΟΔΟΧΗΣ ΤΟΥ PGP

- Διατίθεται δωρεάν σε διάφορες εκδόσεις που λειτουργούν σε ποικιλία από πλατφόρμες (Win, Unix, Mac κλπ)
- Βασίζονταν σε αλγορίθμους που έχουν επιβιώσει μετά από ανάλυση και είναι σχετικά αξιόπιστοι
  - RSA, DSS, Diffie-Hellman: Κρυπτογράφηση δημοσίου κλειδιού
  - CAST-128, IDEA, 3DES: Κρυπτογράφηση ιδιωτικού κλειδιού
  - SHA-1: Κωδικοποίηση συνάρτησης κατακερματισμού
- Ευρύ πεδίο εφαρμογών (κρυπτογράφηση αρχείων και μηνυμάτων, επικοινωνία μέσω διαδικτύου)
- Δεν αναπτύχθηκε ούτε ελέγχεται από κάποιο κυβερνητικό φορέα ή οργανισμό προτύπων

ΠΕΡΙΓΡΑΦΗ ΛΕΙΤΟΥΡΓΙΑΣ

- Αποτελείται από πέντε λειτουργίες
  - Πιστοποίηση (Authentication)
  - Εμπιστευτικότητα (Confidentiality)
  - Συμπίεση (Compression)
  - Συμβατότητα με ηλεκτρονικό ταχυδρομείο (E-mail compatibility)
  - Κατάτμηση (Segmentation)

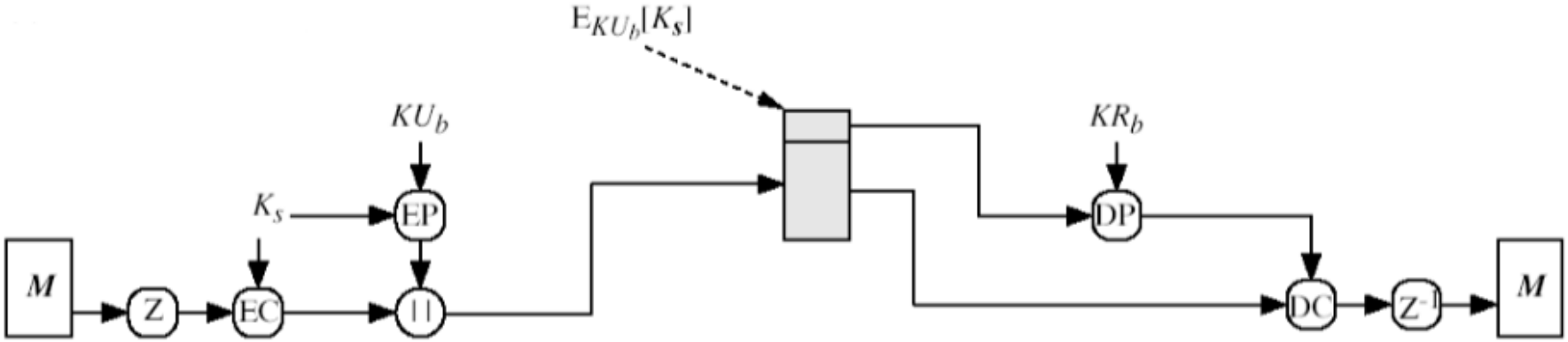
ΠΙΣΤΟΠΟΙΗΣΗ



(a) Authentication only

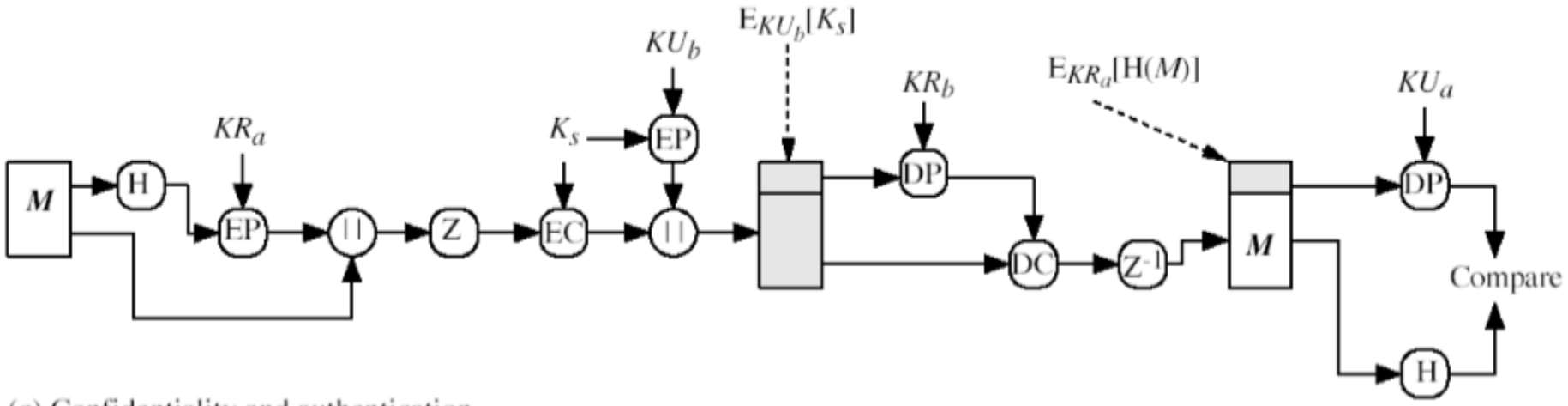
M - message
H – hash function
EP – public key encryption
|| - concatenation
Z - compression using ZIP algorithm
KR_a – private key of user A
KU_a – public key of user A

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ



M - message
Z - compression using ZIP algorithm
EC / DC – classical (secret-key) encryption / decryption
EP / DP – public key encryption / decryption
|| - concatenation
K_s - session key
KR_b – private key of user B
KU_b – public key of user B

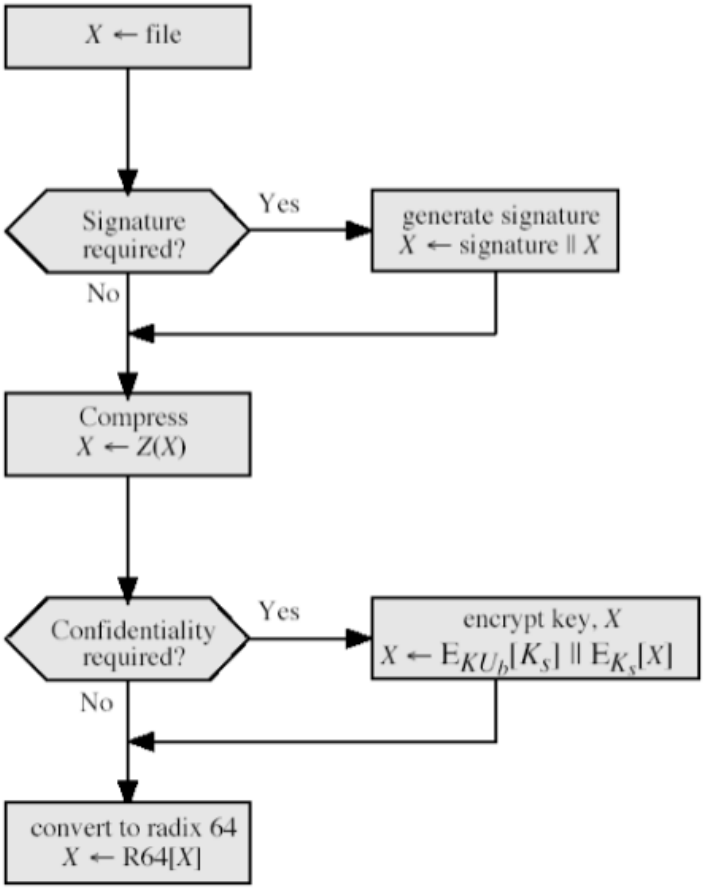
ΠΙΣΤΟΠΟΙΗΣΗ και ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

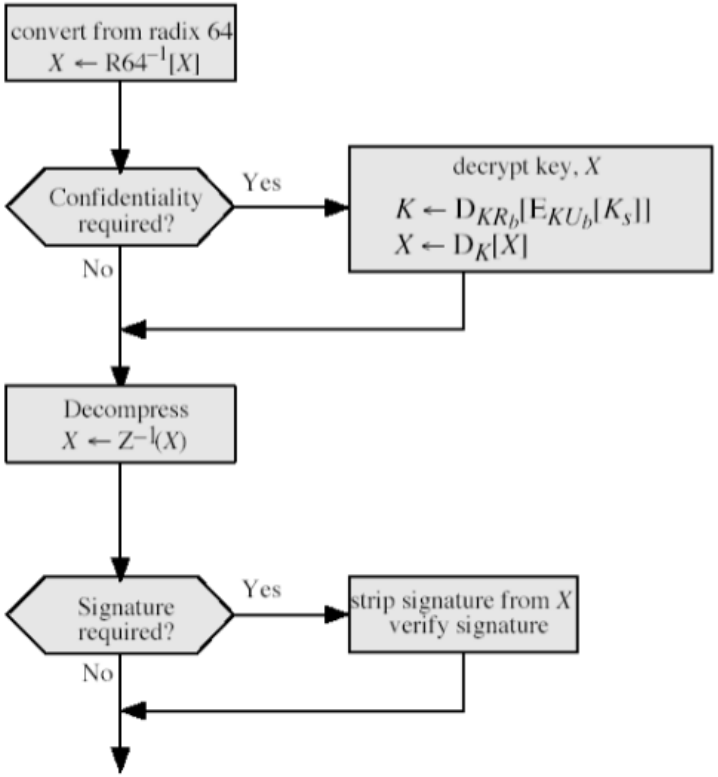


(c) Confidentiality and authentication

M - message
H – hash function
Z - compression using ZIP algorithm
EP / DP – public key encryption / decryption
|| - concatenation
EC / DC – classical (secret-key) encryption / decryption
K_s - session key
KR_a / KR_b – private key of user A / B
KU_a / KU_b – public key of user A / B

ΑΠΟΣΤΟΛΗ – ΛΗΨΗ ΜΥΝΗΜΑΤΩΝ PGP

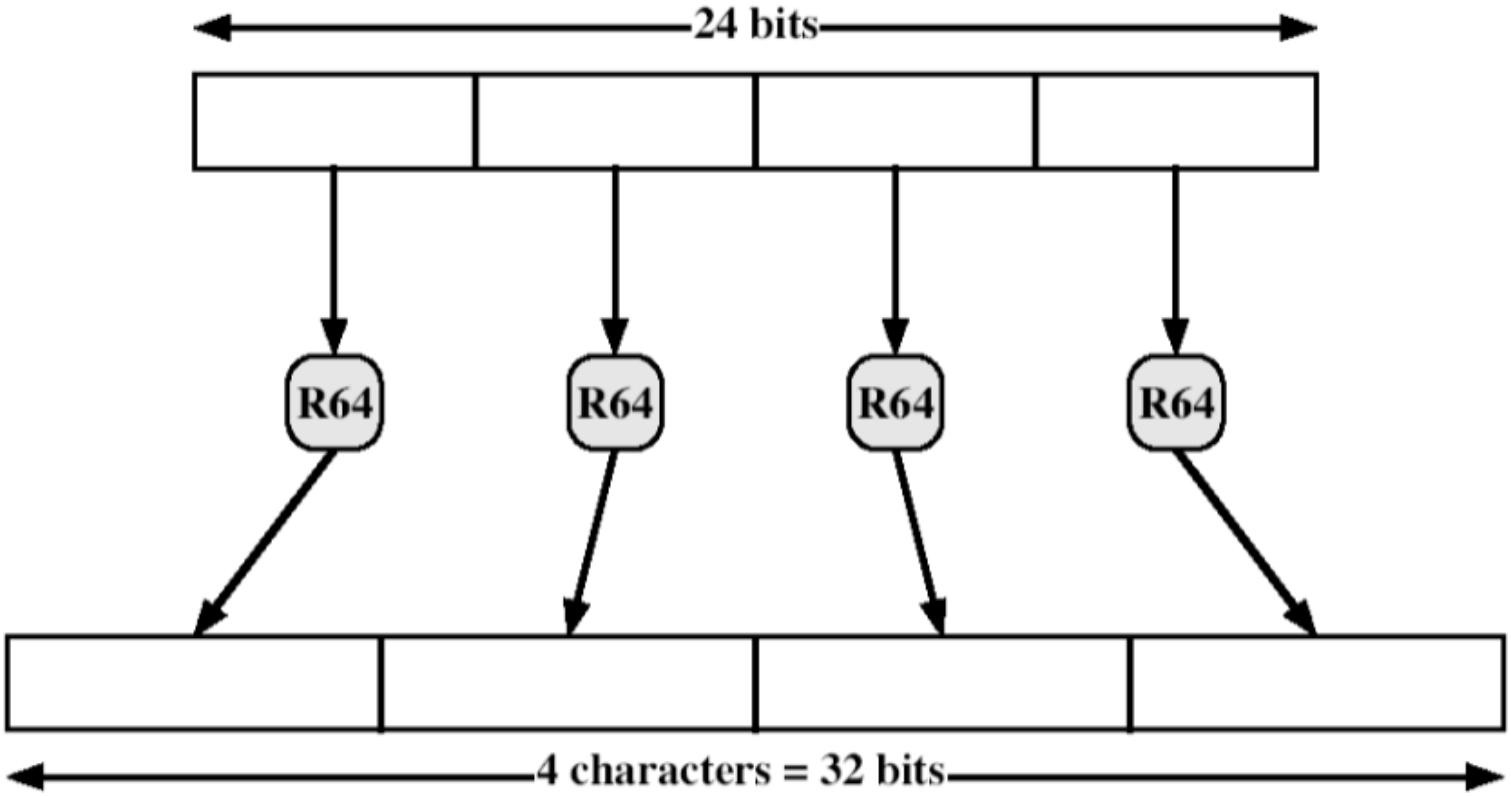




ΣΥΜΠΙΕΣΗ

- Το PGP συμπιέζει το μήνυμα μετά τη ψηφιακή υπογραφή αλλά πριν τη κρυπτογράφηση
- Η θέση της συνάρτησης συμπίεσης είναι υψήστης σημασίας
- Ο αλγόριθμος συμπίεσης είναι ο ZIP

RADIX-64



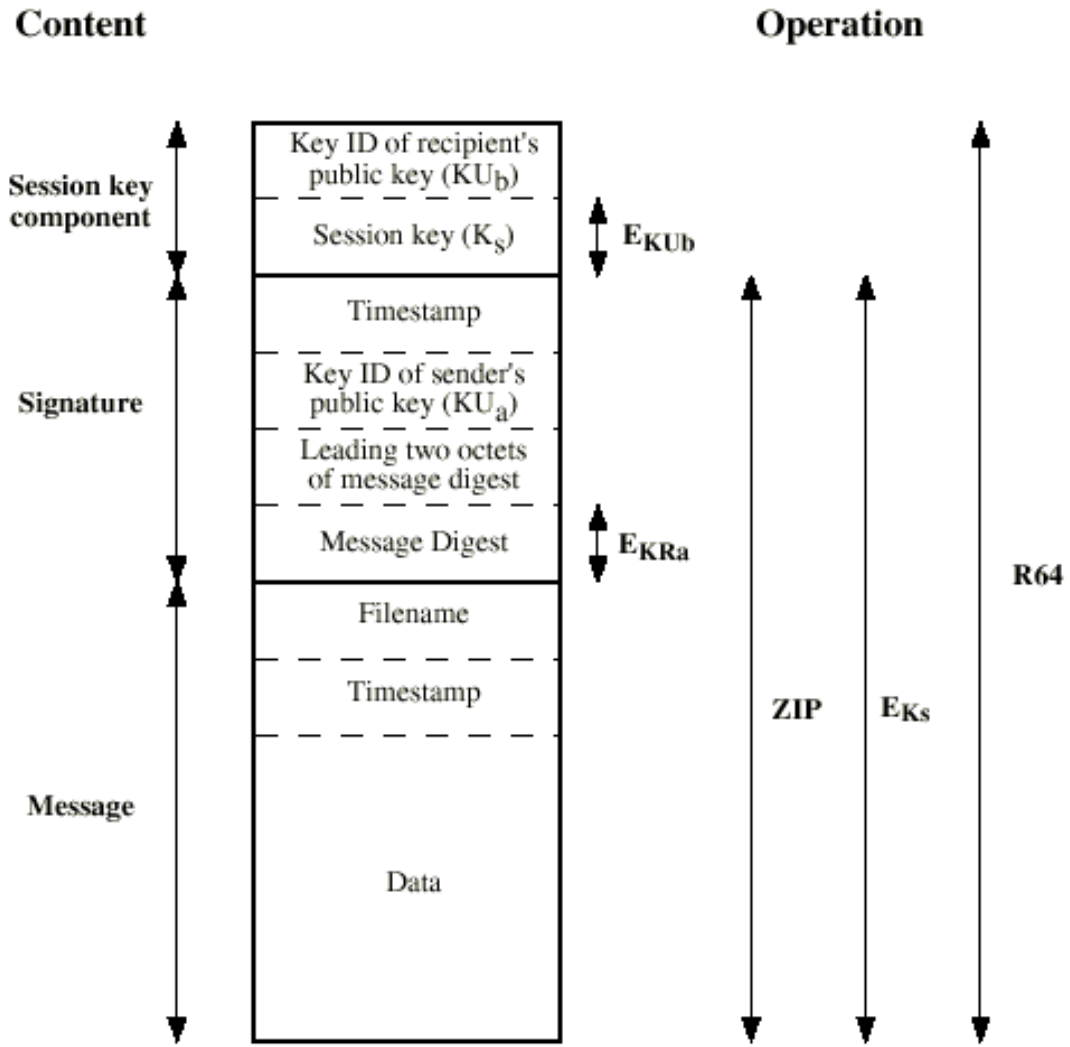
ΚΩΔΙΚΟΠΟΙΗΣΗ RADIX-64

6-bit value	character encoding	6-bit value	character encoding	6-bit value	character encoding	6-bit value	character encoding
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(pad)	=

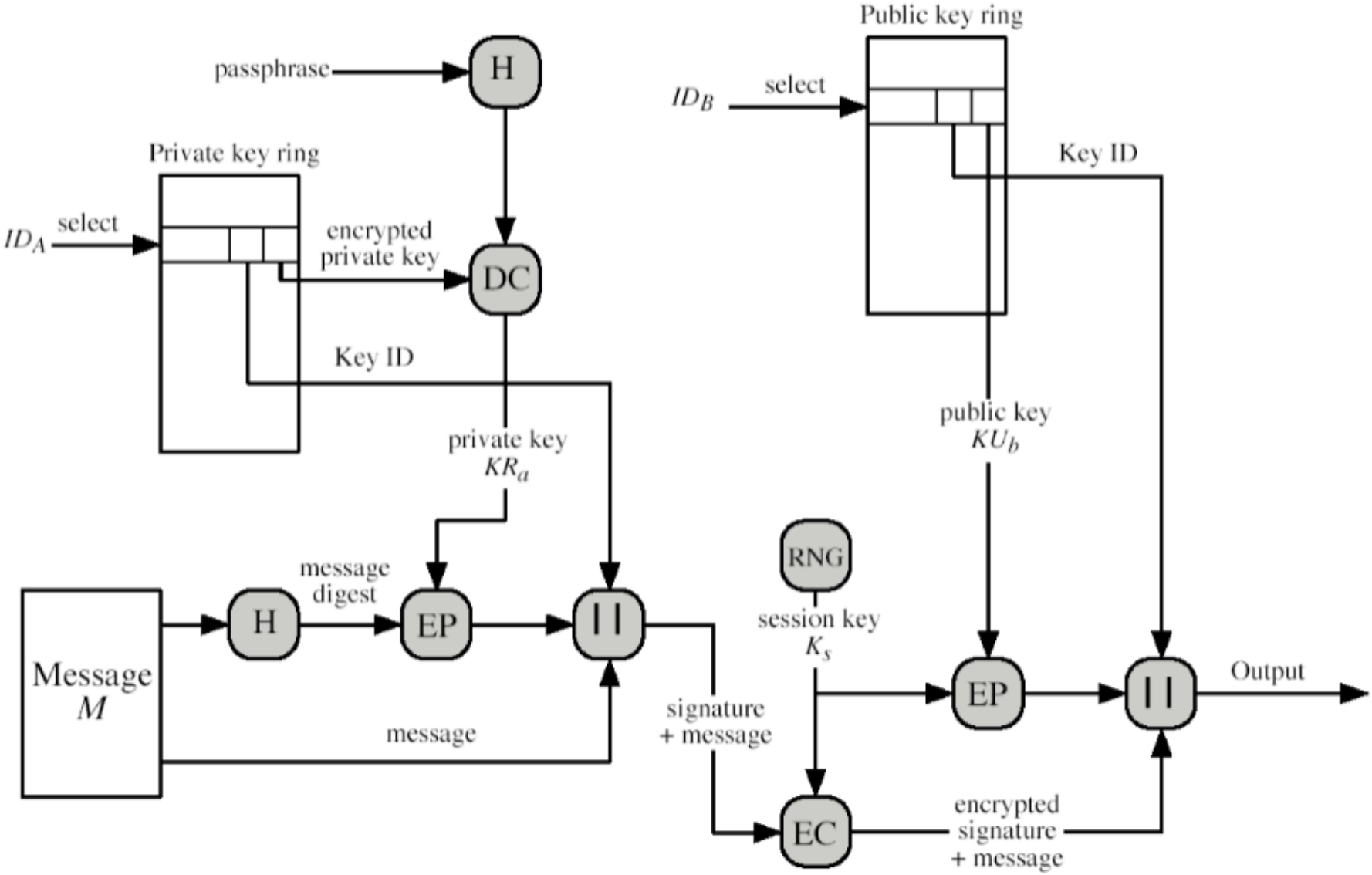
ΚΑΤΑΤΜΗΣΗ ΚΑΙ ΣΥΝΑΡΜΟΛΟΓΗΣΗ

- Συνήθως αναφέρεται σε μηνύματα μήκους έως 50,000 bytes
- Μεγαλύτερα μηνύματα πρέπει να τμηματοποιηθούν σε μικρότερα τεμάχια
- Το PGP τμηματοποιεί αυτόματα ένα μήνυμα που είναι μεγάλο
- Ο δέκτης αφαιρεί όλες τις επικεφαλίδες του e-mail και συναρμολογεί το μήνυμα με σκοπό να το λάβει στην αρχική του μορφή

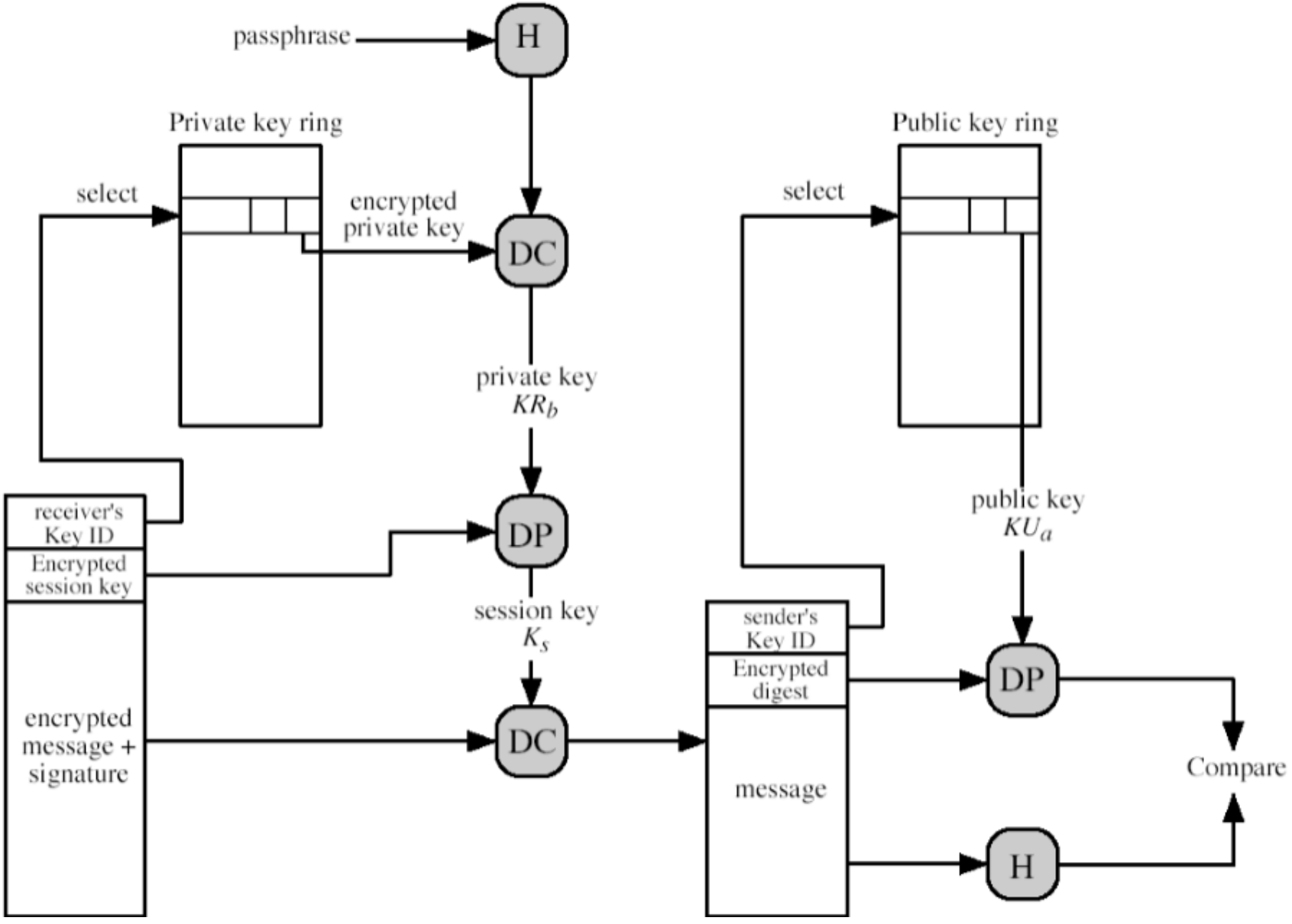
FORMAT ΤΟΥ PGP ΜΗΝΥΜΑΤΟΣ



ΔΗΜΙΟΥΡΓΙΑ PGP ΜΗΝΥΜΑΤΟΣ



ΛΗΨΗ PGP ΜΗΝΥΜΑΤΟΣ



OPENPGP

- Είναι ανοιχτό πρότυπο (RFC 4880) που ορίζεται από την Internet Engineering Task Force (IETF)

ΑΛΓΟΡΙΘΜΟΙ ΣΤΟ OPENPGP

Ciphers – Encryption Algorithms	Message Authentication Code (MAC) – Hashing algorithms
• AES256 • AES192 • AES128 • Twofish • 3-DES • CAST 5 • IDEA	• SHA512 • SHA384 • SHA256 • MD5 • SHA1 • RIPEMD-160

S/MIME

MIME

- Επέκταση της παλαιάς προδιαγραφής RFC 822 η οποία αφορά τη μορφή του ταχυδρομείου Διαδικτύου
  - Η ορίζει μια απλή κεφαλίδα με τα πεδία Το (Προς), From (Από), Subject (Θέμα)
  - Υποθέτει ότι χρησιμοποιείται μορφή κειμένου ASCII
- Παρέχει αρκετά νέα πεδία κεφαλίδας που ορίζουν πληροφορίες για το σώμα του μηνύματος

S/MIME

- Ασφαλείς Γενικές Επεκτάσεις Ταχυδρομείου Διαδικτύου
- Βελτίωση ως προς την ασφάλεια της μορφής MIME για το ηλεκτρονικό ταχυδρομείο Διαδικτύου
  - Βασίζεται σε τεχνολογία της εταιρείας RSA Data Security
- Παρέχει τη δυνατότητα υπογραφής ή/και κρυπτογράφησης μηνυμάτων e-mail

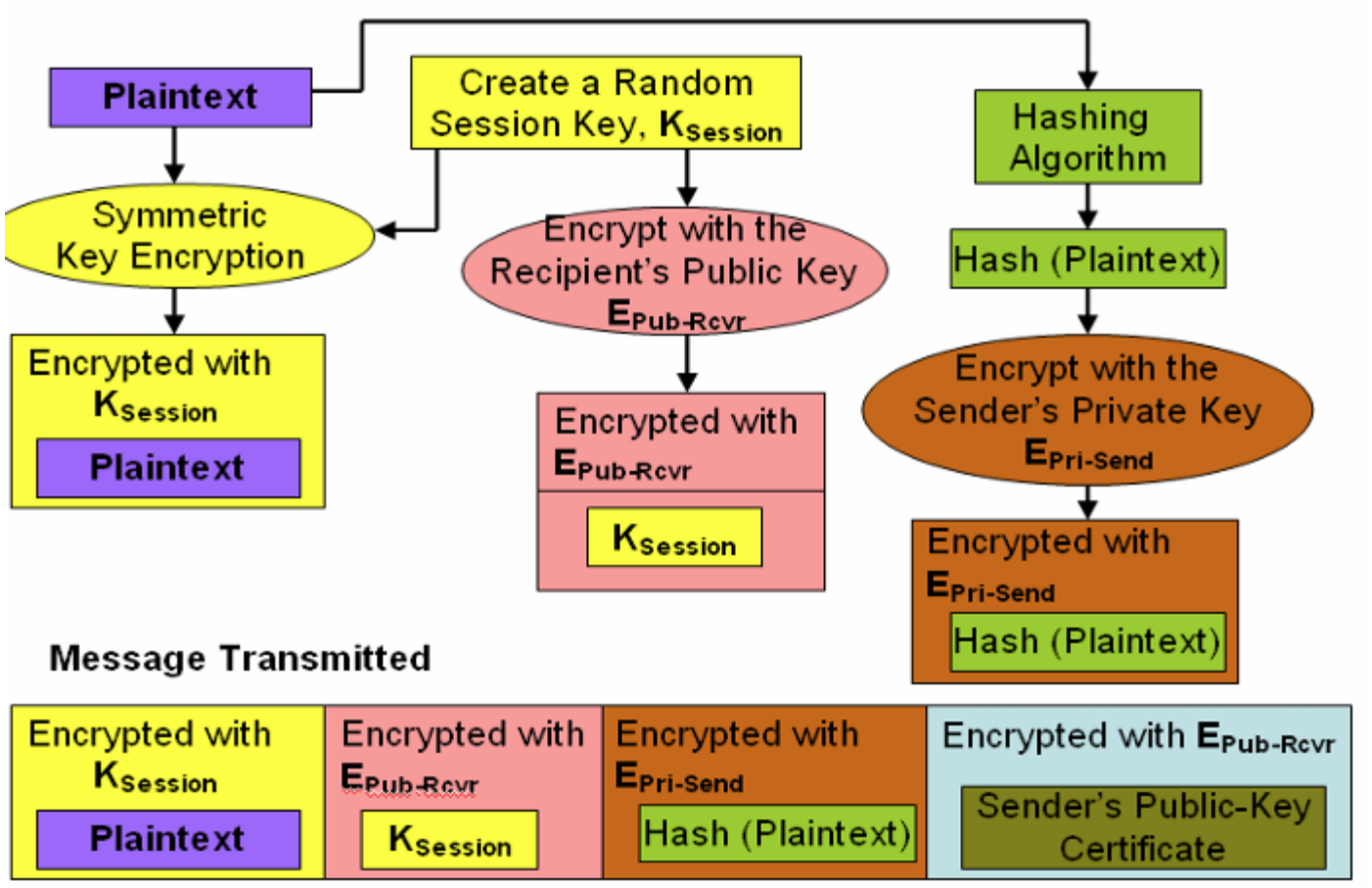
ΥΠΗΡΕΣΙΕΣ S/MIME

- **Εμπιστευτικότητα:** Μόνο ο εξουσιοδοτημένος παραλήπτης μπορεί να διαβάσει το μήνυμα
- **Αυθεντικότητα:** Ο παραλήπτης μπορεί να ελέγξει την αυθεντικότητα του αποστολέα του μηνύματος
- **Ακεραιότητα:** Ο παραλήπτης μπορεί να ελέγξει εάν το περιεχόμενο του μηνύματος έχει αλλοιωθεί κατά τη διαδρομή του στο δίκτυο

ΑΛΓΟΡΙΘΜΟΙ S/MIME

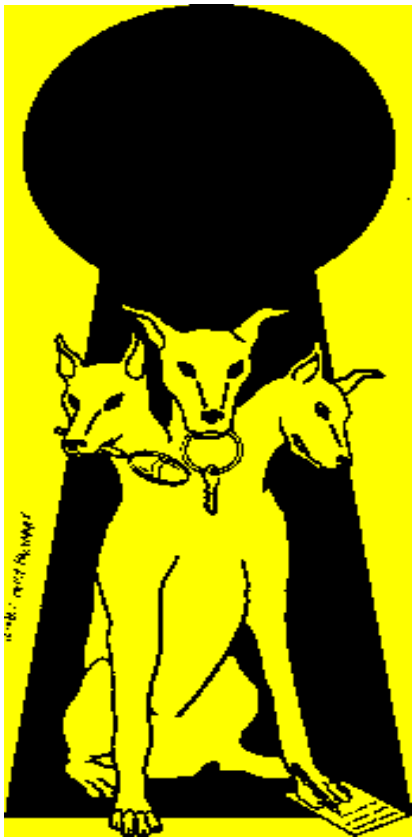
- Συναρτήσεις κατακερματισμού: SHA256, SHA512
- Ψηφιακές υπογραφές: DSS & RSA
- Κρυπτογράφηση μυστικού κλειδιού: RSA, Diffie-Hellman
- Κρυπτογράφηση μηνύματος: AES, Triple-DES

ΣΧΗΜΑ ΤΟΥ S/MIME



Meghanathan, Natarajan. (2014). A Tutorial on Network Security: Attacks and Controls. 1. 10.4018/978-1-4666-4789-3.ch011.

KERBEROS: ΠΡΟΕΛΕΥΣΗ ΟΝΟΜΑΣΙΑΣ



- Κατά την μυθολογία, το όνομα «Κέρβερος» παρέπεμπε σε ένα σκύλο με τρία κεφάλια, φύλακα της εισόδου στον «Άδη»

ΤΟ ΣΥΣΤΗΜΑ KERBEROS: ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

- Παρέχει έναν κεντρικό authentication server, με σκοπό την πιστοποίηση της ταυτότητας των χρηστών (users) στους εξυπηρετητές (servers) και αντίστροφα (servers to users)
- Στηρίζεται στην conventional encryption, ενώ δεν χρησιμοποιείται η κρυπτογράφηση δημοσίου κλειδιού
- Υποστηρίζονται διαφορετικές εκδόσεις: Version 4 και Version 5
- Στην έκδοση 5 γίνεται χρήση πολλαπλών symmetric block ciphers

KERBEROS ΕΚΔΟΣΗ 4

- Για να εξασφαλίσει την υπηρεσία της πιστοποίησης αυθεντικότητας χρησιμοποιεί Block Cipher
- Παράμετροι:
  - **C** = client (πελάτης)
  - **AS** = authentication server (διακομιστής πιστοποίησης)
  - **V** = server (εξυπηρετητής)
  - **IDc** = identifier of user on C (αναγνωριστικό του χρήστη C)
  - **IDv** = identifier of V (αναγνωριστικό του V)
  - **P_c** = password of user on C (συνθηματικό του χρήστη C)
  - **ADc** = network address of C (διεύθυνση δικτύου του C)
  - **Kv** = secret encryption key shared by AS an V (μυστικό κλειδί)
  - **TS** = timestamp
  - **||** = concatenation

ΕΝΑΣ ΑΠΛΟΣ ΔΙΑΛΟΓΟΣ ΠΙΣΤΟΠΟΙΗΣΗΣ

Ο διακομιστής πιστοποίησης AS γνωρίζει τα συνθηματικά όλων των χρηστών και τα έχει αποθηκεύσει σε κάποια κεντρική βάση δεδομένων.

Ο AS μοιράζεται ένα μοναδικό μυστικό κλειδί με κάθε διακομιστή

Σενάριο: Ο χρήστης C ζητά πρόσβαση στο διακομιστή V

- Client → Authentication Server: IDc || P_c || IDv
- Authentication Server → Client: Ticket
- Client → V (Server): IDc || Ticket

P_c : συνθηματικό του χρήστη C

IDv : αναγνωριστικό του διακομιστή V

IDc : αναγνωριστικό του χρήστη C

Kv : μυστικό κλειδί

$$\mathbf{Ticket = E_{Kv}[IDc \,||\, P_c \,||\, IDv]}$$

VERSION 4 ΜΗΧΑΝΙΣΜΟΣ ΠΙΣΤΟΠΟΙΗΣΗΣ

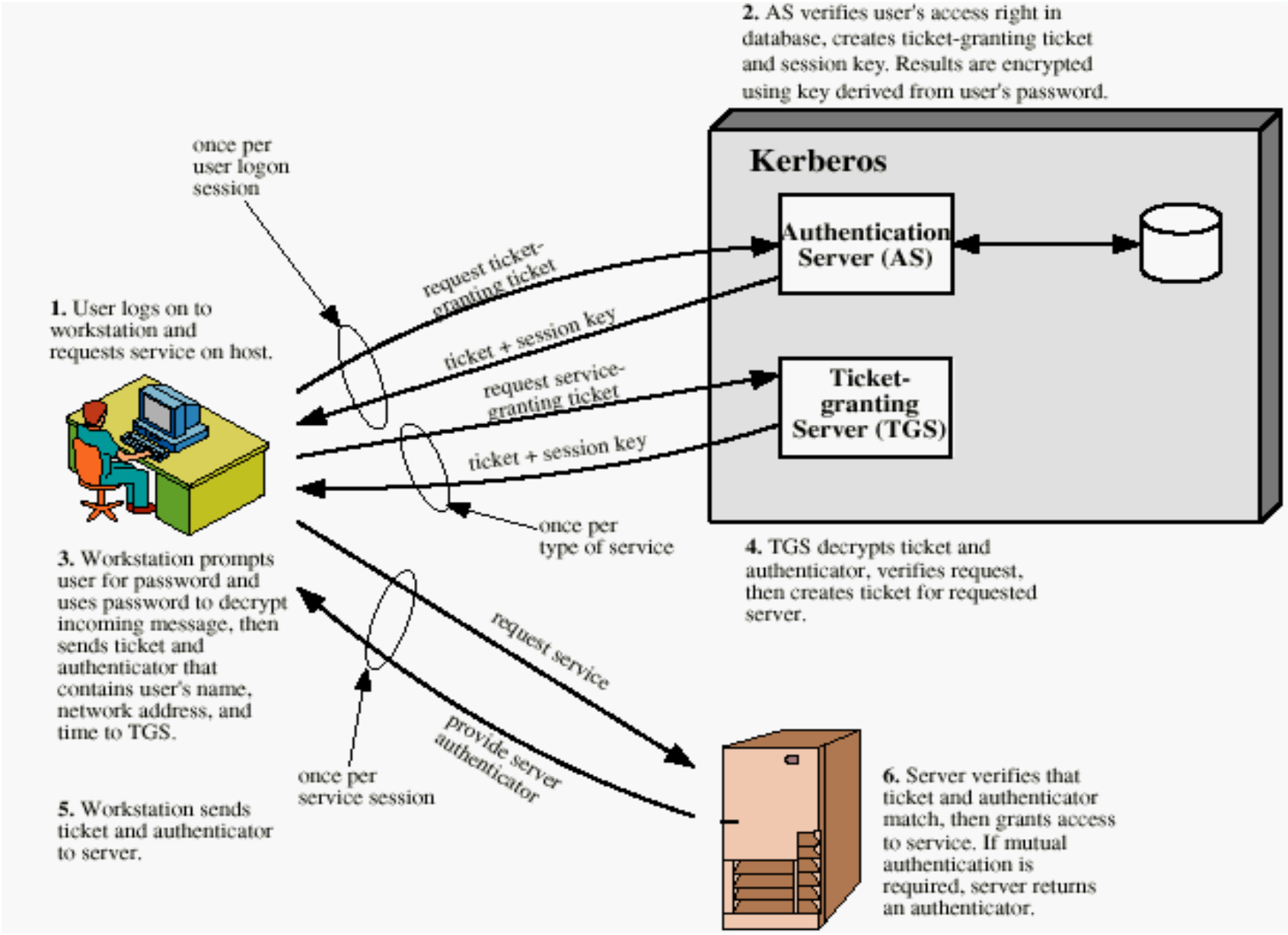
- Προβλήματα:
  - Χρήση συνθηματικού πολλές φορές
  - Η πρώτη μετάδοση του συνθηματικού είναι μη κρυπτογραφημένη

- Η απειλή έγκειται στο γεγονός ότι ένας εισβολέας μπορεί να υποκλέψει το συνθηματικό και να το χρησιμοποιήσει στις υπηρεσίες που έχει πρόσβαση το θύμα.

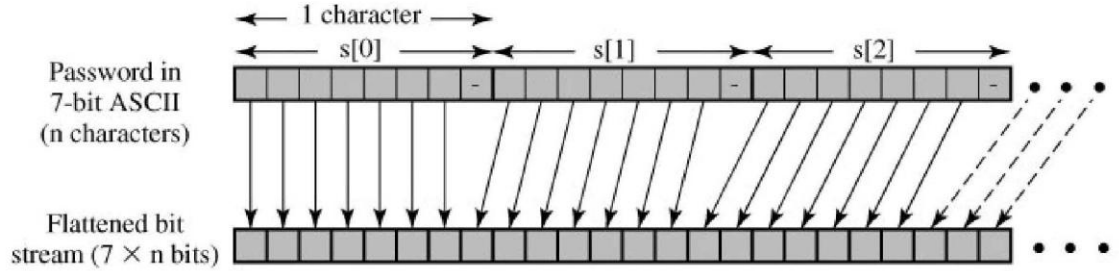
ΤΕΛΙΚΗ ΠΡΟΣΕΓΓΙΣΗ

1. Ο χρήστης εισέρχεται στο σταθμό εργασίας και ζητά υπηρεσία από τον υπολογιστή υπηρεσίας
2. Ο AS επιβεβαιώνει το δικαίωμα πρόσβασης και δημιουργεί το εισιτήριο εκχώρησης εισιτηρίου και το κλειδί περιόδου τα οποία κρυπτογραφούνται
3. Ο σταθμός εργασίας ζητά συνθηματικό χρήστη για να αποκρυπτογραφήσει τα μηνύματα και μετά στέλνει στον διακομιστή εκχώρησης εισιτηρίων το εισιτήριο με το όνομά του, την IP του και το χρόνο
4. Ο TGS αποκρυπτογραφεί το εισιτήριο, επιβεβαιώνει την αίτηση και δημιουργεί το εισιτήριο για τον αντίστοιχο διακομιστή μαζί με το κλειδί περιόδου
5. Ο σταθμός εργασίας στέλνει το εισιτήριο στο διακομιστή
6. Ο διακομιστής επιβεβαιώνει το εισιτήριο και δίνει πρόσβαση στην υπηρεσία

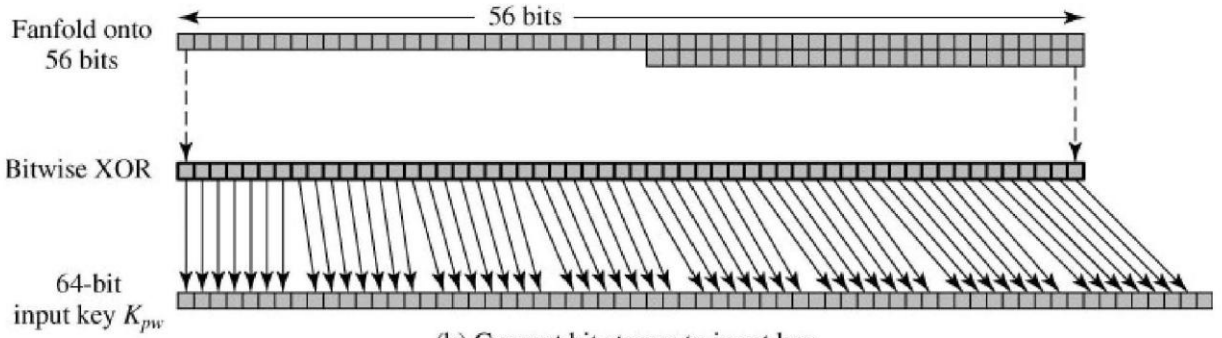
KERBEROS: ΤΕΛΙΚΗ ΠΡΟΣΕΓΓΙΣΗ



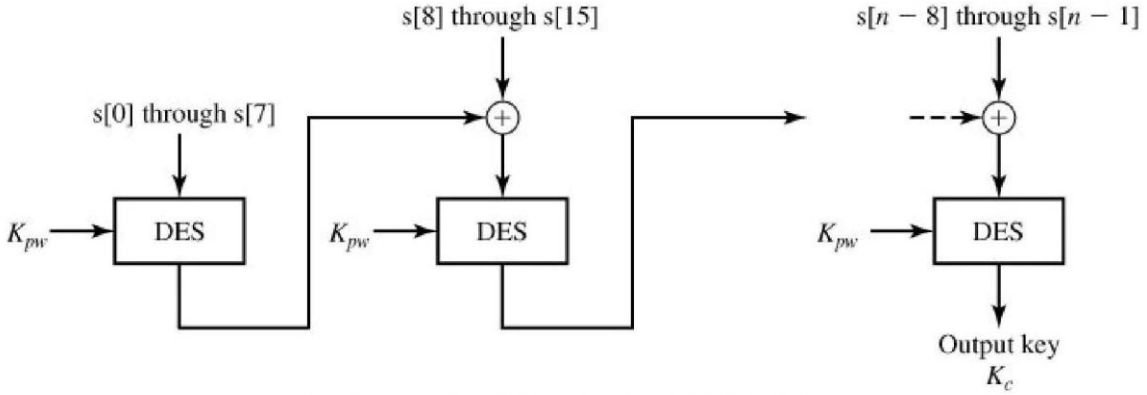
ΤΕΧΝΙΚΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΣΤΟ ΣΥΣΤΗΜΑ KERBEROS



(a) Convert password to bit stream

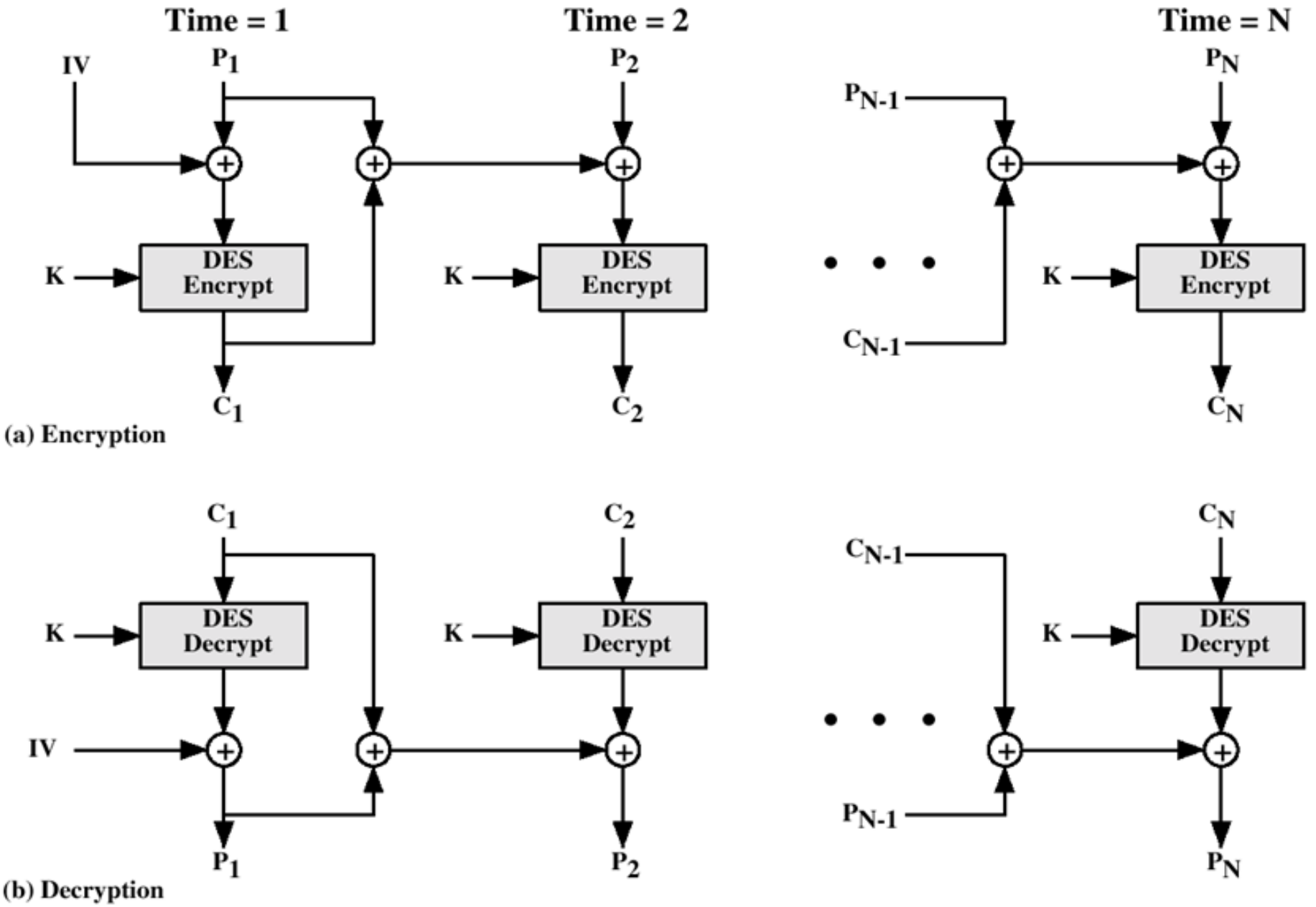


(b) Convert bit stream to input key



(c) Generate DES CBC checksum of password

PCBC ΜΗΧΑΝΙΣΜΟΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ



KERBEROS Version 4 vs Version 5

- Ο K4 χρησιμοποιεί DES για κρυπτογράφηση ενώ ο K5 χρησιμοποιεί AES
- Ο K4 χρησιμοποιεί απλούστερη δομή εισιτηρίων σε σύγκριση με το K5. Τα εισιτήρια στο K4 δεν περιέχουν πληροφορίες σχετικά με τα δεδομένα εξουσιοδότησης του χρήστη
- Ο K5 εισάγει μια πιο ευέλικτη και επεκτάσιμη δομή εισιτηρίων. Τα εισιτήρια στο K5 περιέχουν πρόσθετες πληροφορίες, όπως τα δεδομένα εξουσιοδότησης, επιτρέποντας πιο εξελιγμένους μηχανισμούς ελέγχου πρόσβασης και υποστήριξη για ανανεώσιμα εισιτήρια

Απορίες???