CHƯƠNG 04
CÁC GIẢI THUẬT MÃ HÓA DỮ LIỆU BẤT ĐỐI XỨNG

TS. Lê Quang Minh
quangminh@vnu.edu.vn

Nội Dung

- Số nguyên tố
- Hệ mã hoá khoá công khai
- Giao thức trao đổi khoá Diffie-Hellman
- RSA
- Quản lý khoá

Nội Dung

- **Số nguyên tố**
- Hệ mã hoá khoá công khai
- Giao thức trao đổi khoá Diffie-Hellman
- RSA
- Quản lý khoá

Số nguyên tố
Giới thiệu

quangminh@vnu.edu.vn

- Bất kỳ số nguyên a > 1 đều có thể viết dưới dạng:

  $a = p_1^{a1} p_2^{a2} p_3^{a3} \ldots p_t^{at}$

  - Trong đó $p_1 < p_2 < \ldots < p_t$ là các số nguyên tố.

- Ví dụ:

  $85 = 5 \times 17$

  $91 = 7 \times 13$

  $1200 = 2^4 \times 3 \times 5^2$

  $11011 = 7 \times 11^2 \times 13$

Số nguyên tố
Giới thiệu

- Một số nguyên p> 1 là số nguyên tố nếu và chỉ nếu ước duy nhất của nó là ± 1 và ± p.
- Bảng dưới đây trình bày các số nguyên tố nhỏ hơn 2000

2	101	211	307	401	503	601	701	809	907	1009	1103	1201	1301	1409	1511	1601	1709	1801	1901
3	103	223	311	409	509	607	709	811	911	1013	1109	1213	1303	1423	1523	1607	1721	1811	1907
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319	1429	1543	1613	1733	1831	1931
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
13	127	239	337	433	547	631	739	829	941	1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
29	149	263	359	457	571	653	761	859	971	1061	1181	1277	1381	1459	1579	1663	1783	1877	1987
31	151	269	367	461	577	659	769	863	977	1063	1187	1279	1399	1471	1583	1667	1787	1879	1993
37	157	271	373	463	587	661	773	877	983	1069	1193	1283		1481	1597	1669	1789	1889	1997
41	163	277	379	467	593	673	787	881	991	1087		1289		1483		1693			1999
43	167	281	383	479	599	677	797	883	997	1091		1291		1487		1697			
47	173	283	389	487		683		887		1093		1297		1489		1699			
53	179	293	397	491		691				1097				1493					
59	181			499										1499					
61	191																		
67	193																		
71	197																		
73	199																		
79																			
83																			
89																			
97																			

Nội Dung

- Số nguyên tố
- **Hệ mã hoá khoá công khai**
- Giao thức trao đổi khoá Diffie-Hellman
- RSA
- Quản lý khoá

Hệ mã hoá khoá công khai

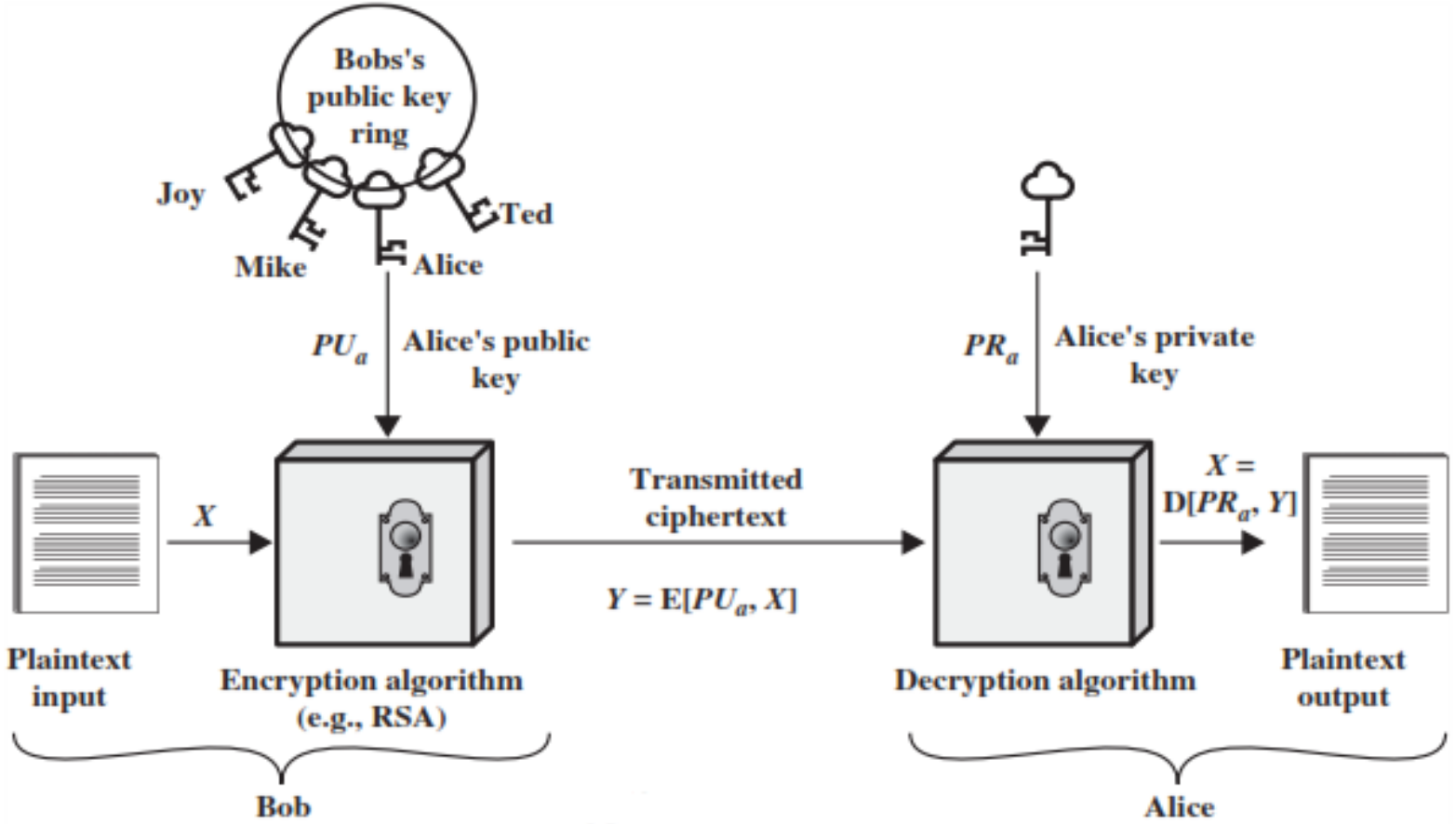
- **Mã hóa bất đối xứng** là cơ chế mã hóa và giải mã sử dụng 2 key khác nhau
  - **Public Key :** là key dùng để mã hóa
  - **Private Key :** là key dùng để giải hóa

- **Mã hóa bất đối xứng** còn được sử dụng để tạo ra **chữ ký điện tử**

Hệ mã hoá khoá công khai

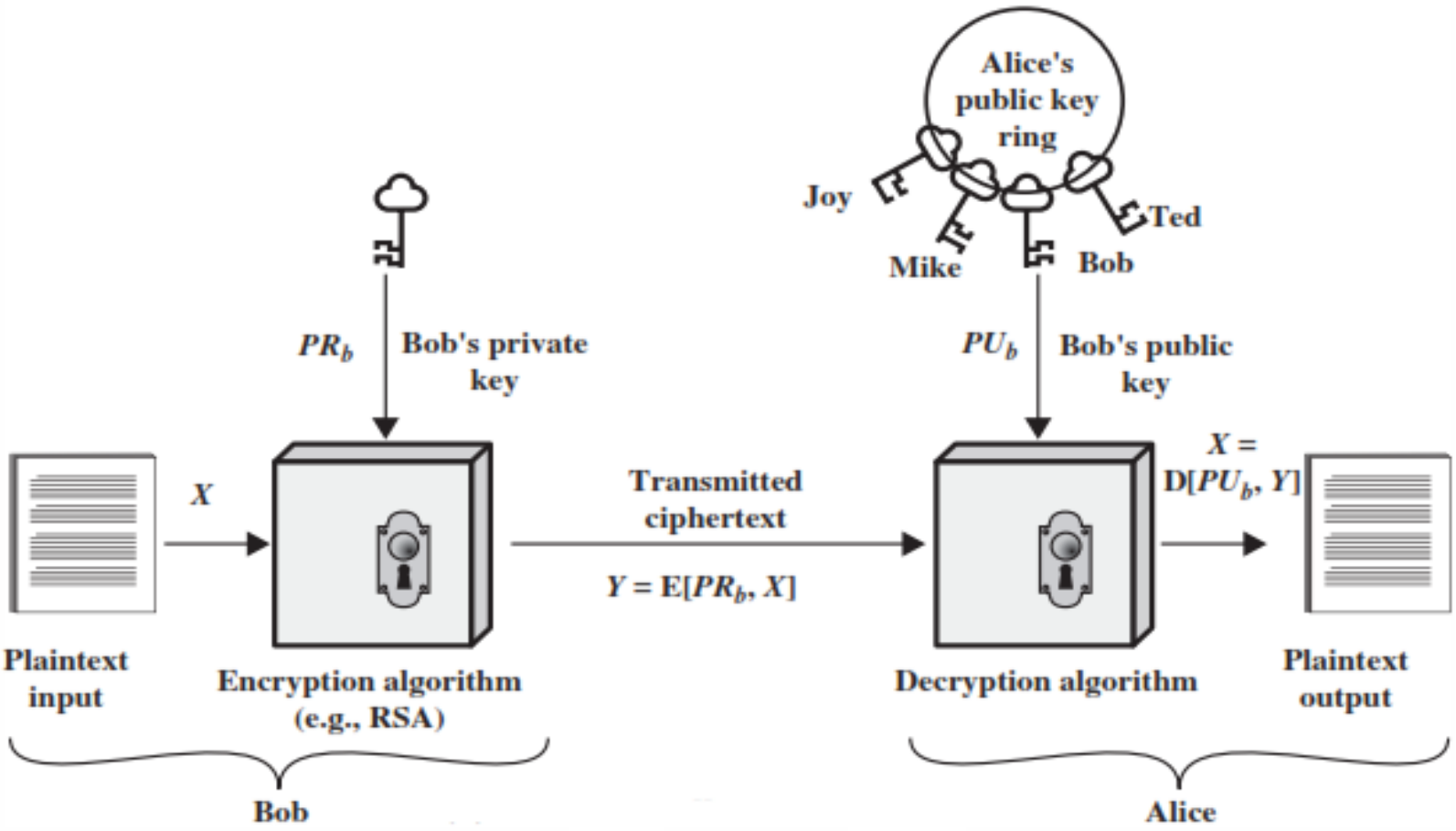
quangminh@vnu.edu.vn

- Mã hóa với Public Key



Hệ mã hoá khoá công khai

- Mã hóa với Private Key



Hệ mã hoá khoá công khai

quangminh@vnu.edu.vn

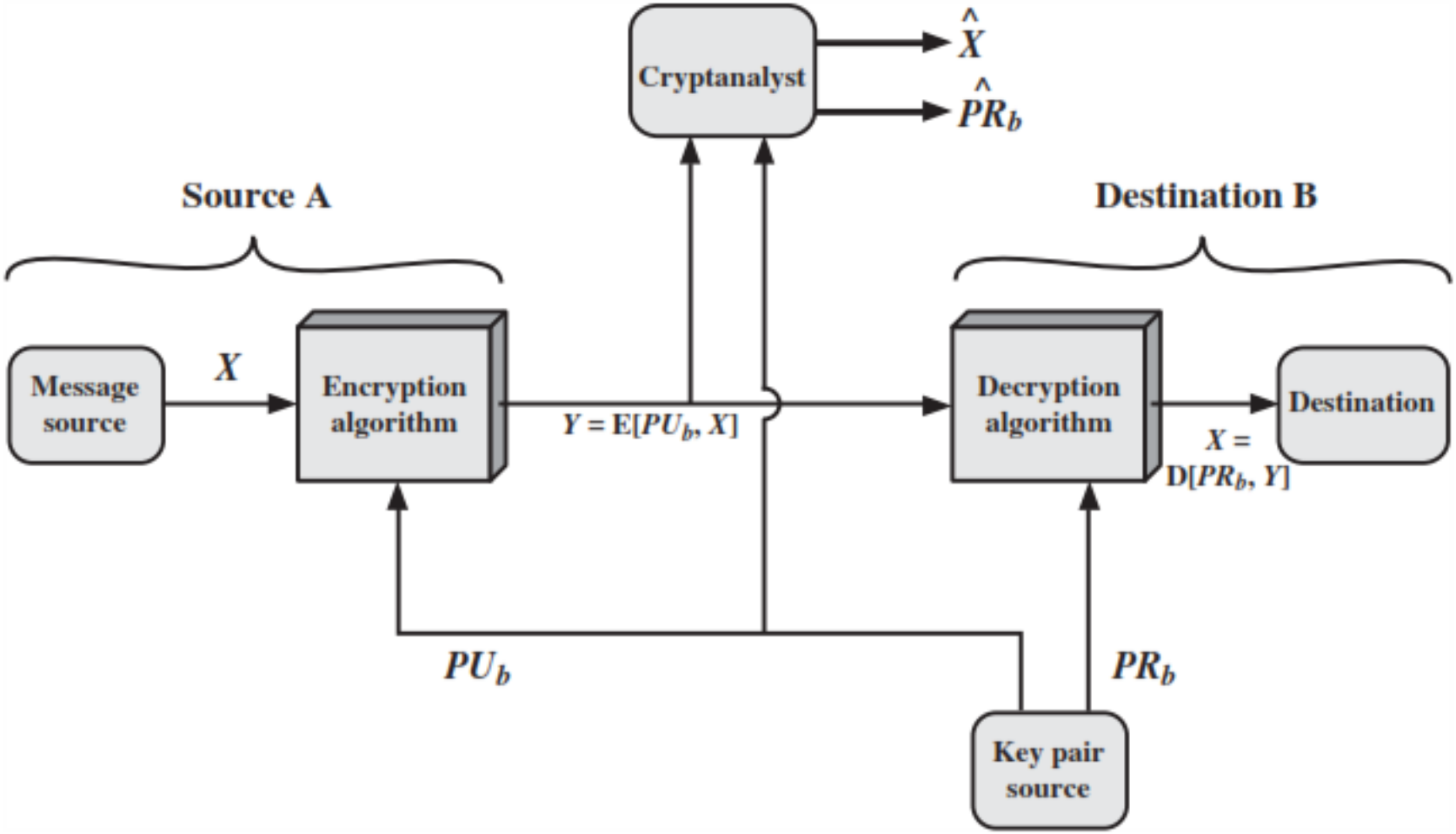
- Mỗi user tạo ra một cặp khoá được sử dụng cho việc mã hoá và giải mã thông điệp.
- Mỗi user đặt một trong hai khoá trong một đăng ký công cộng. Đây là khoá công khai. Khoá còn lại được giữ kín.
- Nếu Bob muốn gửi một tin nhắn bí mật cho Alice, Bob mã hoá tin nhắn này bằng cách sử dụng khoá công khai của Alice.
- Khi Alice nhận được tin nhắn, cô giải mã nó bằng cách sử dụng khoá riêng của mình. Không có ai khác có thể giải mã thông điệp bởi vì chỉ có Alice biết khoá riêng của Alice

Hệ mã hoá khoá công khai

- Ứng dụng thông dụng nhất của mật mã hoá khoá công khai là **bảo mật** (mã hoá/giải mã): một văn bản được mã hoá bằng **khoá công khai** của một người sử dụng thì chỉ có thể giải mã với **khoá bí mật** của người đó.
- Ứng dụng khác của mật mã hóa khóa công khai là dùng để chứng thực: Một người sử dụng có thể mã hoá văn bản với khoá bí mật của mình. Nếu một người khác có thể giải mã với **khoá công khai** của người gửi thì có thể tin rằng văn bản thực sự xuất phát từ người gắn với khoá công khai đó.

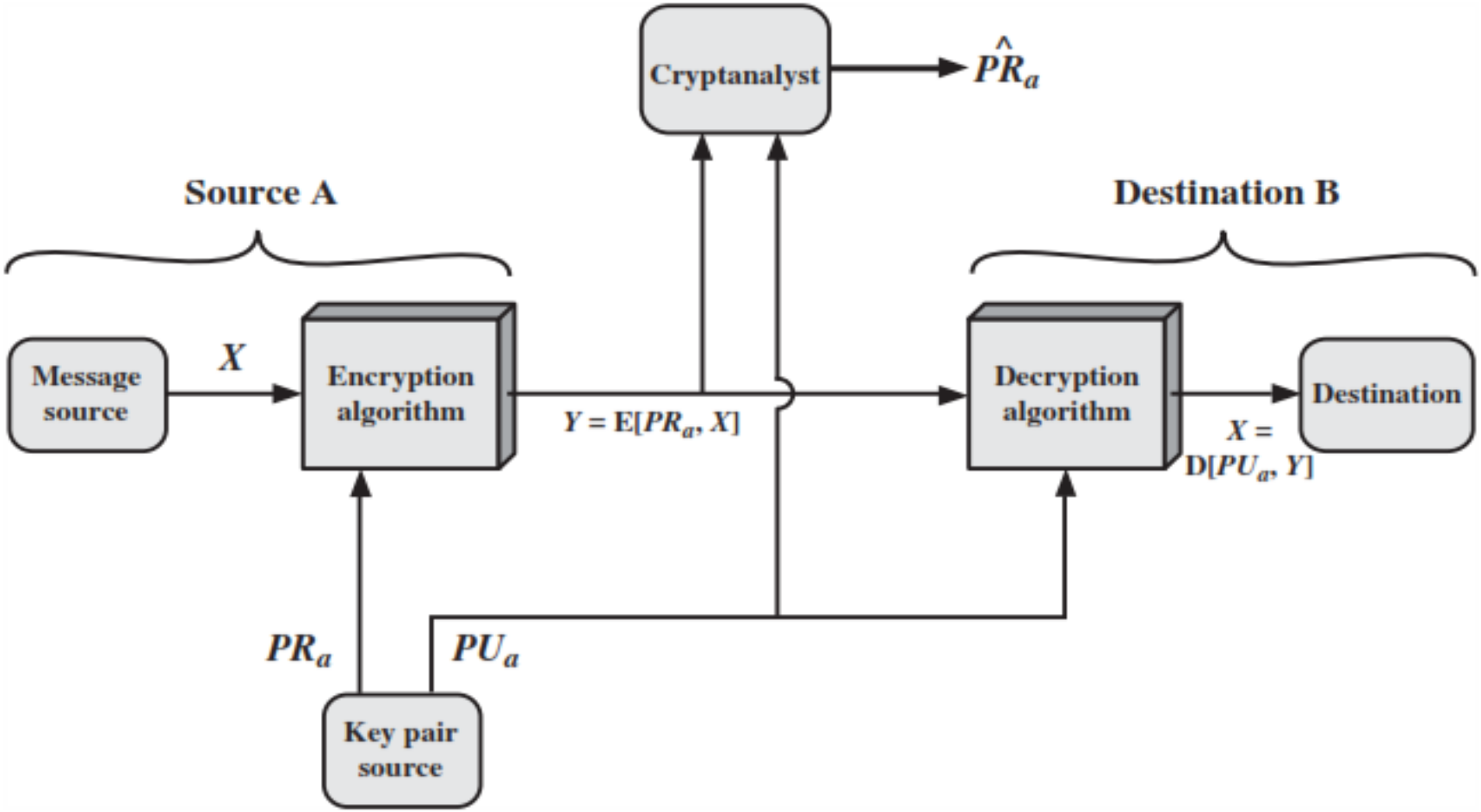
Hệ mã hoá khoá công khai
Ứng dụng: bảo mật dữ liệu

quangminh@vnu.edu.vn



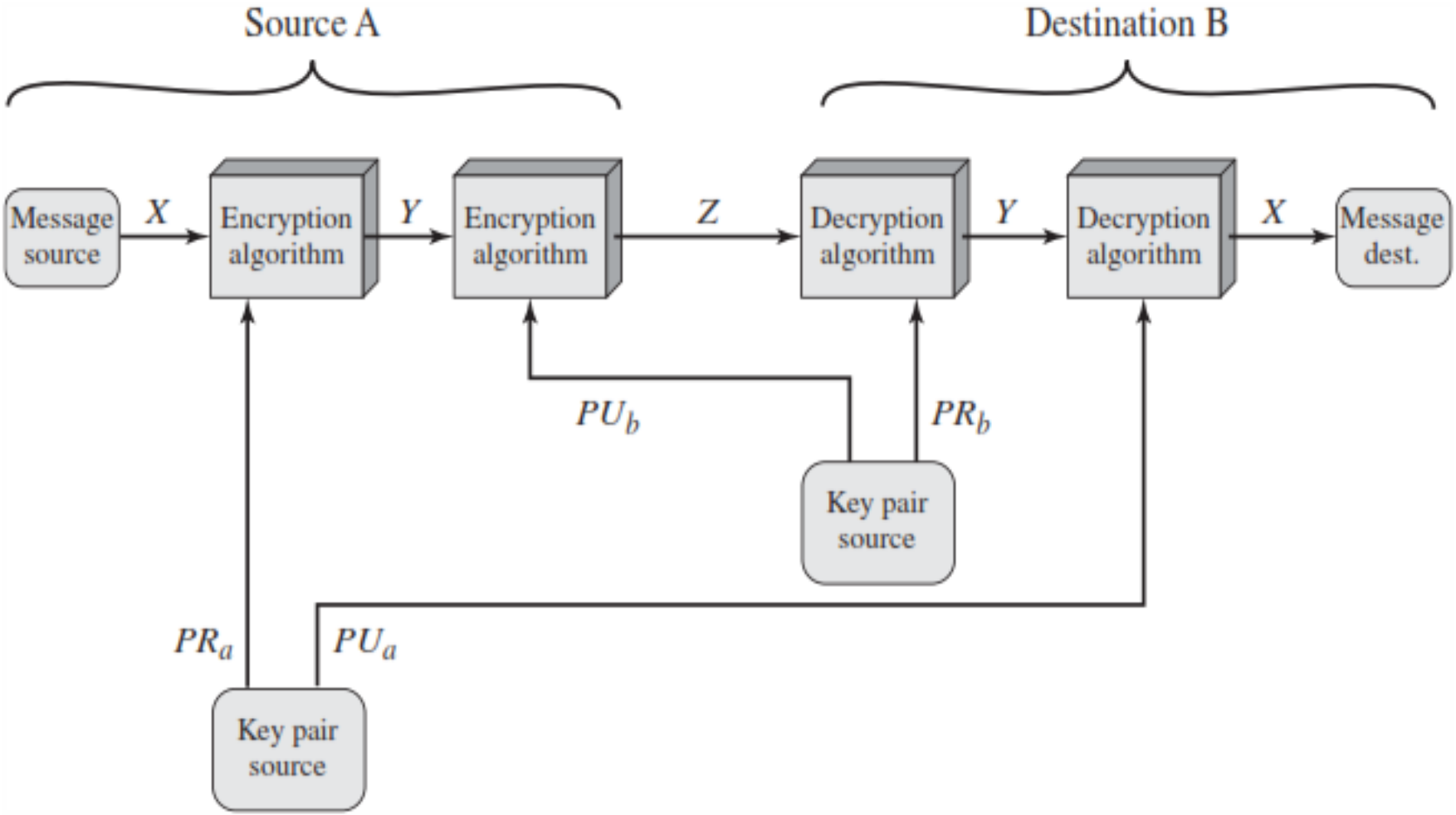
Hệ mã hoá khoá công khai
Ứng dụng: xác thực dữ liệu

quangminh@vnu.edu.vn



Hệ mã hoá khoá công khai
Ứng dụng: bảo mật và xác thực dữ liệu

quangminh@vnu.edu.vn



Hệ mã hoá khoá công khai

- Chúng ta có thể thấy mục đích của hệ thống mã hóa công khai được được nhóm lại trong 3 thể loại sau:
  - **Encryption /decryption**
  - **Digital signature**
  - **Key exchange**

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

Nội Dung

- Số nguyên tố
- Hệ mã hoá khoá công khai
- **Giao thức trao đổi khoá Diffie-Hellman**
- RSA
- Quản lý khoá

Giao thức trao đổi khoá Diffie-Hellman

- Mục đích của thuật toán là cho phép hai người dùng trao đổi khóa bí mật dùng chung trên mạng công cộng, sau đó có thể sử dụng để mã hóa các thông điệp.
- Thuật toán tập trung vào giới hạn việc trao đổi các giá trị bí mật, xây dựng dựa trên bài toán khó logarit rời rạc.

Giao thức trao đổi khoá Diffie-Hellman

- Giao thức trao đổi khoá giữa A và B:
  - A và B thống nhất chọn chung một số nguyên tố p và một phần tử sinh g.
  - A chọn ngẫu nhiên một số $X_A \in \{1, 2, ..., p-1\}$ rồi gởi cho B kết quả $Y_A = g^{XA} \bmod p$.
  - B chọn ngẫu nhiên một số $X_B \in \{1, 2, ..., p-1\}$ rồi gởi cho A kết quả $Y_B = g^{XB} \bmod p$.
  - A tính khoá bí mật: $K=(g^{XB})^{XA} \bmod p = g^{XAXB} \bmod p$
  - B tính khoá bí mật: $K=(g^{XA})^{XB} \bmod p = g^{XAXB} \bmod p$

Diffie-Hellman Key Exchange

Alice

Bob and Alice know and have the following :
$p = 23$ *(a prime number)* $g = 11$ *(a generator)*

Bob

Alice	Bob
Alice chooses a secret random number a = 6	Bob chooses a secret random number b = 5
Alice computes : $A = g^a \bmod p$ $A = 11^6 \bmod 23 = 9$	Bob computes : $B = g^b \bmod p$ $B = 11^5 \bmod 23 = 5$
Alice receives B = 5 from Bob	**Bob receives A = 9 from Alice**
Secret Key = $K = B^a \bmod p$	Secret Key = $K = A^b \bmod p$
$K = 5^6 \bmod 23 = 8$	$K = 9^5 \bmod 23 = 8$

The common secret key is : 8

N.B. We could also have written : $K = g^{ab} \bmod$

Giao thức trao đổi khoá Diffie-Hellman

- Giả sử Alice và Bob đồng ý sử dụng:
  - p = 47 and g = 5
- Alice chọn một số ngẫu nhiên X_A giữa 0 và 46
  - a = 18
- Bob chọn một số ngẫu nhiên X_B giữa 0 và 46
  - b = 22
- Alice tính toán Y_A và gởi kết quả cho Bob.
  - Y_A = 5^18 (mod 47) = 2
- Bob tính toán Y_B và gởi kết quả cho Alice
  - Y_B = 5^22 (mod 47) = 28

Giao thức trao đổi khoá Diffie-Hellman

- Alice tính toán khóa bí mật:
  - $K = Y_B$^a (mod p) = 28^18 (mod 47) = 24
- Bob tính toán khóa bí mật
  - $K = Y_A$^b (mod p) = 2^22 (mod 47) = 24

Nội Dung

- Số nguyên tố
- Hệ mã hoá khoá công khai
- Giao thức trao đổi khoá Diffie-Hellman
- **RSA**
- Quản lý khoá

RSA

- Giải thuật được phát triển bởi Rivest, Shamir và Adleman này sử dụng một biểu thức với hàm mũ.
- Văn bản gốc được mã hóa ở dạng khối, kích cỡ của khối phải nhỏ hơn hoặc bằng $\log_2(n)$.
- Trong thực tế, kích thước khối là i bit, với $2^i < n <= 2^{i+1}$.
- Mã hóa và giải mã được thực hiện với một số khối rõ M (plaintext) và khối mã C (cyphertext):

$C = M^e \bmod n$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

RSA

Giới thiệu

- Giải thuật được phát triển bởi Rivest, Shamir và Adleman này sử dụng một biểu thức với hàm mũ.
- Văn bản gốc được mã hóa ở dạng khối, kích cỡ của khối phải nhỏ hơn hoặc bằng $\log_2(n)$.
- Trong thực tế, kích thước khối là i bit, với $2^i < n <= 2^{i+1}$.
- Mã hóa và giải mã được thực hiện với một số khối rõ M (plaintext) và khối mã C (cyphertext):

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

RSA

Quá trình tạo Public/Private Key

- Chọn ngẫu nhiên 2 số nguyên tố lớn - p, q
- Tính N=p.q
  - ø(N)=(p-1)(q-1)
- Chọn ngẫu nhiên giá trị e (encryption key)
  - where 1<e<ø(N), gcd(e,ø(N))=1
- Tính toán d (decryption key)
  - (e.d) mod ø(N) =1 and 0≤d≤N
- Public key: **KU={e,N}**
- Private key: **KR={d,N}**

RSA
Ứng dụng RSA trong mã hóa/giải mã

- Để mã hóa M, người gởi:
  - Lấy **public key** của người nhận KU={e,N}
  - Tính toán: $C=M^e \bmod N$, where $0 \le M < N$
- Để giải mã C, người nhận:
  - Sử dụng **private key** của mình KR={d,N}
  - Tính toán: $M=C^d \bmod N$

RSA
Ví dụ

1. Select primes: p=17 & q=11
2. Compute $n = pq$ =17×11=187
3. Compute ø(n)=(p–1)(q-1)=16×10=160
4. Select e *:* gcd(e,160)=1; choose e=7
5. Determine d*: (de)* mod 160 = 1 and d < 160
   Value is d=23 since 23×7=161= 1×160+1
6. Publish public key KU={7,187}
7. Keep secret private key KR={23,187}

RSA
Ví dụ

- RSA encryption/decryption is:
  - M = 88 (88<187)
- Mã hóa:
  - $C = 88^7 \bmod 187 = 11$
- Giải mã:
  - $M = 11^{23} \bmod 187 = 88$

RSA

Những cặp khóa tham khảo

p prime	q prime	n=(p*q)	m = (p-1)* (q-1)	e (prime)	Calc. 'd'	Private (n, d)	Public (n, e)	x	ed-xm
5	3	15	8	11	3	(15,3)	(15,11)	4	1
7	5	35	24	11	11	(35,11)	(35,11)	5	1
13	17	221	192	11	35	(221,35)	(221,11)	2	1
17	23	391	352	5	141	(391,141)	(391,5)	2	1
17	23	391	352	7	151	(391,151)	(391,7)	3	1
17	23	391	352	13	325	(391,325)	(391,13)	12	1
17	23	391	352	29	85	(391,85)	(391,29)	7	1
17	23	391	352	31	159	(391,159)	(391,31)	14	1
17	23	391	352	37	333	(391,333)	(391,37)	35	1
17	23	391	352	19	315	(391,315)	(391,19)	17	1

Nội Dung

- Số nguyên tố
- Hệ mã hoá khoá công khai
- Giao thức trao đổi khoá Diffie-Hellman
- RSA
- **Quản lý khoá**

Quản lý khoá
Thu hồi khóa

- Thu hồi khoá khi khoá bị sai sót hoặc có tính phá hoại.
- Thường được tham gia bởi từ hai thực thể trở lên. Ví dụ: cả Alice và Bob cùng thoả thuận thu hồi khoá.
- Cần đảm bảo:
  - Càng nhiều bên tham gia càng tốt (chống phá hoại).
  - Càng ít bên tham gia càng tốt (thu hồi nhanh).

Quản lý khoá
Phân phối khóa mới

- Phải phân phối khoá mới sau khi khoá cũ bị thu hồi nhằm đảm bảo hệ thống tiếp tục hoạt động một cách an toàn.
- Cần giảm thời gian giữa thời điểm thu hồi khoá và thời điểm phân phối khoá mới tới mức tối thiểu.
- Phải đảm bảo yêu cầu về an ninh và yêu cầu về tính sẵn sàng của hệ thống.

Quản lý khoá

Thông báo thông tin về thu hồi khoá

- Thông báo về một khóa nào đó bị thu hồi cần đến được tất cả những người đang sử dụng nó trong thời gian ngắn nhất có thể.
- Hai cách:
  - Thông tin được chuyển từ trung tâm tới người dùng.
  - Người dùng lấy thông tin từ trung tâm.
- Cung cấp các chứng thực có thời hạn

Quản lý khoá
Thông báo thông tin về thu hồi khoá

- Hầu hết các trường hợp thu hồi khoá xảy ra khi khoá bí mật đã bị lộ. Hai khả năng xảy ra:
  - Các văn bản mã hóa với khóa công khai sau thời điểm T không còn được xem là bí mật.
  - các chữ ký số thực hiện với khóa bí mật sau thời điểm T không còn được xem là thật.
- Cần xác định người có quyền thu hồi khóa, cách thức truyền thông tin tới người dùng, cách thức xử lý các văn bản mã hóa với khóa bị lộ.

Question ???