Chương 6

AN TOÀN THƯ ĐIỆN TỬ

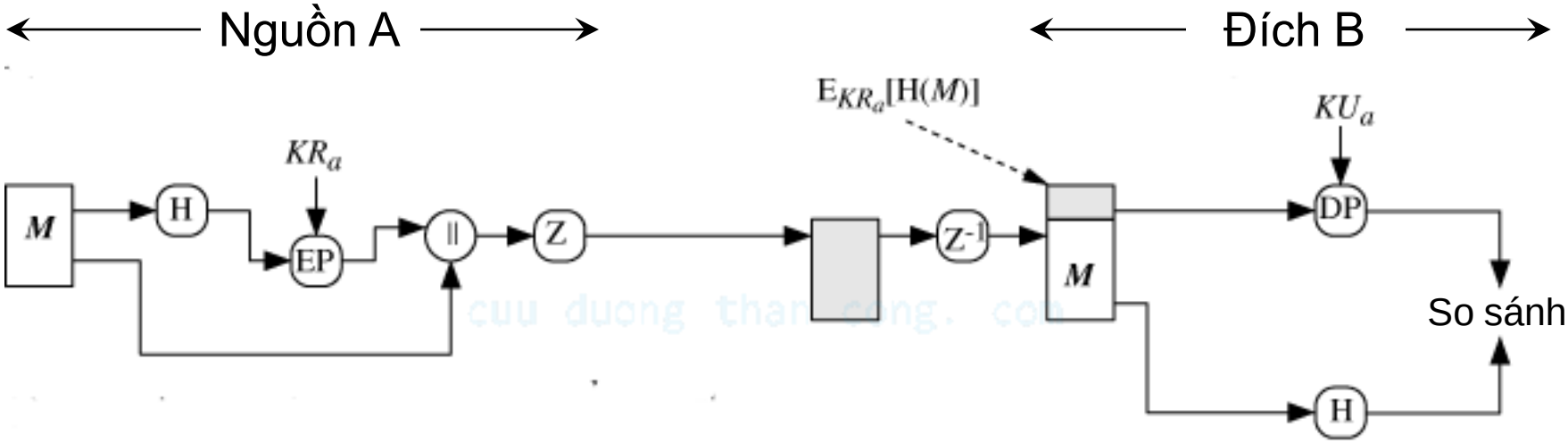
Giới thiệu

- Thư điện tử là dịch vụ mạng phổ dụng nhất
- Hiện nay các thông báo không được bảo mật
  - Có thể đọc được nội dung trong quá trình thông báo di chuyển trên mạng
  - Những người dùng có đủ quyền có thể đọc được nội dung thông báo trên máy đích
  - Thông báo dễ dàng bị giả mạo bởi một người khác
  - Tính toàn vẹn của thông báo không được đảm bảo
- Các giải pháp xác thực và bảo mật thường dùng
  - PGP (Pretty Good Privacy)
  - S/MIME (Secure/Multipurpose Internet Mail Extensions)

PGP

- Do Phil Zimmermann phát triển vào năm 1991
- Chương trình miễn phí, chạy trên nhiều môi trường khác nhau (phần cứng, hệ điều hành)
  - Có phiên bản thương mại nếu cần hỗ trợ kỹ thuật
- Dựa trên các giải thuật mật mã an ninh nhất
- Chủ yếu ứng dụng cho thư điện tử và file
- Độc lập với các tổ chức chính phủ
- Bao gồm 5 dịch vụ : xác thực, bảo mật, nén, tương thích thư điện tử, phân và ghép
  - Ba dịch vụ sau trong suốt đối với người dùng

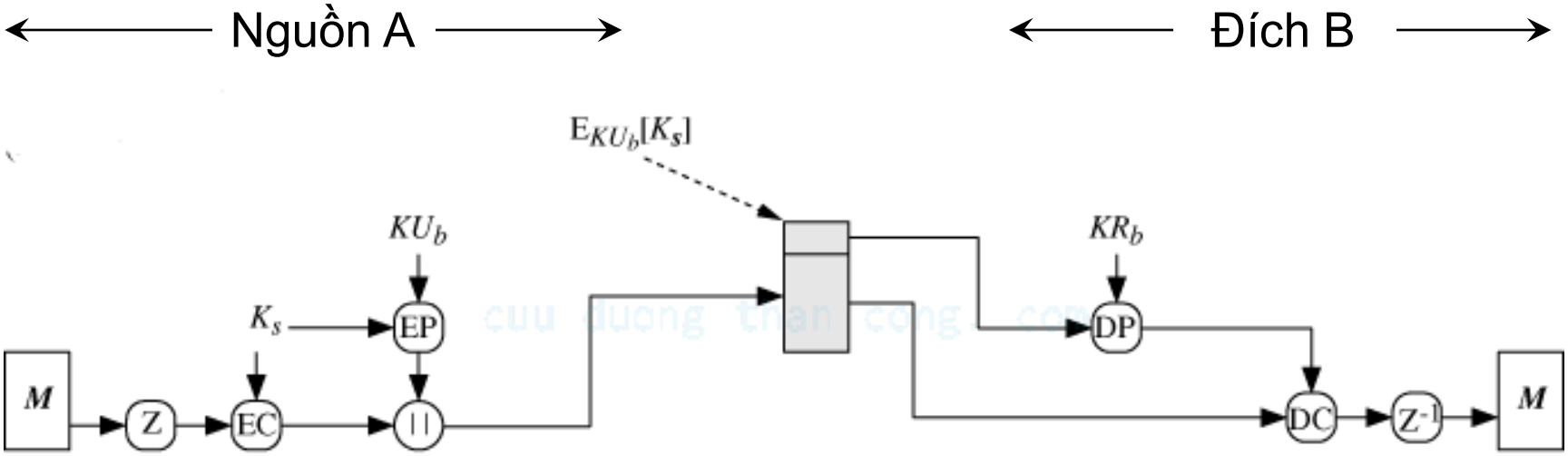
Xác thực của PGP



M = Thông báo gốc
H = Hàm băm
‖ = Ghép
Z = Nén
Z^{-1} = Cởi nén

EP = Mã hóa khóa công khai
DP = Giải mã khóa công khai
KR_a = Khóa riêng của A
KU_a = Khóa công khai của A

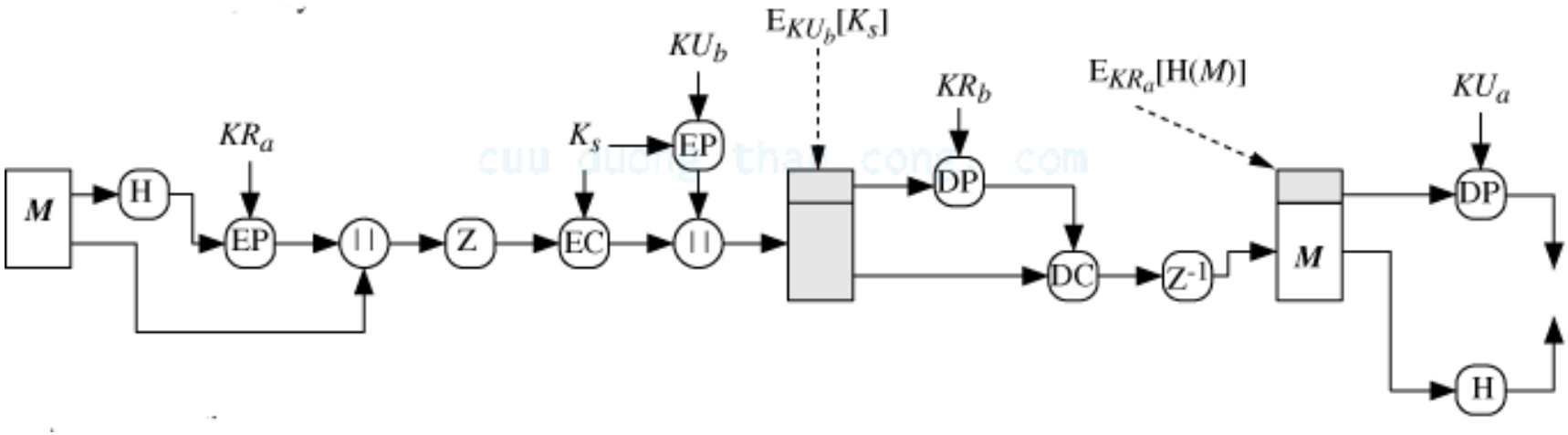
Bảo mật của PGP



EC = Mã hóa đối xứng
DC = Giải mã đối xứng
K_s = Khóa phiên

Xác thực và bảo mật của PGP

Nguồn A → ← Đích B



Nén của PGP

- PGP nén thông báo sử dụng giải thuật ZIP
- Ký trước khi nén
  - Thuận tiện lưu trữ và kiểm tra, nếu ký sau khi nén thì
    - Cần lưu phiên bản nén với chữ ký, hoặc
    - Cần nén lại thông báo mỗi lần muốn kiểm tra
  - Giải thuật nén không cho kết quả duy nhất
    - Mỗi phiên bản cài đặt có tốc độ và tỷ lệ nén khác nhau
    - Nếu ký sau khi nén thì các chương trình PGP cần sử dụng cùng một phiên bản của giải thuật nén
- Mã hóa sau khi nén
  - Ít dữ liệu sẽ khiến việc mã hóa nhanh hơn
  - Thông báo nén khó phá mã hơn thông báo thô

Tương thích thư điện tử của PGP

- PGP bao giờ cũng phải gửi dữ liệu nhị phân
- Nhiều hệ thống thư điện tử chỉ chấp nhận văn bản ASCII (các ký tự đọc được)
  - Thư điện tử vốn chỉ chứa văn bản đọc được
- PGP dùng giải thuật cơ số 64 chuyển đổi dữ liệu nhị phân sang các ký tự ASCII đọc được
  - Mỗi 3 byte nhị phân chuyển thành 4 ký tự đọc được
- Hiệu ứng phụ của việc chuyển đổi là kích thước thông báo tăng lên 33%
  - Nhưng có thao tác nén bù lại

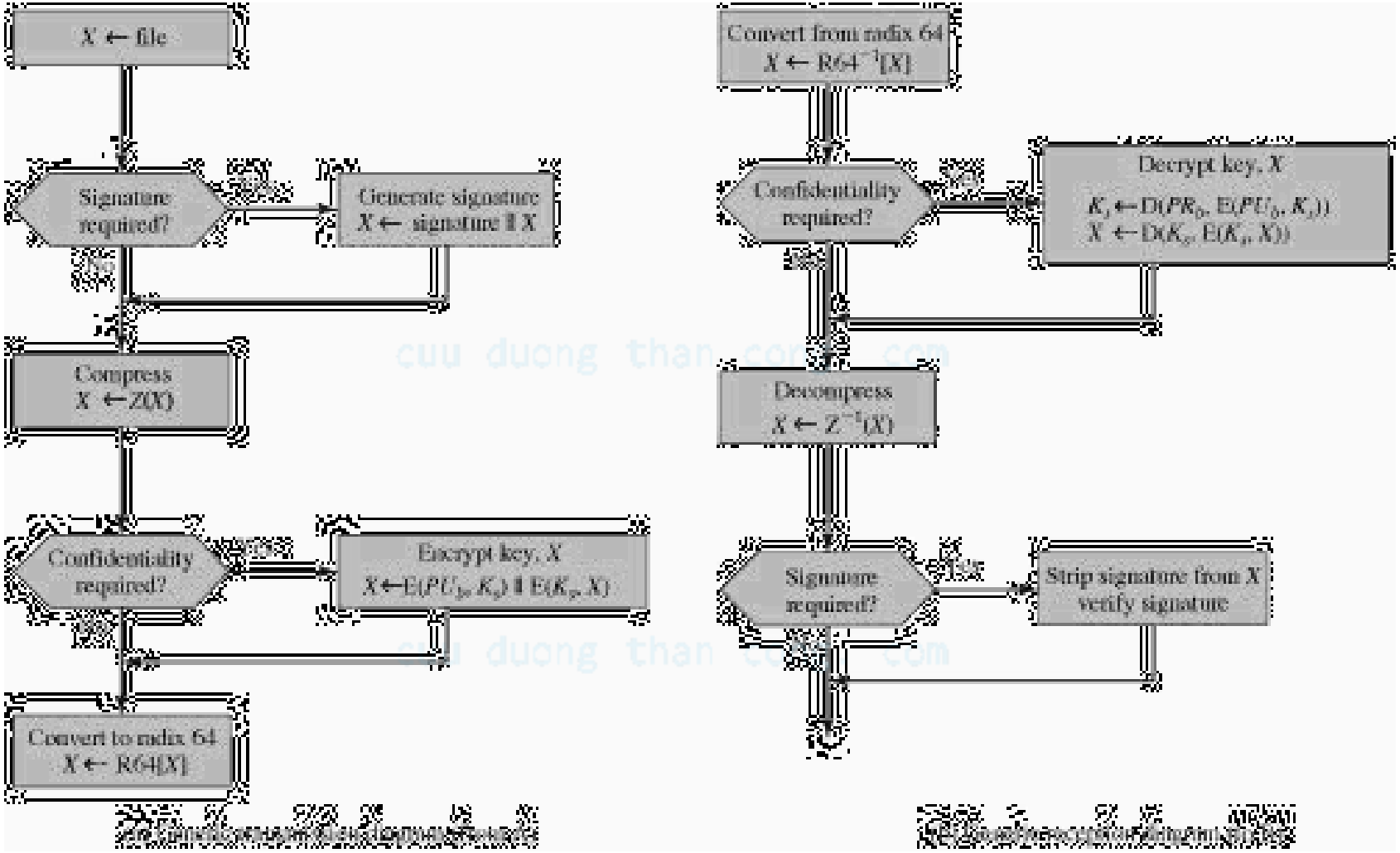
Bảng chuyển đổi cơ số 64

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)	=

Phân và ghép của PGP

- Các giao thức thư điện tử thường hạn chế độ dài tối đa của thông báo
  - Ví dụ thường là 50 KB
- PGP phân thông báo quá lớn thành nhiều thông báo đủ nhỏ
- Việc phân đoạn thông báo thực hiện sau tất cả các công đoạn khác
- Bên nhận sẽ ghép các thông báo nhỏ trước khi thực hiện các công đoạn khác

Sơ đồ xử lý PGP



Khóa phiên PGP

- Cần sử dụng một khóa phiên cho mỗi thông báo
  - Độ dài 56 bit với DES, 128 bit với CAST-128 và IDEA, 168 bit với 3DES
- Cách thức sinh khóa phiên cho CAST-128
  - Sử dụng chính CAST-128 theo phương thức CBC
  - Từ một khóa 128 bit và 2 khối nguyên bản 64 bit sinh ra 2 khối bản mã 64 bit tạo thành khóa phiên 128 bit
  - Hai khối nguyên bản đầu vào được sinh ngẫu nhiên dựa vào chuỗi các phím gõ từ người dùng
  - Khóa đầu vào được sinh từ các khối nguyên bản đầu vào và khóa phiên đầu ra trước đó

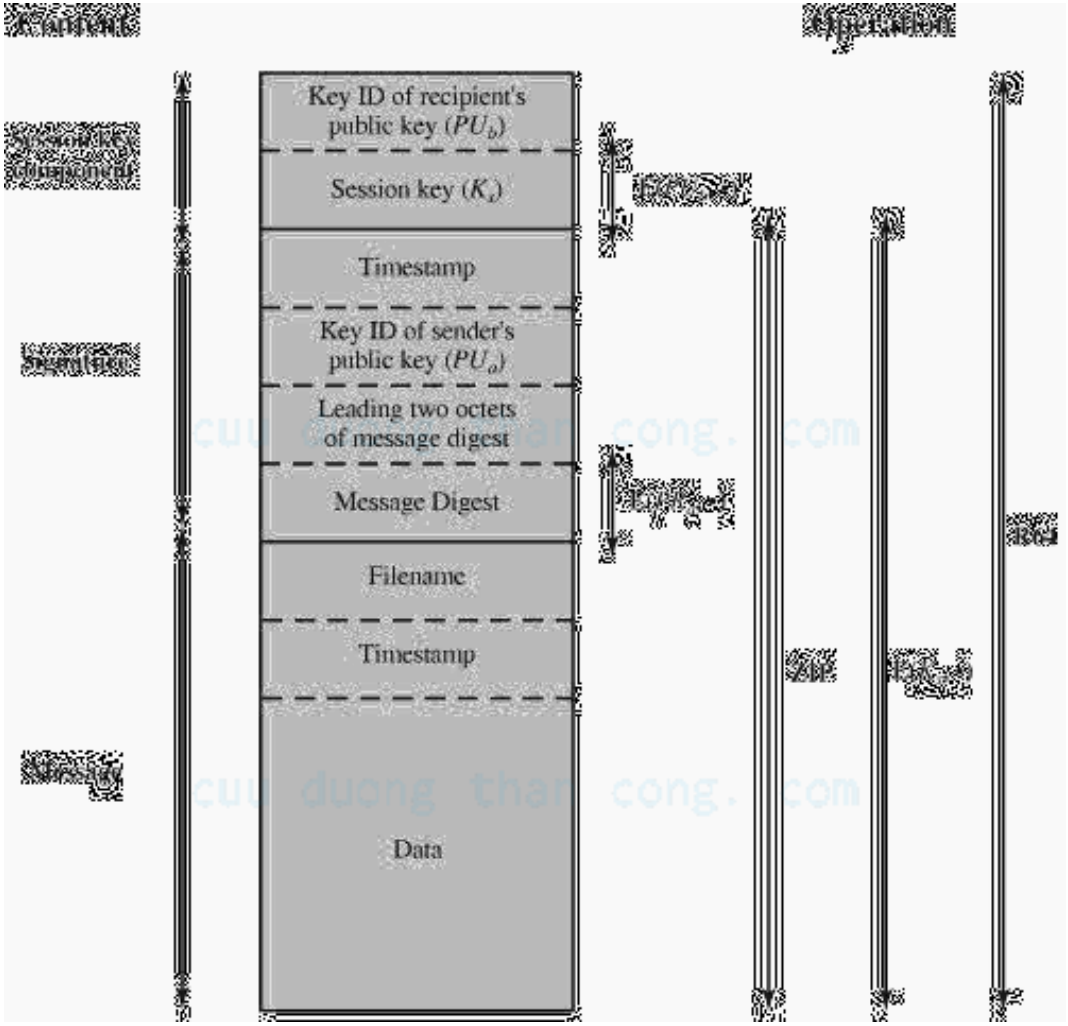
Khóa công khai/khóa riêng PGP

- Người dùng có thể có nhiều cặp khóa công khai/khóa riêng
  - Nhu cầu thay đổi cặp khóa hiện thời
  - Giao tiếp với nhiều nhóm đối tác khác nhau
  - Hạn chế lượng thông tin mã hóa với mỗi khóa để nâng cao độ an toàn
- Cần chỉ ra khóa công khai nào được sử dụng để mã hóa khóa phiên
- Cần chỉ ra chữ ký của bên gửi tương ứng với khóa công khai nào

Định danh khóa công khai PGP

- Để chỉ ra mã công khai nào được sử dụng có thể truyền khóa công khai cùng với thông báo
  - Không hiệu quả
    - Khóa công khai RSA có thể dài hàng trăm chữ số thập phân
- Định danh gắn với mỗi khóa công khai là 64 bit trọng số nhỏ nhất của nó
  - ID của KU_a = KU_a mod 2^{64}
  - Xác suất cao là mỗi khóa công khai có một định danh duy nhất

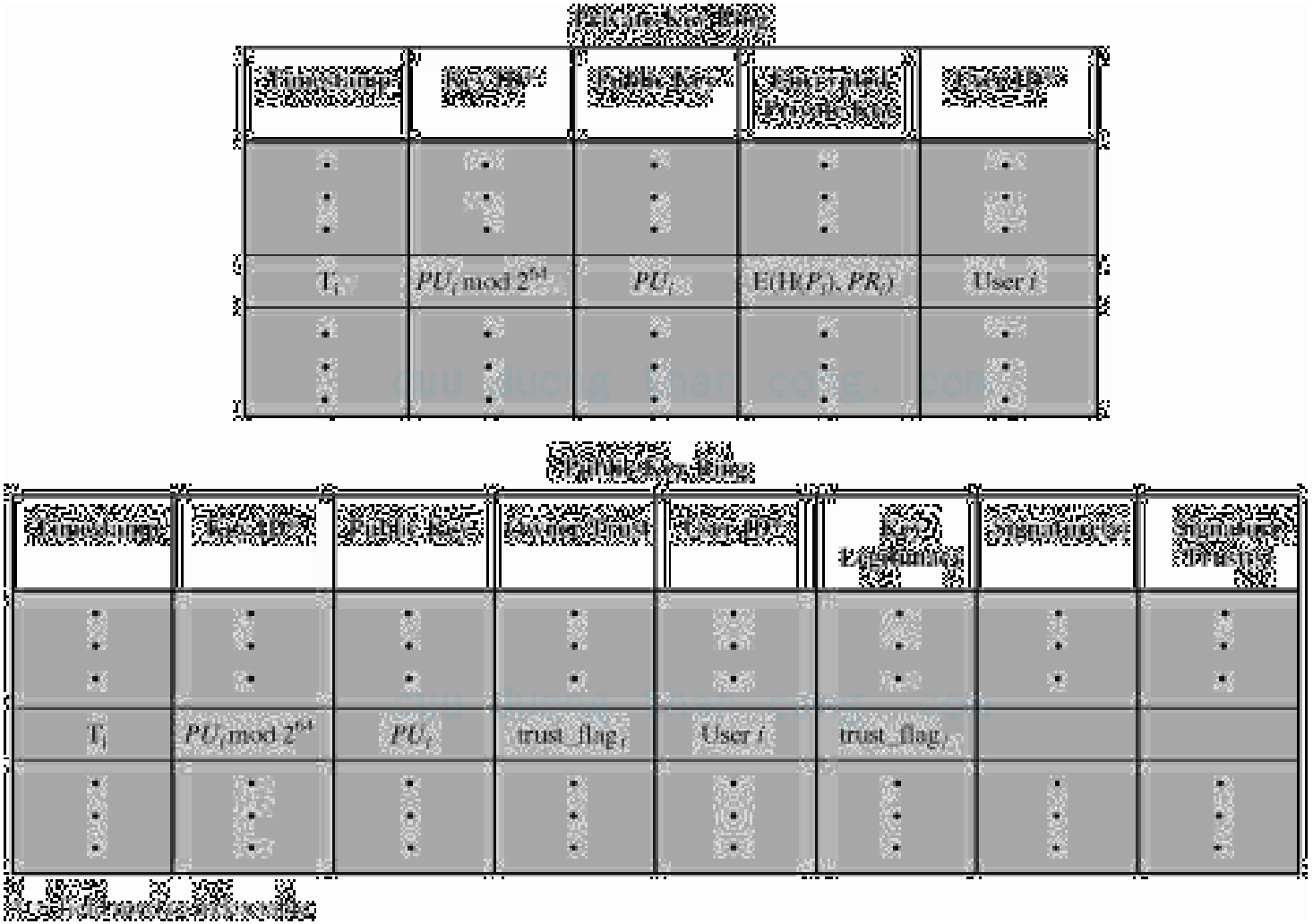
Khuôn dạng thông báo PGP



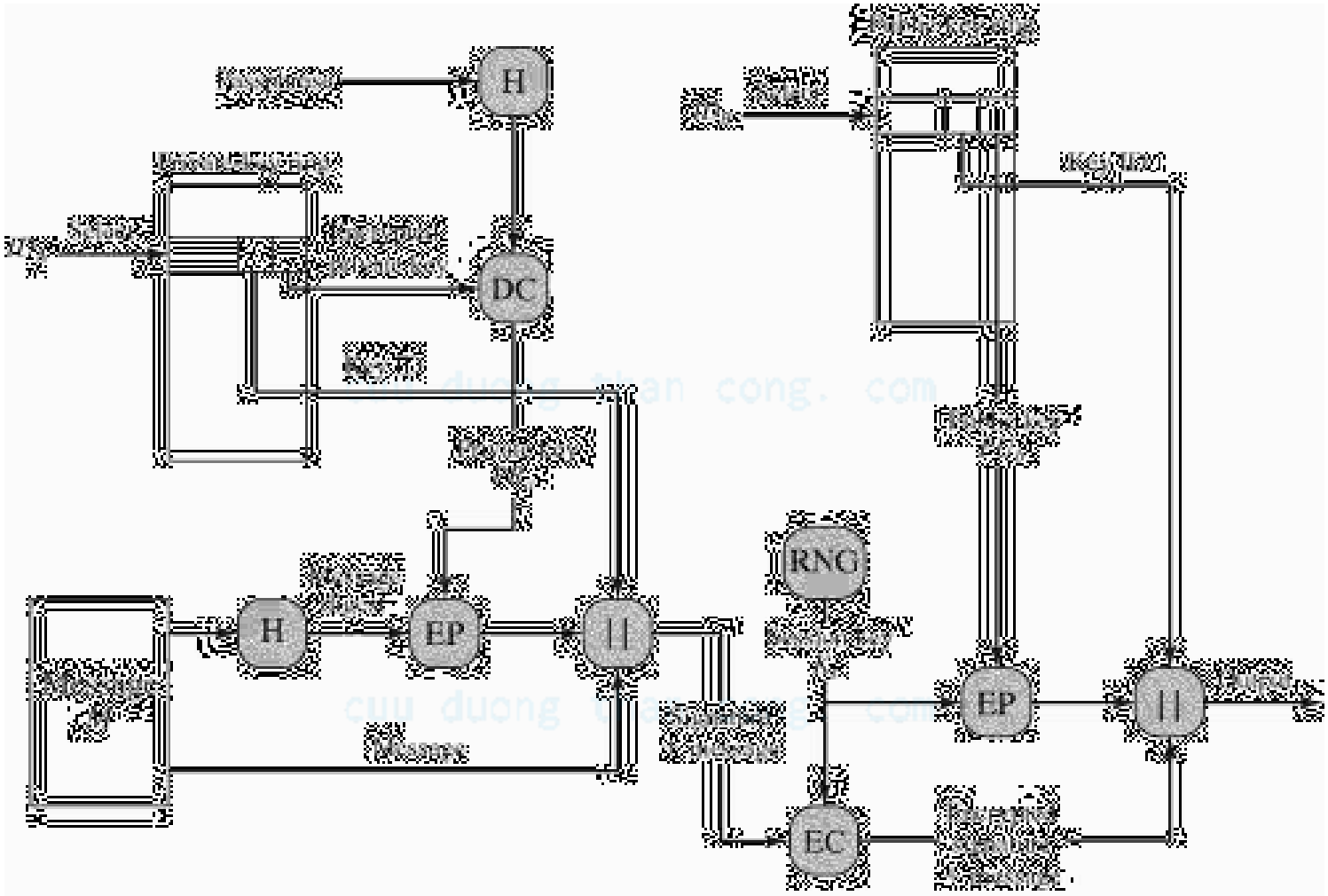
Vòng khóa PGP

- Mỗi người dùng PGP có hai vòng khóa
  - Vòng khóa riêng chứa các cặp khóa công khai/khóa riêng của người dùng hiện thời
    - Có thể được chỉ mục bởi định danh khóa công khai (**Key ID**) hoặc định danh người dùng (**User ID**)
    - Khóa riêng được mã hóa sử dụng khóa là giá trị băm của mật khẩu nhập trực tiếp từ người dùng
  - Vòng khóa công khai chứa các khóa công khai của những người dùng quen biết với người dùng hiện thời
    - Có thể được chỉ mục bởi định danh khóa công khai hoặc định danh người dùng

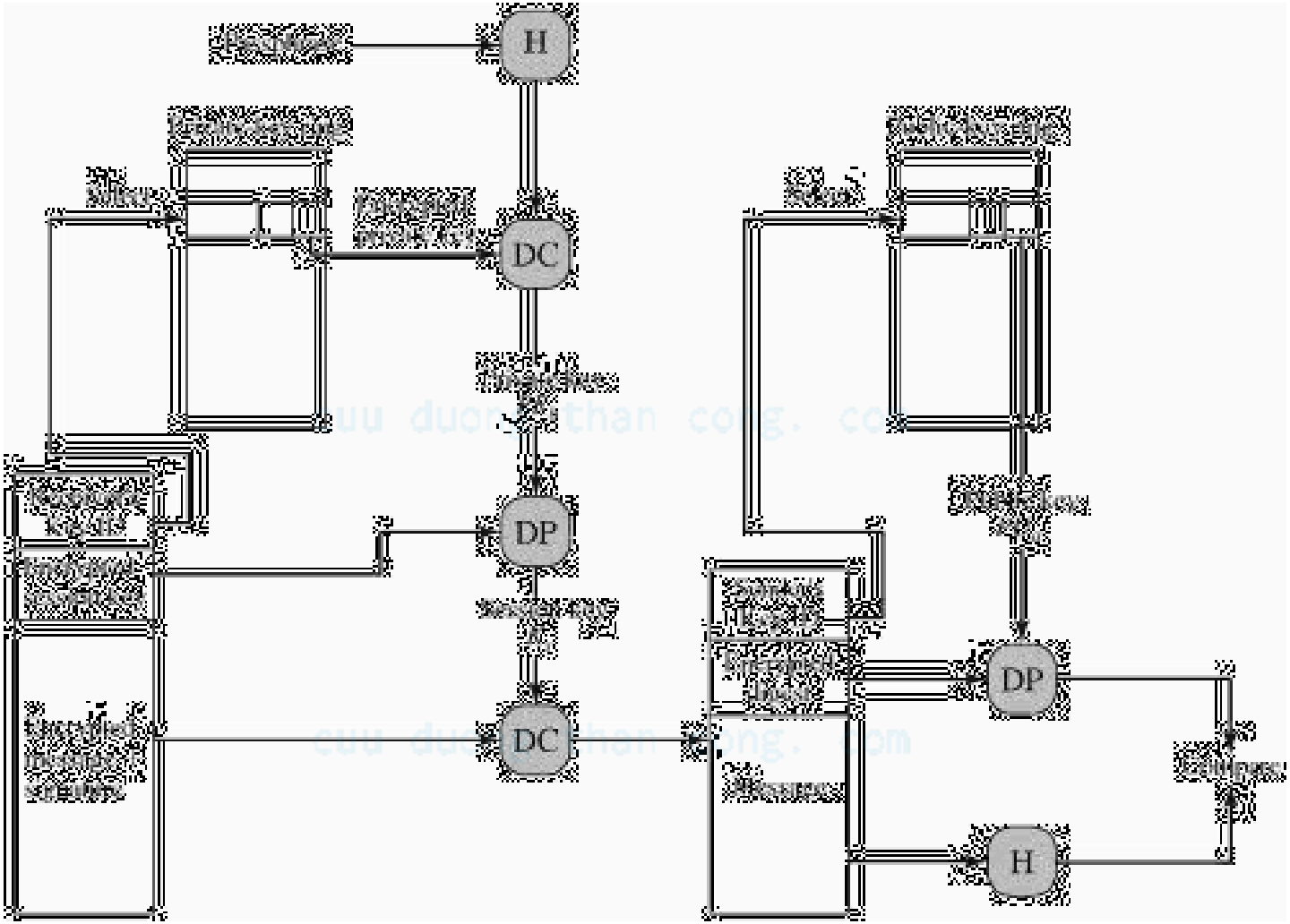
Cấu trúc các vòng khóa PGP



Sơ đồ tạo thông báo PGP



Sơ đồ nhận thông báo PGP



Quản lý khóa PGP

- Thay vì dựa trên các CA (cơ quan chứng thực), đối với PGP mỗi người dùng là một CA
  - Có thể ký cho những người dùng quen biết trực tiếp
- Tạo nên một mạng lưới tin cậy
  - Tin các khóa đã được chính bản thân ký
  - Có thể tin các khóa những người dùng khác ký nếu có một chuỗi các chữ ký tới chúng
- Mỗi khóa có một chỉ số tin cậy
- Các người dùng có thể thu hồi khóa của họ

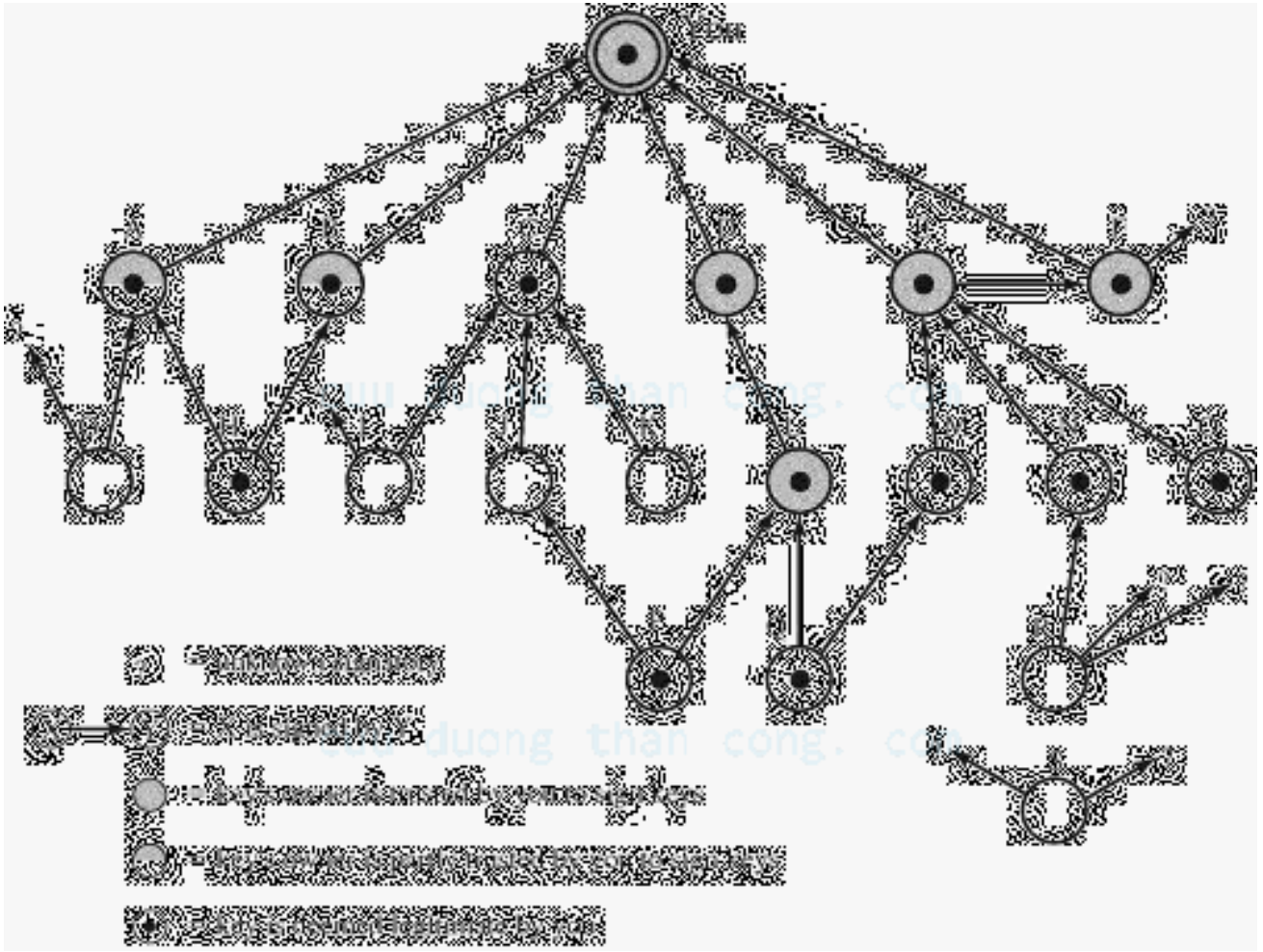
Mô hình tin cậy PGP (1)

- Với mỗi khóa công khai người dùng ấn định độ tin cậy vào chủ nhân của nó trong trường **Owner trust**
  - Giá trị *ultimate trust* được tự động gán nếu khóa công khai có trong vòng khóa riêng
  - Giá trị người dùng có thể gán là *unknown*, *untrusted*, *marginally trusted*, hay *completely trusted*
- Giá trị các trường **Signature trust** được sao chép từ các trường **Owner trust** tương ứng
  - Nếu không có thì được gán giá trị *unknown user*

Mô hình tin cậy PGP (2)

- Xác định giá trị của trường **Key legitimacy**
  - Nếu khóa công khai có ít nhất một chữ ký với giá trị **Signature trust** là *ultimate* thì **Key legitimacy** là *ultimate*
  - Nếu không, **Key legitimacy** được tính bằng tổng có trọng số các giá trị **Signature trust**
    - Các chữ ký *completely trusted* có trọng số là 1/*X*
    - Các chữ ký *marginally trusted* có trọng số là 1/*Y*
    - *X* và *Y* là các tham số do người dùng xác định
    - Nếu tổng số đạt hoặc vượt ngưỡng 1 thì **Key legitimacy** được gán giá trị *complete*

Ví dụ mô hình tin cậy PGP



Thu hồi khóa công khai

- Lý do thu hồi khóa công khai
  - Địch thủ biết nguyên bản khóa riêng
  - Địch thủ biết bản mã khóa riêng và mật khẩu
  - Tránh sử dụng cùng một khóa trong một thời gian dài
- Quy trình thu hồi khóa công khai
  - Chủ sở hữu phát hành chứng thực thu hồi khóa
    - Cùng khuôn dạng như chứng thực bình thường nhưng bao gồm chỉ dấu thu hồi khóa công khai
    - Chứng thực được ký với khóa riêng tương ứng khóa công khai cần thu hồi
  - Mau chóng phát tán chứng thực một cách rộng rãi để các đối tác kịp thời cập nhật vòng khóa công khai

S/MIME

- Nâng cấp từ chuẩn khuôn dạng thư điện tử MIME có thêm tính năng an ninh thông tin
- MIME khắc phục những hạn chế của SMTP (Simple Mail Transfer Protocol)
  - Không truyền được file nhị phân (chương trình, ảnh,...)
  - Chỉ gửi được các ký tự ASCII 7 bit
  - Không nhận thông báo vượt quá kích thước cho phép
  - ...
- S/MIME có xu hướng trở thành chuẩn công nghiệp sử dụng trong thương mại và hành chính
  - PGP dùng cho cá nhân

Các chức năng của S/MIME

- Bao bọc dữ liệu
  - Mã hóa nội dung thông báo và các khóa liên quan
- Ký dữ liệu
  - Chữ ký số tạo thành nhờ mã hóa thông tin tổng hợp thông báo sử dụng khóa riêng của người ký
  - Thông báo và chữ ký số được chuyển đổi cơ số 64
- Ký và để nguyên dữ liệu
  - Chỉ chữ ký số được chuyển đổi cơ số 64
- Ký và bao bọc dữ liệu
  - Kết hợp ký và bao bọc dữ liệu

Xử lý chứng thực S/MIME

- S/MIME sử dụng các chứng thực khóa công khai theo X.509 v3
- Phương thức quản lý khóa lai ghép giữa cấu trúc phân cấp CA theo đúng X.509 và mạng lưới tin cậy của PGP
- Mỗi người dùng có một danh sách các khóa của bản thân, danh sách các khóa tin cậy và danh sách thu hồi chứng thực
- Chứng thực phải được ký bởi CA tin cậy