Bài 4. An toàn thư điện tử

From Slide của thầy Thọ

Nội dung

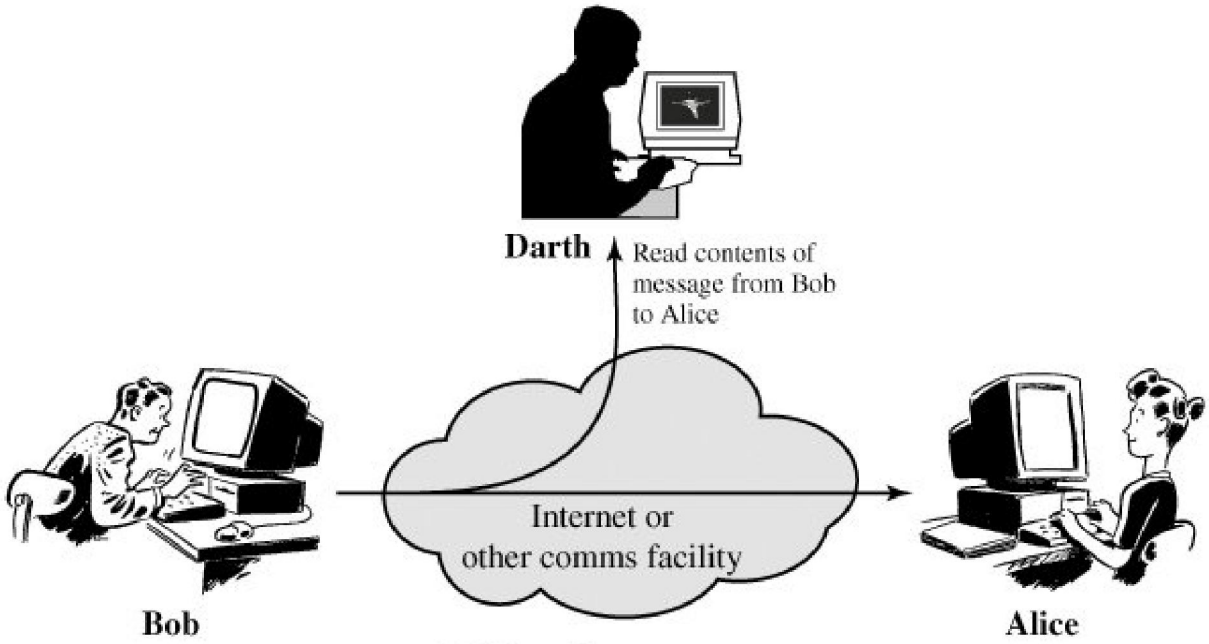
- 4.1. Giới thiệu
- 4.2. PGP
- 4.3. S/MIME

4.1. Giới thiệu

- Thư điện tử là dịch vụ mạng phổ dụng nhất hiện nay
- Tuy nhiên, việc gửi và nhận thư hữu hạt đều không được bảo mật

4.1. Giới thiệu

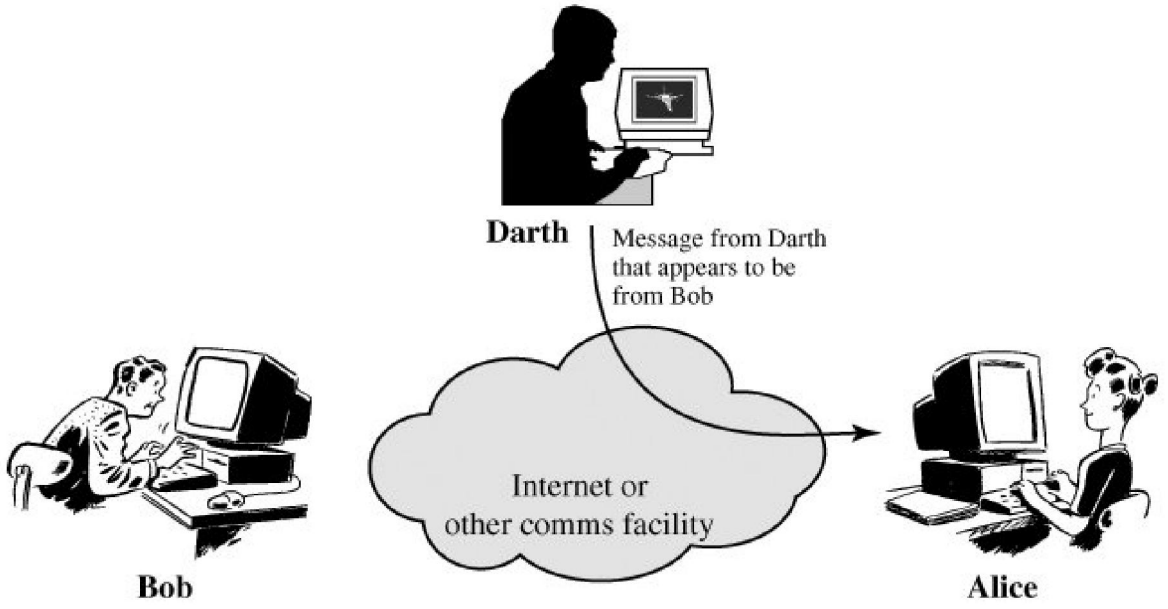
- Nguy cơ 1: Thư b. đ.c tr.m trong quá trình di chuy.n trên m.ng



(a) Release of message contents

4.1. Giới thiệu

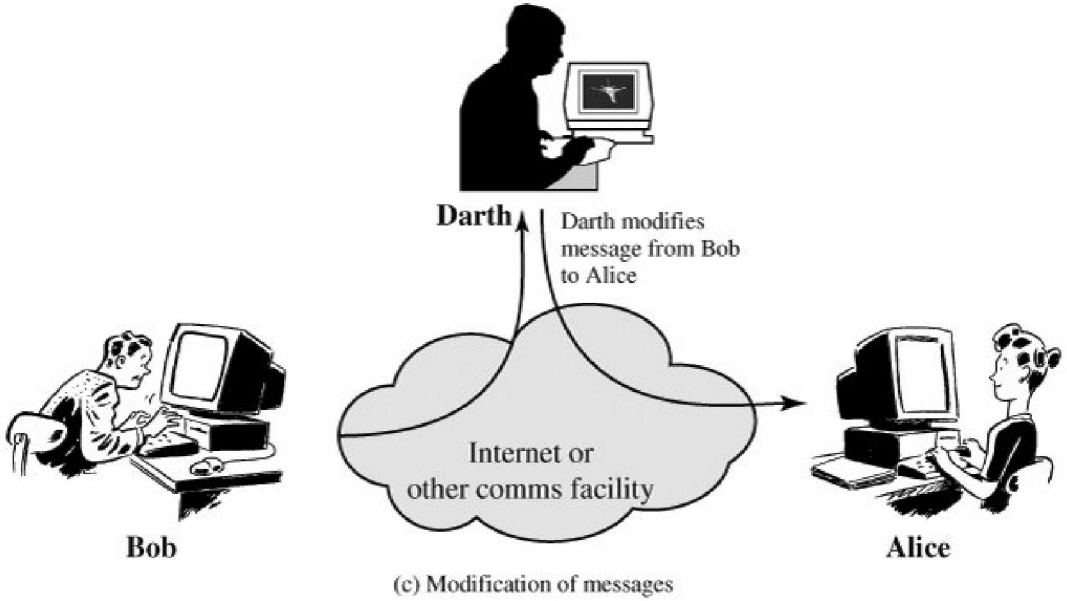
- Nguy cơ 2: Thư d. dàng b. gi. m.o b.i m.t ngư.i khác



(a) Masquerade

4.1. Giới thiệu

- Nguy cơ 3: Tính toàn v.n c.a n.i dung thư không đư.c đ.m b.o



(c) Modification of messages

4.1. Giới thiệu

- Cần các phương pháp để xác thực và bảo mật
- Các giải pháp thường dùng
  - PGP (Pretty Good Privacy)
  - S/MIME (Secure/Multipurpose Internet Mail Extensions)

4.2. PGP

- Do Phil Zimmermann phát tri.n vào năm 1991
- Chương trình mi.n phí, ch.y trên nhi.u môi trư.ng khác nhau (ph.n c.ng, h. đi.u hành)
  - Có phiên b.n thương m.i n.u c.n h. tr. k. thu.t

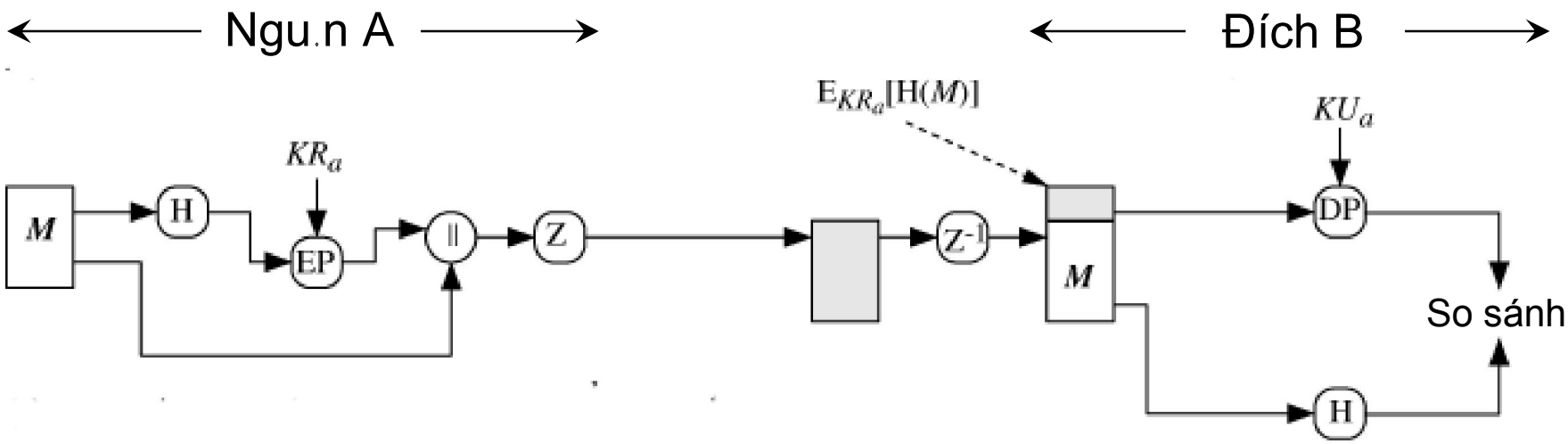
4.2. PGP

- D.a trên các gi.i thu.t m.t mã an toàn nh.t
- Ch. y.u .ng d.ng cho thư đi.n t. và file
- Đ.c l.p v.i các t. ch.c chính ph.
- Bao g.m 5 d.ch v. : xác th.c, b.o m.t, nén, tương thích thư đi.n t., phân và ghép
  - Ba d.ch v. sau trong su.t đ.i v.i ngư.i dùng

4.2. PGP

- Có độ an toàn rất cao nếu được sử dụng đúng cách
- Được sử dụng trong một số chương trình thư điện tử (Outlook Express, ...)

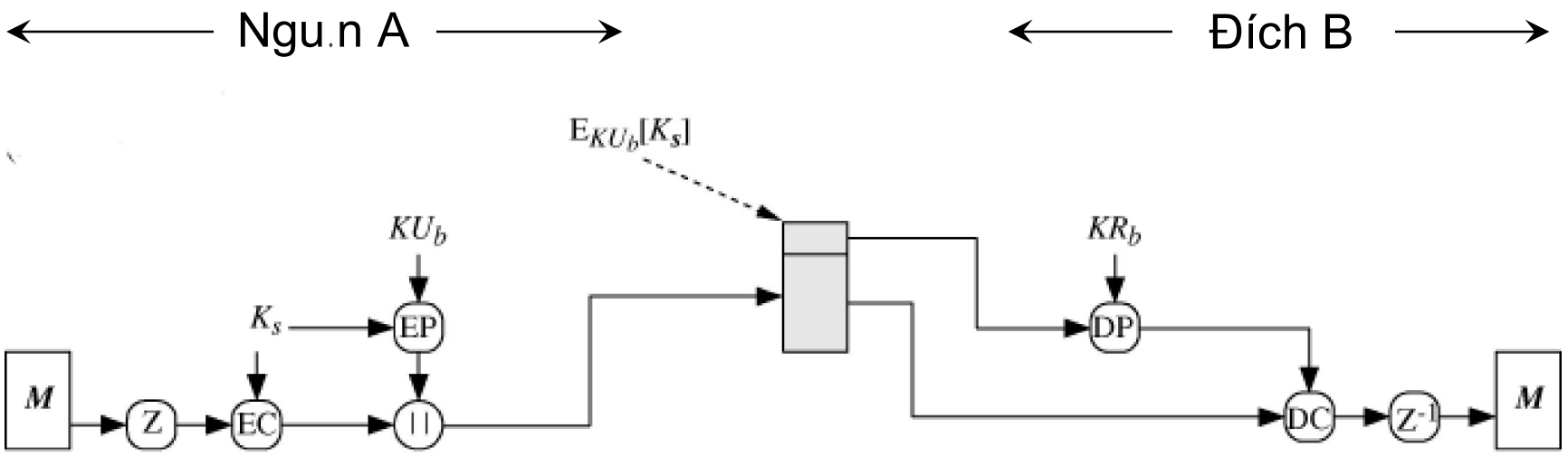
Xác th.c c.a PGP



M = Thông báo g.c
H = Hàm băm
. = Ghép
Z = Nén
Z^{-1} = C.i nén

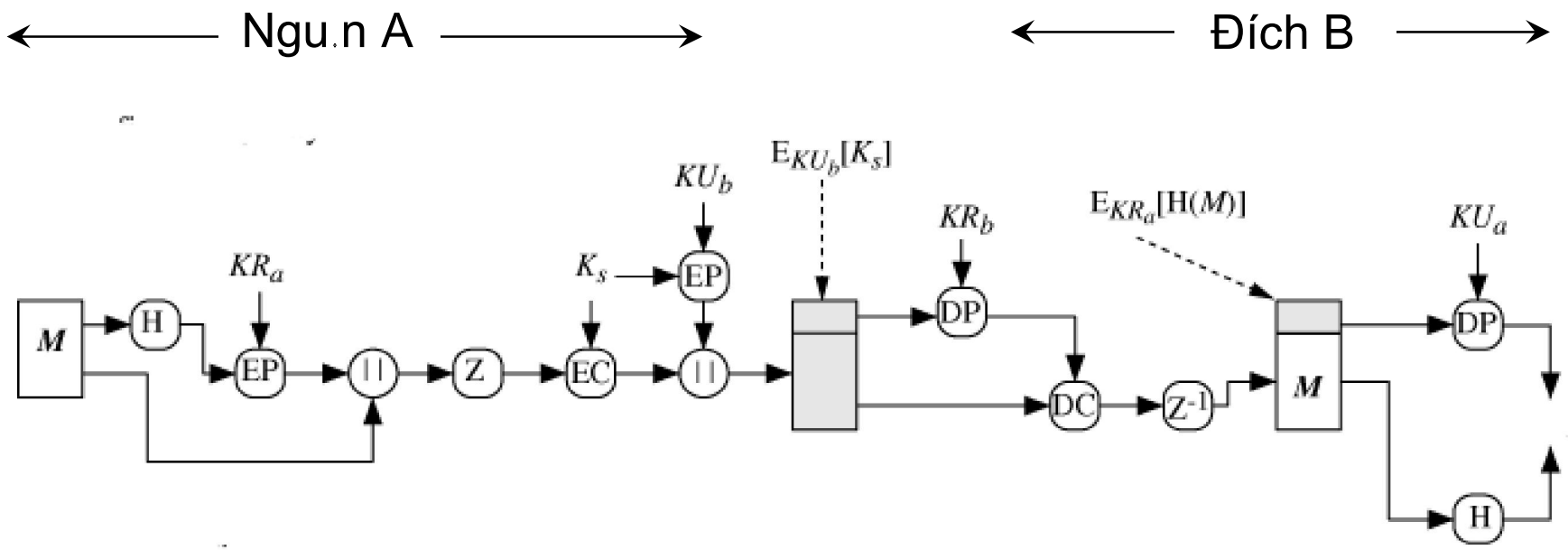
EP = Mã hóa khóa công khai
DP = Gi.i mã khóa công khai
KR_a = Khóa riêng c.a A
KU_a = Khóa công khai c.a A

B.o m.t c.a PGP



EC = Mã hóa đ.i x.ng
DC = Gi.i mã đ.i x.ng
K_s = Khóa phiên

Xác th.c và b.o m.t c.a PGP



Nén của PGP

- PGP nén thông báo sử dụng giải thuật ZIP
- Nén thông báo giúp giảm dung lượng gói tin truyền trên mạng

Nén của PGP

- Ký trước khi nén
  - Thuận tiện lưu trữ và kiểm tra, nếu ký sau khi nén thì
    - Cần nén lại thông báo mỗi lần muốn kiểm tra
  - Các phiên bản khác nhau của giải thuật nén không cho kết quả duy nhất
    - Mỗi phiên bản cài đặt có tốc độ và tỉ lệ nén khác nhau

Nén của PGP

- 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 đi.n t. c.a PGP

- PGP bao gi. c.ng ph.i g.i d. li.u nh. phân
- Nhi.u h. th.ng thư đi.n t. ch. ch.p nh.n văn b.n ASCII (các ký t. đ.c đư.c)
  - Thư đi.n t. v.n ch. ch.a văn b.n đ.c đư.c

Tương thích thư điện tử của PGP

- PGP dùng giải thuật cơ sở 64 chuyển đổi dữ liệu nhị phân sang các ký tự ASCII để được được
  - Mỗi 3 byte nhị phân chuyển thành 4 ký tự để được được
- Hiệu ứng phụ của việc chuyển đổi là kích thước thông báo tăng lên 33%
  - Nhưng có thao tác nén bù lại

B.ng chuy.n đ.i cơ s. 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 c.a PGP

- Các giao th.c thư đi.n t. thư.ng h.n ch. đ. dài t.i đa c.a thông báo
  - Ví d. thư.ng là 50 KB
- PGP phân thông báo quá l.n thành nhi.u thông báo đ. nh.
- Vi.c phân đo.n thông báo th.c hi.n sau t.t c. các công đo.n khác
- Bên nh.n s. ghép các thông báo nh. trư.c khi th.c hi.n các công đo.n khác

Danh tính khóa PGP

- V.i m.t thông báo nh.t đ.nh c.n xác đ.nh s. d.ng khóa nào trong nhi.u khóa công khai / khóa riêng
  - Có th. g.i khóa công khai cùng v.i thông báo nhưng lãng phí đư.ng truy.n không c.n thi.t
- Gán cho m.i khóa m.t danh tính riêng
  - G.m 64 bit bên ph.i c.a khóa
  - Xác su.t cao là m.i khóa có m.t danh tính duy nh.t
- S. d.ng danh tính khóa trong ch. ký

Qu.n lý khóa PGP

- Thay vì d.a trên các CA (cơ quan ch.ng th.c), đ.i v.i PGP m.i ngư.i dùng là m.t CA
  - Có th. ch.ng th.c cho nh.ng ngư.i dùng quen bi.t
- T.o nên m.t m.ng lư.i tin c.y
  - Tin các khóa đã đư.c ch.ng th.c
- M.i khóa có m.t ch. s. tin c.y
- Ngư.i dùng có th. thu h.i khóa c.a b.n thân

S/MIME

- Nâng c.p t. chu.n khuôn d.ng thư đi.n t. MIME có thêm tính năng an toàn thông tin
- MIME kh.c ph.c nh.ng h.n ch. c.a SMTP (Simple Mail Transfer Protocol)
  - Không truy.n đư.c file nh. phân (chương trình, .nh,...)
  - Ch. g.i đư.c các ký t. ASCII 7 bit
  - Không nh.n thông báo vư.t quá kích thư.c cho phép
  - ...
- S/MIME có xu hư.ng tr. thành chu.n công nghi.p s. d.ng trong thương m.i và hành chính
  - PGP dùng cho cá nhân

Các ch.c năng c.a S/MIME

- Bao b.c d. li.u
  - Mã hóa n.i dung thông báo và các khóa liên quan
- Ký d. li.u
  - Ch. ký s. t.o thành nh. mã hóa thông tin t.ng h.p thông báo s. d.ng khóa riêng c.a ngư.i ký
  - Thông báo và ch. ký s. đư.c chuy.n đ.i cơ s. 64
- Ký và đ. nguyên d. li.u
  - Ch. ch. ký s. đư.c chuy.n đ.i cơ s. 64
- Ký và bao b.c d. li.u
  - K.t h.p ký và bao b.c d. li.u

X. lý ch.ng th.c S/MIME

- S/MIME s. d.ng các ch.ng th.c khóa công khai theo X.509 v3
- Phương th.c qu.n lý khóa lai ghép gi.a c.u trúc phân c.p CA theo đúng X.509 và m.ng lư.i tin c.y c.a PGP
- M.i ngư.i dùng có m.t danh sách các khóa c.a b.n thân, danh sách các khóa tin c.y và danh sách thu h.i ch.ng th.c
- Ch.ng th.c ph.i đư.c ký b.i CA tin c.y