UNIVERSITÄT DUISBURG ESSEN

introduction to public key cryptography

A.J. Han Vinck

University of Duisburg-Essen

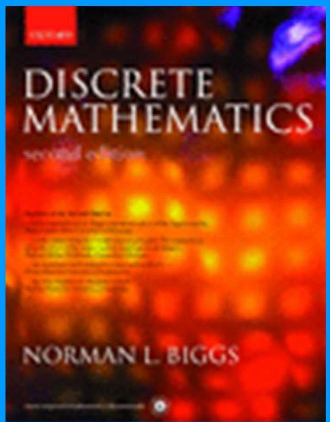
Last changes, May 12, 2012

Vinck@iem.uni-essen.de

content

- Public key formalisms
- Diffie Hellman key exchange
- Pohlig-Hellman a-symmetric encryption
- El-Gamal public key
- RSA

- Book: Norman L. Biggs, Discrete Mathematics, Oxford science publications.



Important principle

- One way function
  - Given X, easy to calculate $Y = F(X)$
  - Given Y it is „hard“ to find $X = F^{-1}(Y)$

    but „easy“ with special info (trapdoor)

$$Y = X^2$$

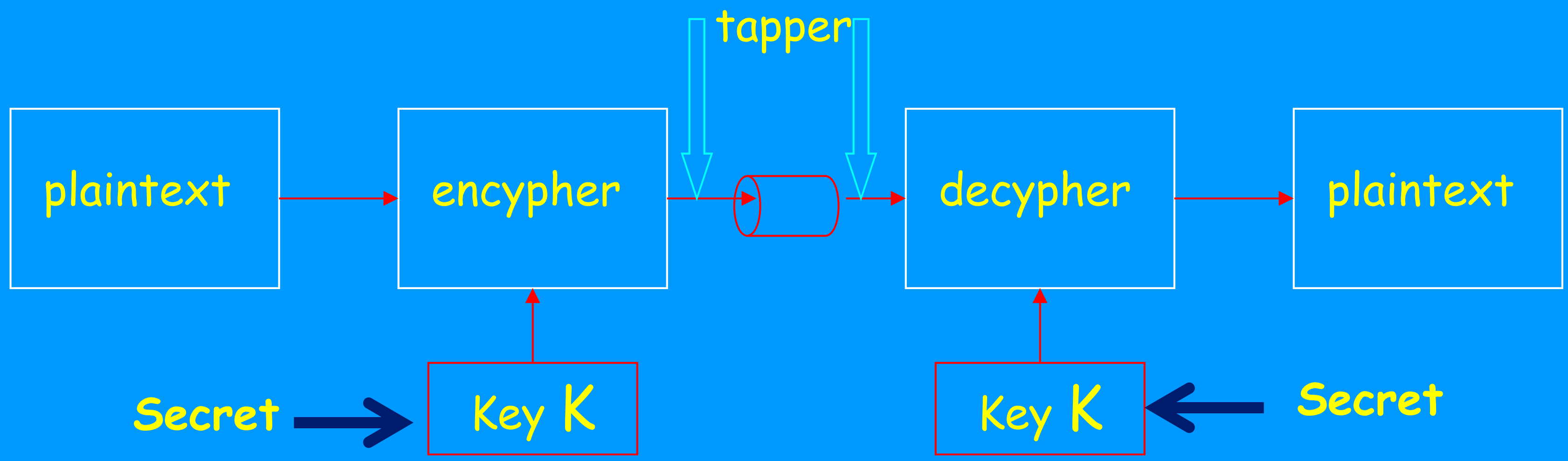
$$X = \sqrt{Y}$$

- Example: $Y = a^X$;

  $N = pq$; p and q large prime numbers

  $Y = X^2$

The classical „one-key“ system

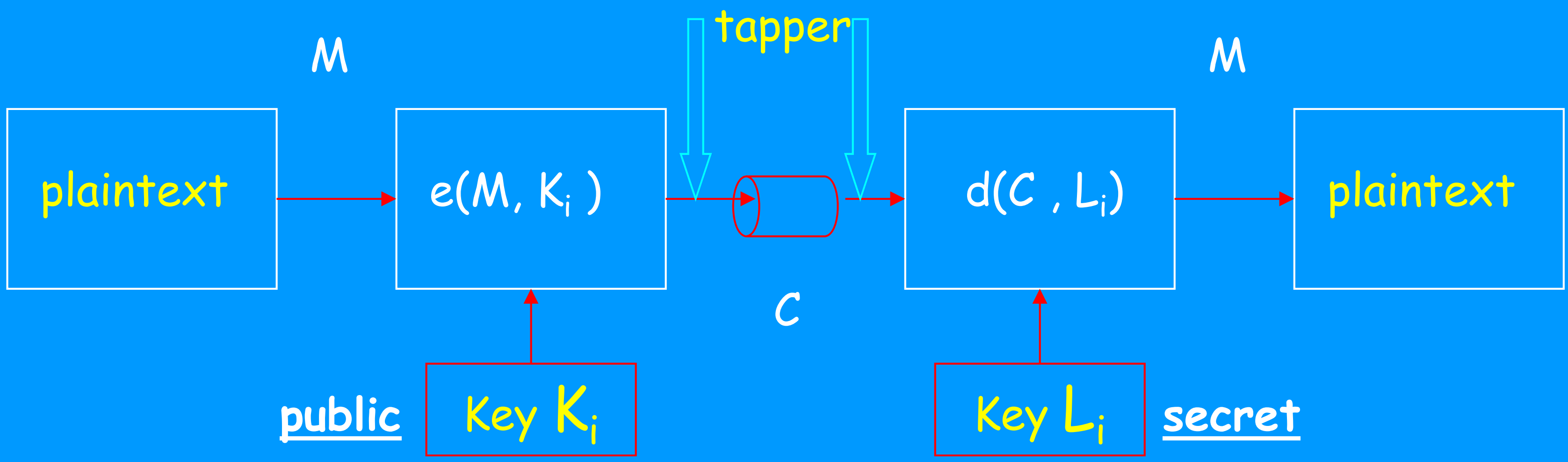


Secret K. System condition $d(e (M, K), K) = M$

Known to the public:

- $e(*,*)$, $d(*,*)$, easy to calculate functions
- from $C = e(M, K)$ and M it is „impossible“ to find K (plaintext-ciphertext attack)

public „only one secret" key: privacy

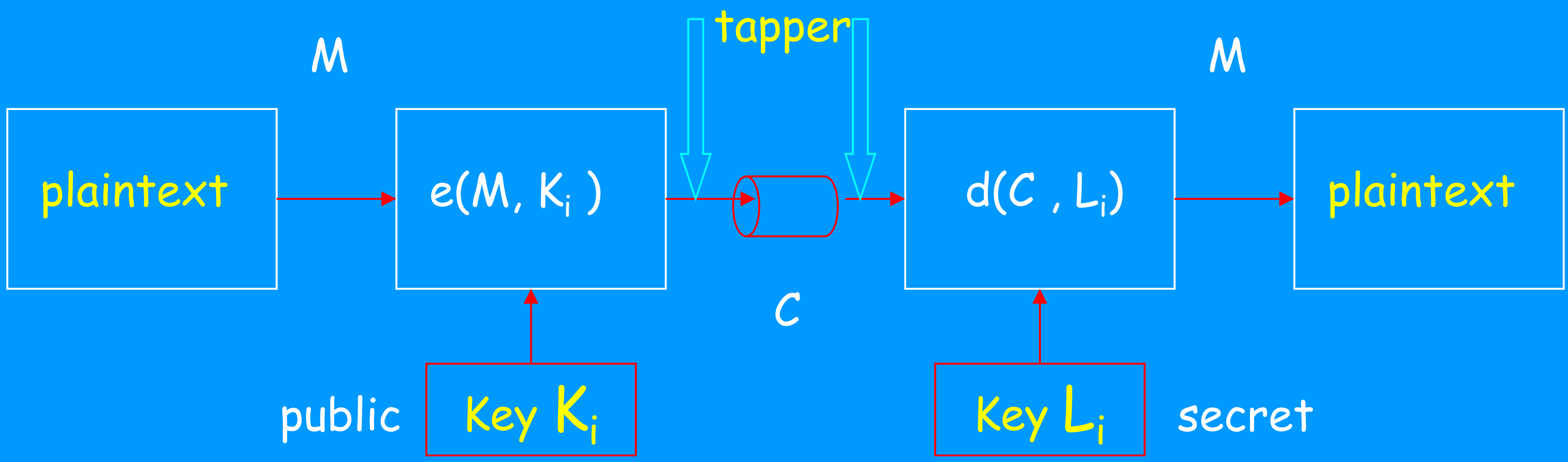


Assumption: from $C = e(M, K_i)$ and K_i it is impossible to find M and L_i

CONSEQUENCE:

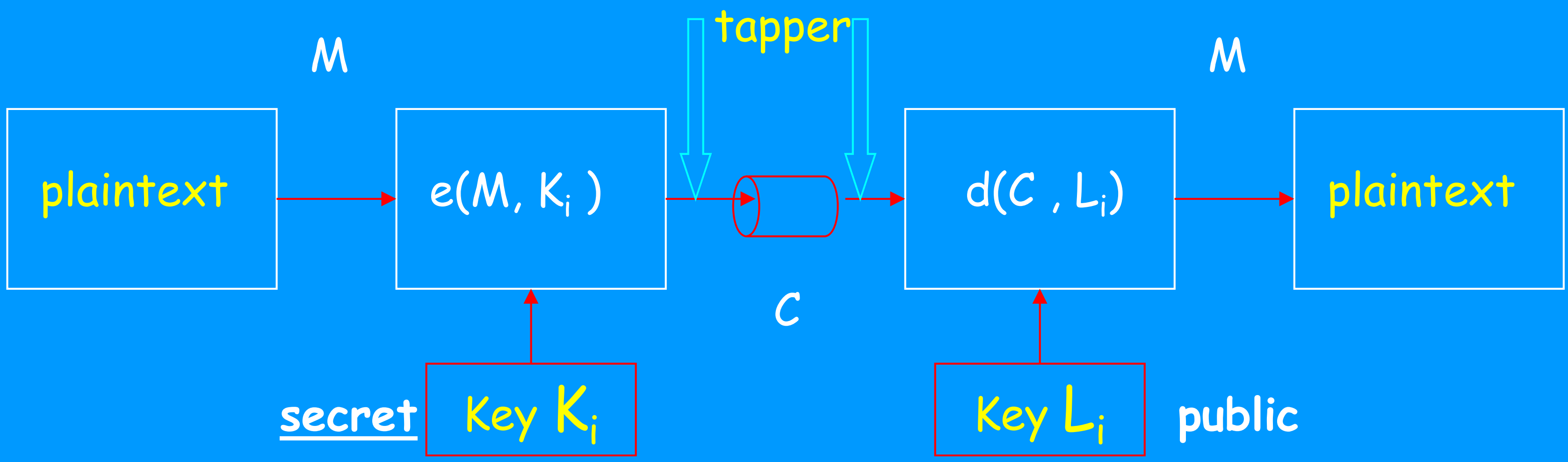
with the *public* key K_i we can send a secret message only decryptable with the *secret* key L_i

public „only one secret“ key: privacy



NOTE: $C = e(M,K_i)$

Public: only one secret key: signature



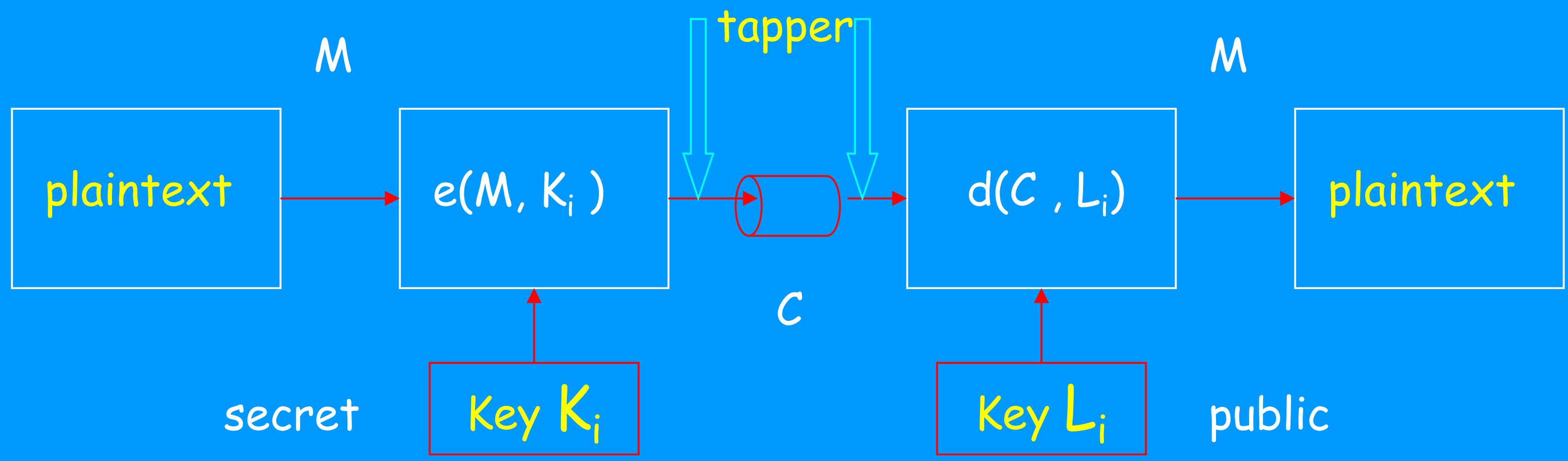
Assumption: from $M = d(C, L_i)$ and L_i it is „impossible" to find K_i

CONSEQUENCE:

with the *secret* key K_i we can sign a message only

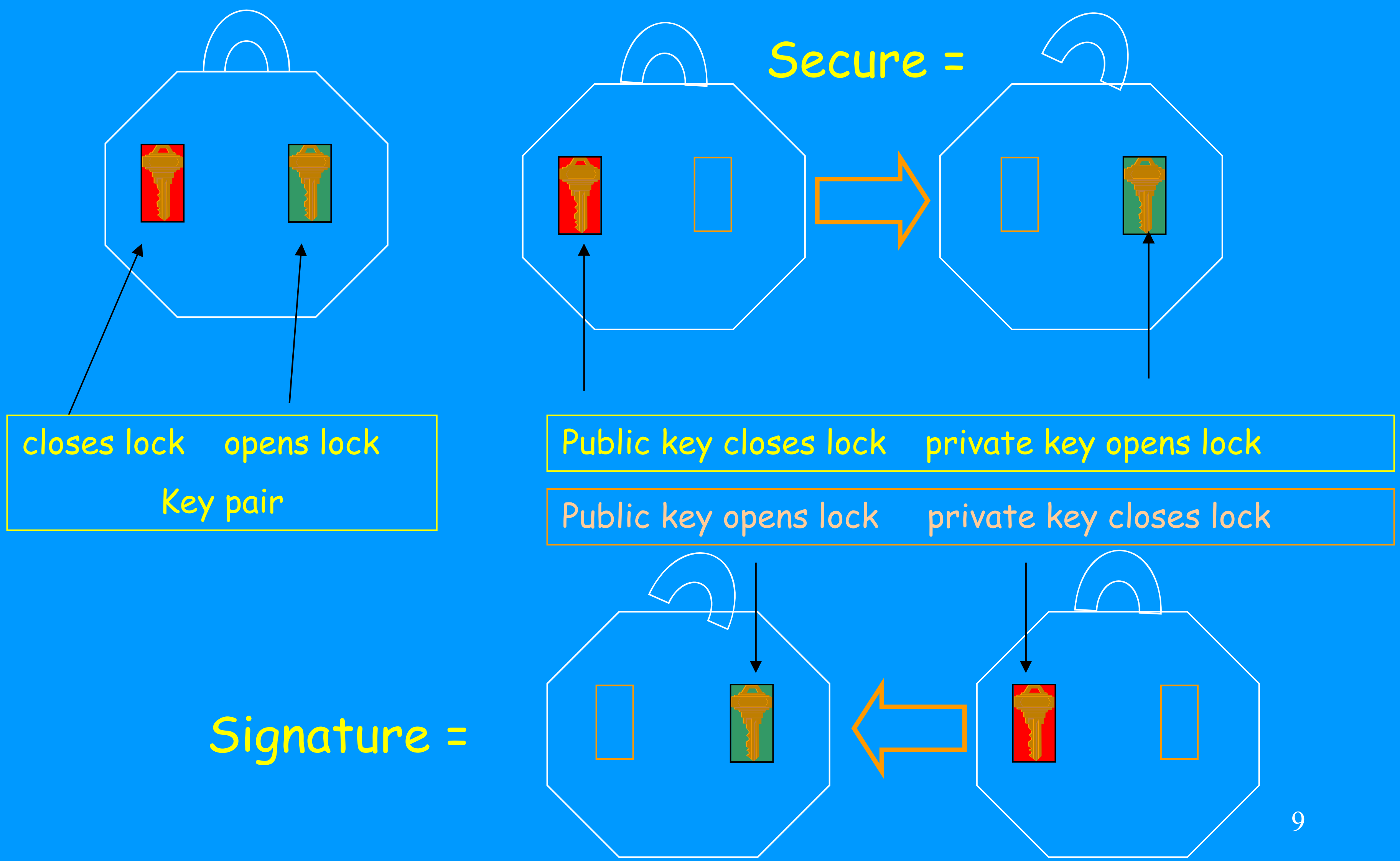
decryptable with the *public* key L_i

Public: only one secret key: privacy



NOTE: $M = d(C,L_i)$

Special lock: visualization (any other idea?)



- 3 famous crypto scientists

Martin Hellman Whitfield Diffie. Merkle, Ralph C

Patent 1977- US4200770: Cryptographic apparatus and method
Hellman, Martin E.; Stanford, CA, **Diffie, Bailey W.**; Berkeley, CA, **Merkle, Ralph C.**; Palo Alto, CA

A patent is automatically invalid if the patented invention was published more than a year before the patent's filing date.
It appears, therefore, that the Diffie-Hellman-Merkle patent was invalid.

- it is used by several protocols, including Secure Sockets Layer (SSL), Secure Shell (SSH),and Internet Protocol Security (IPSec).

- The numbers (prime and primitive element) should be big (> 500 bit)

Diffie-Hellman (based on discrete logarithm problem)

A

common parameters:
- large prime p
- constant $1 < a < p-1$

B

$1 < X(A) < p-1$ Generate <u>secrets</u> $1 < X(B) < p-1$

Exchange the <u>public</u> numbers:

$Y(A) = a^{X(A)}$ modulo p

$Y(B) = a^{X(B)}$ modulo p

calculate: $Y(B)^{X(A)}$ modulo p

$= a^{X(B)\,X(A)}$ modulo p = K !!!

calculate: $Y(A)^{X(B)}$ modulo p

$= a^{X(A)\,X(B)}$ modulo p = K !!!

ASSUMPTION: given X , easy to calculate $Y = a^X$;

given Y , hard to calculate X

Diffie-Hellman (the mathematics behind)

Given: prime p and $1 < a < p-1$

Calculate numbers: $1, a, a^2, a^3, \ldots, a^{p-2}$ modulo p

for a **primitive**, these p-1 numbers **are different**

Example: $p = 7$, $a = 3$:

$[\,1, 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5\,]$ modulo 7

Note: for a **not primitive**: $a^i = a^j \bmod p \Rightarrow a^{i-j} = 1 \bmod p$, $0 \le i, j \le p-2$

Example: $p = 7$, $a = 2$:

$[\,1, 2, 2^2 = 4, 2^3 = 1, 2^4 = 2, 2^5 = 4\,]$ modulo 7

Property of a primitive element (to be remembered)

Given: prime p and $1 < a < p-1$

Assumption: for a **primitive**,

the p-1 numbers $1, a, a^2, a^3, \ldots, a^{p-2}$ modulo p **are different**

Proposition: $a^{p-1} = 1$ modulo p:

- all (p-1) numbers a^i mod p, $0 \le i \le p-2$; are different modulo p
- suppose $a^i = 1$ mod p, $i < p-1$, then $a^{i+1} = a$, which contradicts the assumption

$\rightarrow$ for $1 \le b \le p-1$, $b^{p-1} = (a^i)^{p-1} = (a^{p-1})^i = 1$ mod p Fermat-Euler

$\rightarrow$ $a^{p-1} = (a^{p-1-i})a^i = 1$ mod p; $b := a^{p-1-i} = a^{-i}$ mod p is the inverse of a^i mod p

an example

Given: prime $p = 7$ and $1 < a = 3 < 6$

Calculate numbers: $1, 3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5$ modulo 7

$\rightarrow 3^6 = 1$ modulo 7.

$\rightarrow$ for $1 < 2 < 6$, $2^6 = (3^2)^6 = (3^6)^2 = 1 \mod 7$

$\rightarrow 3^6 = (3^4)\, 3^2 = 1 \mod p$ $\quad b = 3^4 = 3^{-2} \mod p$ is the inverse of $3^2 \mod p$

For $a = 2$: $\quad 1,\ 2,\ 2^2 = 4,\ 2^3 = 1$ modulo 7

Hence, $a = 2$ is not primitive

Example of Diffie Hellman with numbers

Common parameters: prime p = 71 and constant a = 7

Step 1. Generate secrets in A and B: X(A) = 5 ; X(B) = 12

Step 2: exchange the public numbers: Y(A) = 7^5 = 51 modulo 71 → B

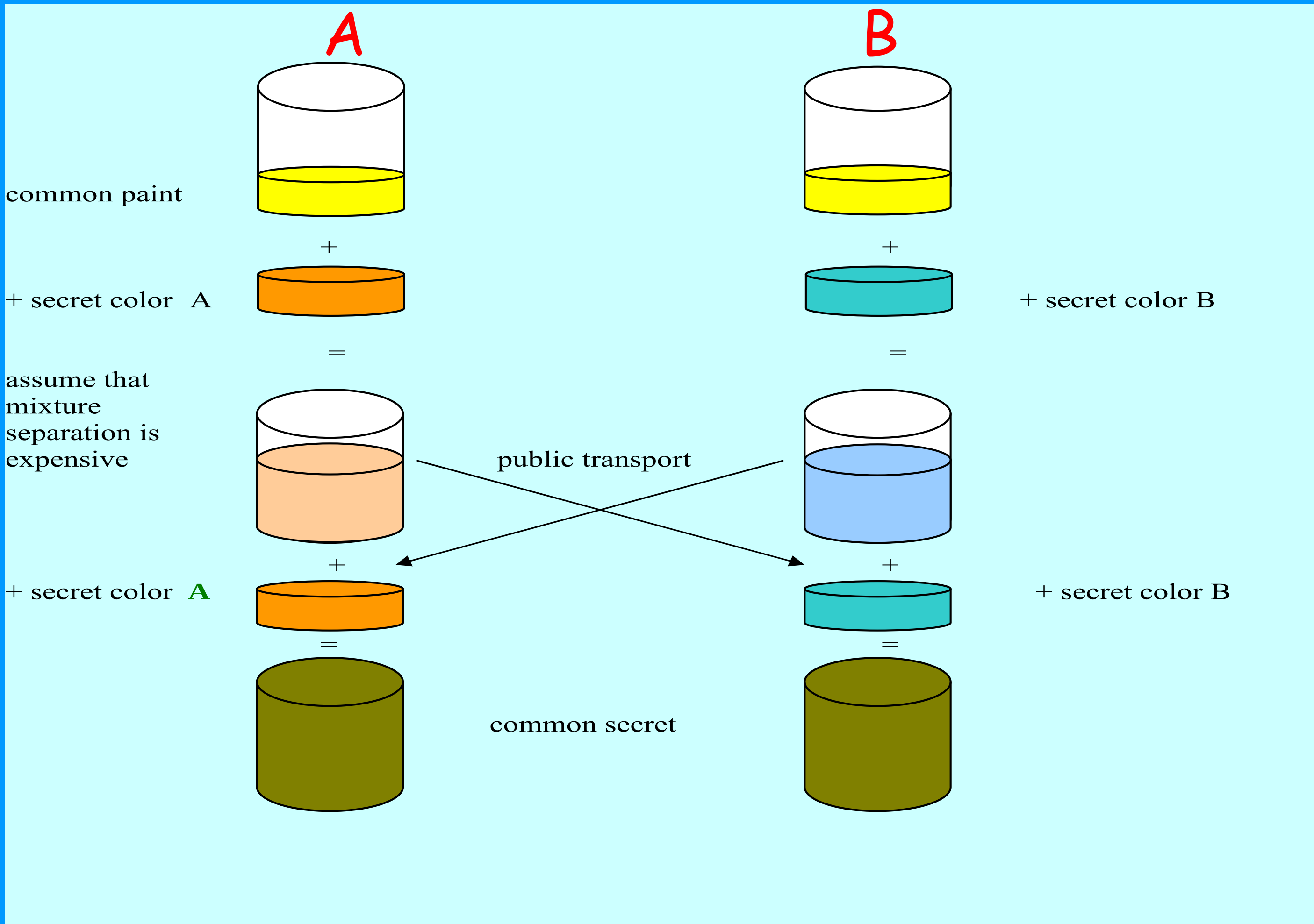
Y(B) = 7^{12} = 4 modulo 71 → A

Step 3: calculate in A: 4^5 modulo 71 = 7^{12*5} modulo 71 = 30 !!!

calculate in B: 51^{12} modulo 71 = 7^{5*12} modulo 71 = 30 !!!

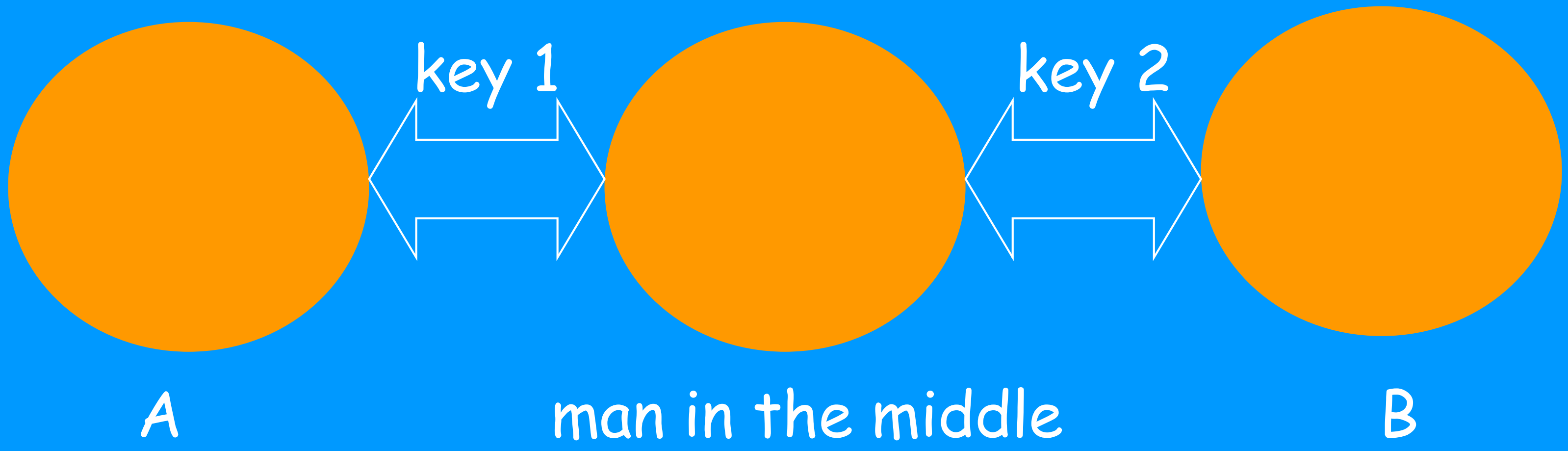
- http://www.youtube.com/watch?v=3QnD2c4Xovk

Diffie-Hellman key exchange (illustration)



Patent 1977- US4200770: Cryptographic apparatus and method

the Man in the middle can be a problem



A and B communicate via the „Man in the Middle"

Security Issues in the D-H Key Agreement Protocol, J-F Raymond and A. Stiglic, December 19, 2000

El Gamal public key

El Gamal:

use Diffie Hellman for key agreement (slow)

classical encryption for message exchange (fast)

El Gamal public key (2)

Step 1: Key exchange

A has public number from B $Y(B)$

A sends to B $Y(A)$

A and B calculate $K = Y(B)^{X(A)}$ modulo p

$K = Y(A)^{X(B)}$ modulo p

Step 2: A transmits $C = K * M$ modulo p

Step 3: B calculates $K^{-1} C = K^{-1} K * M = M$ modulo p

For p prime, gcd(K, p) = 1, and thus K^{-1} can be found .

Note: we need an algorithm to calculate k^{-1} with low complexity

Example for the El Gamal public key (3)

$p = 71, a = 7$

$Y(B) = 3;$ $X(A) = 2$ $K = 9; K^{-1} = 8;$

public key for B secret for A $8 * 9 = 72 = 1 + 71$

encryption of $M = 30$ is

step 1 9 for A and B, common key is 9

step 2 $C = 9 \times 30 \bmod 71 = 57$: from A => B

step 3 $K^{-1} = 8; 8 \times 57 = 456 = 30 \bmod 71$ (in B)

Another hybrid scheme

Step 1: public key K_B from B to A

secret key L_B at B

A $\Leftarrow$ K_B B

Step 2: A generates session key K

A sends $C = e(K, K_B)$ to B

B decrypts $d(C, L_B) = K$

A $\Rightarrow$ C B

$K=d(C, L_B)$

Step 3: K can be used as session K in AES (fast)

Basic property for Pohlig-Hellman (to be remembered)

For integer N and constant $e < N$, s.t. greatest common diviser $(e, N)=1$

there exists an integer d such that $ed = 1$ modulo N

<u>proof</u>: Consider the numbers : $e, 2e, 3e, \ldots, (N-1)e$ modulo N

these $(N - 1)$ numbers are all different and $\neq 0$ modulo N

because - $ke \neq a N$, since $k, e < N$ and $gcd(e, N) = 1$

- $Ie \neq Je$ since otherwise $(Ie - Je) = ke = 0$ modulo N

<u>Conclusion</u>: there exists an integer d such that $de = 1$ modulo N

this is a very basic algorithm to find d (generate all multiples of e until $de = 1$ modulo N).

We will see in the next chapter that it can be faster!

Pohlig-Hellman a-symmetric encryption (1975)

For two constants (e,d) s.t. $ed = 1 + k\,(p-1)$ (Fermat Euler)

($ed = 1$ modulo $(p-1)$ or $\gcd(e, p-1) = 1$)

- Encryption: $C = M^e$ modulo p $M < p$ (rime)

- Decryption: $C^d = M^{ed} = M^{1+k(p-1)} = M\,(M^{k(p-1)}) = M$ modulo p

  follows from Fermat –Euler!

Assumption: from C we cannot find e!

This method in general more complex than symmetric systems, but very close to the following public key system

The famous RSA public key system

RSA: Ron Rivest; Adi Shamir; Leonard Adleman

Use: mathematical problem of factorization

$N = pq$ prime p and q

- to multiply p and q is easy
- to find p and q given N is difficult
- N large (1024 bits), p, q $\approx$ 512 bits

See also: http://www.rsasecurity.com

http://www.youtube.com/watch?v=56fa8Jz-FQQ

RSA (how it works)

<u>Given:</u> secret two large primes p and q

$e < pq$ and $\gcd(e, (p-1)(q-1)) = 1$

<u>Calculate:</u> secret d, s.t. $ed = 1 \text{ modulo } (p-1)(q-1)$

Public key: the pair ($N = pq, e$) Secret key : d

ENCRYPT: $C = M^e \text{ modulo } N$

DECRYPT: $C^d = M^{ed} = M^{1+k(p-1)(q-1)} = M \text{ modulo } pq$

RSA in numbers (how it works)

Given: secret two large primes 47 and 59

$e = 157$ and $\gcd(157, 2668) = 1$

Calculate: secret $d = 17$, s.t. $157*17 = 1$ modulo 2668

Public key: the pair (N = 2773, 157) Secret key : 17

ENCRYPT $M = 920$ as $C = 920^{157}$ modulo 2773

DECRYPT $C^d = M^{ed} = M^{1+k(p-1)(q-1)} = M$ modulo N

Homework: perform the remaining calculations

RSA (show that $M^{ed} = M$ modulo pq)

Given: p, q prime, N = pq; Message $M < pq$

e, d such that $ed = 1 + k(p-1)(q-1)$

Then: $M^{ed} = M^{1+k(p-1)(q-1)} = M\ (M^{p-1})^{k(q-1)} = M$ modulo p (Fermat-Euler)

$M^{ed} = M^{1+k(p-1)(q-1)} = M\ (M^{q-1})^{k(p-1)} = M$ modulo q

$\rightarrow$ p divides ($M^{ed} - M$)

$\rightarrow$ q divides ($M^{ed} - M$)

Since: p and q are different primes,

$\rightarrow$ pq divides ($M^{ed} - M$) BASIS for RSA!

or $M^{ed} = M$ modulo pq

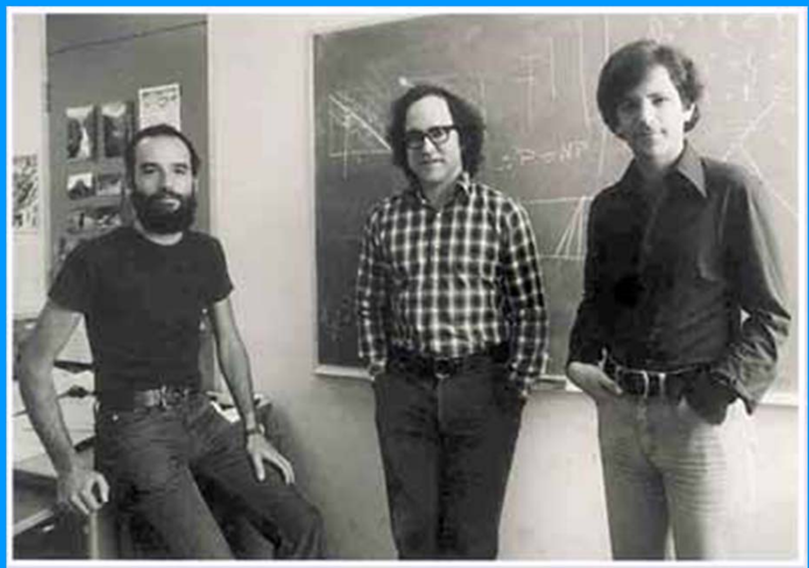
Ron Rivest

Adi Shamir

Len Adleman

- Founders of RSA

RSA SECURITY



History of RSA (from http://en.wikipedia.org/wiki/RSA)

The algorithm was described in 1977 by Ron Rivest, Adi Shamir and Len Adleman at MIT; the letters **RSA** are the initials of their surnames.

Clifford Cocks, a British mathematician working for GCHQ, described an equivalent system in an internal document in 1973. His discovery, however, was not revealed until 1997 due to its top-secret classification.

The algorithm was patented by MIT in 1983 in the United States of America as U.S. Patent 4405829 .

It expired 21 September 2000. Since the algorithm had been published prior to patent application, regulations in much of the rest of the world precluded patents elsewhere. Had Cocks' work been publicly known, a patent in the US would not have been possible either.

RSA (security)

An attack could be based on factoring N into two primes p and q
RSA keys are typically 1024–2048 bits long.

2004: the largest number factored was 174 decimal digits (576 binary bits)
2005: RSA-640 F. Bahr, M. Boehm, J. Franke, T. Kleinjung

The factors [verified by RSA Laboratories] are:

1634733645809253848443133883865090859841783670033092312181110852389333100104508151212118167511579
and
1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571

The effort took approximately 30 2.2GHz-Opteron-CPU years according to the submitters, over five months of calendar time. (This is about half the effort for RSA-200, the 663-bit number that the team factored in 2004.)

The RSA Factoring Challenge is no longer active

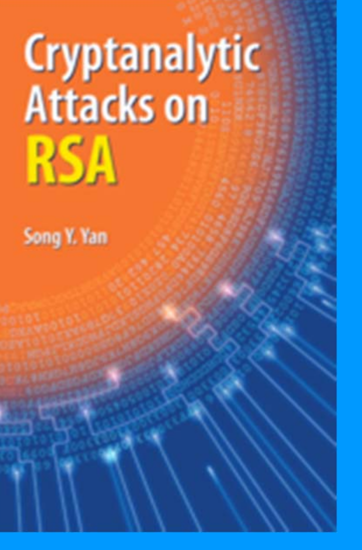
RSA (security)

Attacks can be :

- Mathematical: make use of bad number choices
  - try to factor N

- Technical:
  - timing (exponentiation time differs for different keys);
  - power consumption;
  - hardware errors during computations

- Protocol based
  - use flaws in protocols
  - use different N for all users in a network
    - (e and d together can give the factors of N)

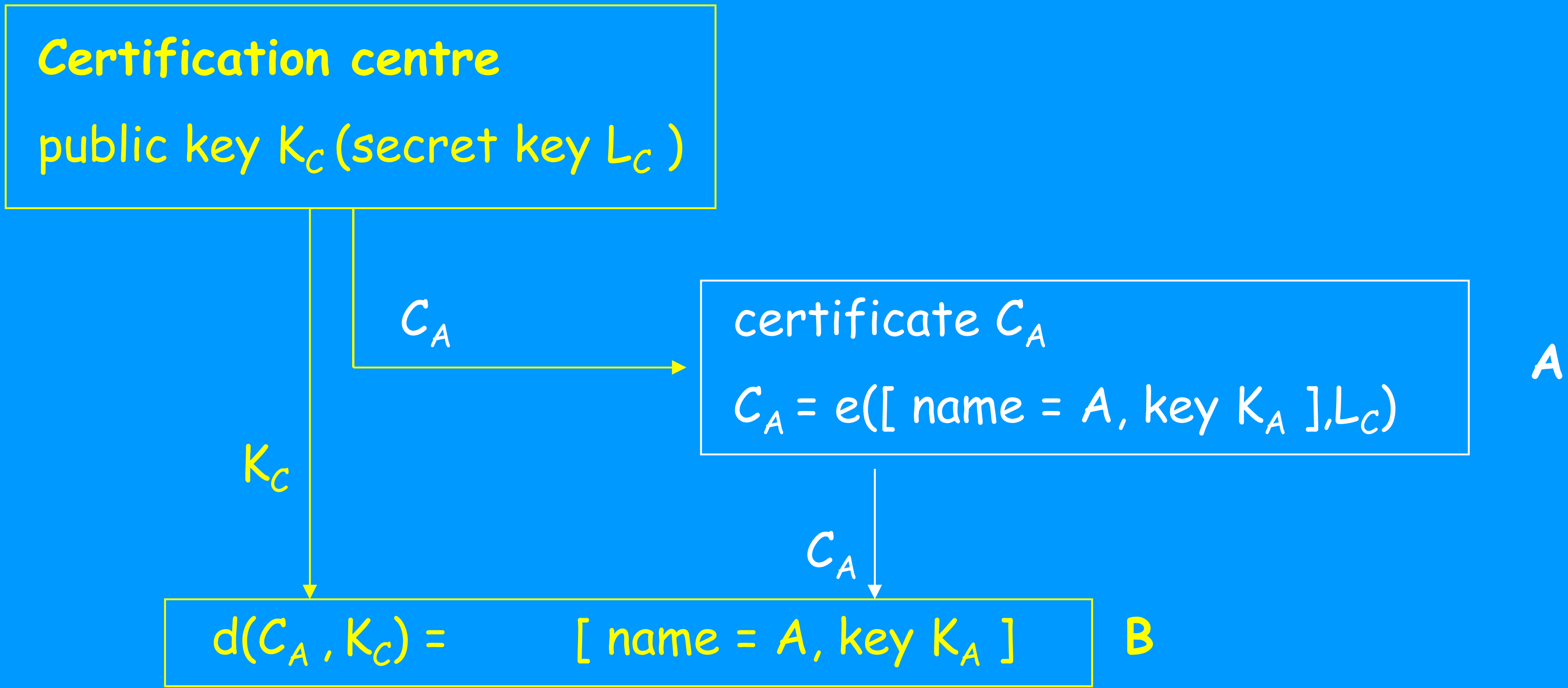


Some facts about prime numbers

- An integer > 1 that can only be divided by itself and 1
- the number of primes up to x is approximately x / ln(x).
- The ancient Sieve of Eratosthenes is a simple way to compute all prime numbers up to a given limit, by making a list of all integers and repeatedly striking out multiples of already found primes.
- Largest prime: 9,808,358 digits, 2006 Cooper, Boone (USA)
- A probable prime is an integer which, by virtue of having passed a certain test, is considered to be probably prime.
- 2002 Breakthrough by: AKS (Agrawal, Kayal and Saxena) primality test of the number N with complexity $(\log N)^6$ which is polynomial in the number of digits in N.
- http://primes.utm.edu/

•http://www.youtube.com/watch?v=9m2cdWorIq8

Applications (1)

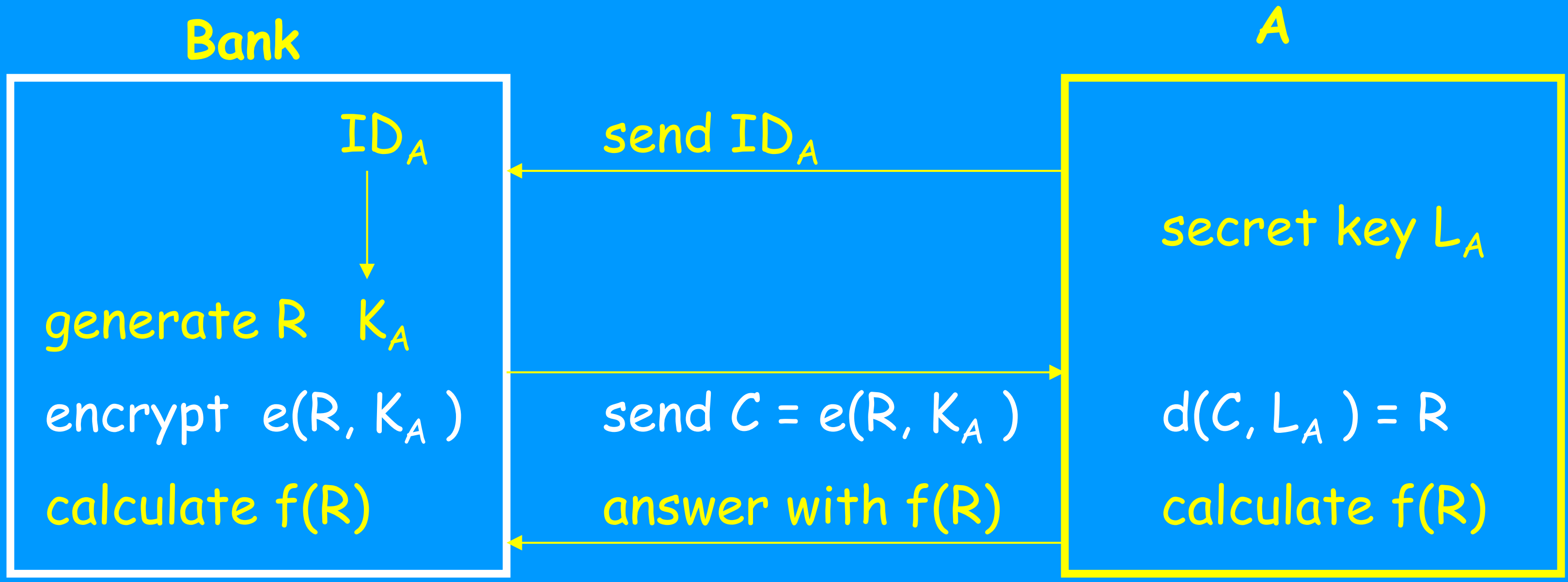


<u>Conclusion:</u> B can encrypt with K_A, only A can decipher with L_A

we guarantee that the public key belongs to A!

Applications (2): challenge response

Given: A has private key L_A and public key K_A

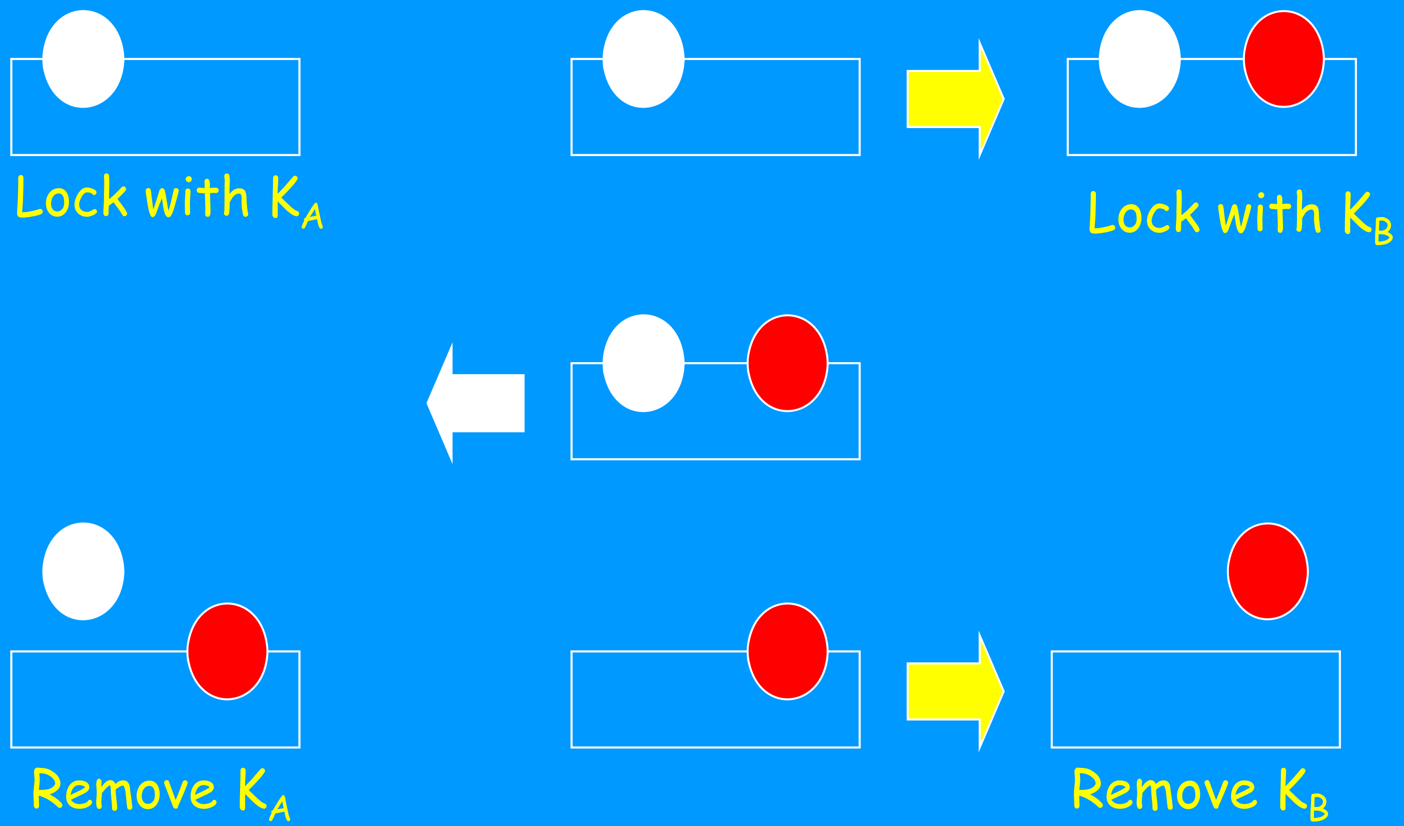


CONCLUSION: Only user A with secret key L_A can answer with f(R)

Note: never use R twice!

System without key exchange

http://www.youtube.com/watch?v=U62S8SchxX4



Q: consider the security

the system without key exchange (math)

user A	prime p	user B	prime p
secret	m, n		u, v
	$(m*n) = 1$ modulo $p-1$		$(u*v) = 1$ modulo $p-1$
	message M		

send:	$C = M^m$ modulo p	$\Rightarrow$	C
	C'	$\Leftarrow$	send: $C' = C^u$ modulo p
send:	$C'' = (C')^n$ modulo p	$\Rightarrow$	calculate:
	$= (M^{mn})^u$ modulo p		$(C'')^v = (M^u)^v = M$ modulo p
	$= M^u$ modulo p		

Diffie-Hellman (based on discrete logarithm problem)

Common parameters in A and B: large prime p and constant $1 < a < p-1$

1. Generate secrets X(A) and X(B): $1 < X(A) < p-1$; $1 < X(B) < p-1$

2: Exchange the public numbers: $Y(A) = a^{X(A)}$ modulo p $\rightarrow$ B

$Y(B) = a^{X(B)}$ modulo p $\rightarrow$ A

3: calculate in A: $Y(B)^{X(A)}$ modulo p $= a^{X(B)\,X(A)}$ modulo p $=$ K !!!

calculate in B: $Y(A)^{X(B)}$ modulo p $= a^{X(A)\,X(B)}$ modulo p $=$ K !!!

ASSUMPTION: given X , easy to calculate $Y = a^X$

given Y , hard to calculate X

Some remarks added

Given: prime p and $1 < a < p-1$, a **primitive**,

=> $a^{p-1} = 1$ modulo p

=> the p-1 numbers $1, a, a^2, a^3, \ldots, a^{p-2}$ modulo p **are all different**

We call (p-1), the order of the element a modulo p.

- For b, $1 \leq b \leq p-1$, $b = a^s$ modulo p and thus $b^{p-1} = 1$ modulo p.

Some remarks added

Given: prime p and $1 < a < p-1$

- For $b = a^k$ modulo p, $1 \le b \le p-1$, the order of b is a divisor of (p-1):

Example: Let p = 13 and a = 2.

$2^{12} = 1$ modulo 13

$4^6 = 1$ modulo 13, $4 = 2^2$ mod13

$3^4 = 1$ modulo 13, $3 = 2^4$ mod13

- Property: for a primitive, $a^{q(p-1)} = 1$ modulo p, $q \ge 1$

Some remarks added

Given: prime p and $1 < a < p-1$

- For $b = a^k$ modulo p, $1 \le b \le p-1$, the order of b is a divisor of (p-1):

we first proof that the order of $(b = a^k) \le \frac{p-1}{\gcd(p-1, k)}$

$\gcd((p-1), k) = c; \quad (p-1) = xc; \quad k = yc;$

then $\frac{p-1}{\gcd(p-1, k)} = \frac{xc}{c} = x$

$(b = a^k)^t = (a^k)^{\frac{p-1}{\gcd(p-1,k)}} = a^{xk} = a^{xcy} = a^{(p-1)y} = 1 \text{ modulo } p$

we see that the order t of b is $\le \frac{p-1}{\gcd(p-1, k)}$

Some remarks added

next we proof that the order is a multiple of $\frac{(p-1)}{\gcd(p-1,k)}$

for a primitive, $(b = a^k)^t = a^{tk} = a^{q(p-1)} = 1$ modulo p.

thus, $tk = q(p-1)$ and $t\frac{k}{\gcd(p-1,k)} = q\frac{(p-1)}{\gcd(p-1,k)}$

=> $\frac{(p-1)}{\gcd(p-1,k)}$ must divide t

- *To make it easy to generate elements* with a large order, one can use „safe primes", where p = 2q+1, p and q prime (Sophie Germain prime) . The order of the integers modulo p is then 2, q or (p-1).

Example of an attacker's scenario

- Example : Let $p = 13 = 2 \times 6 + 1$ and $a = 2$

- Now, Let $X_A = 2$ => public number $2^2 = 4$

  The different powers of 4 modulo 13 are: (4, 3, 12, 9, 10, 1) period 6

- Now, Let $X_B = 3$ => public number $2^3 = 8$

  The different powers of 8 modulo 13 are (8, 12, 5, 1) period 4

- The common key is $K_{AB} = 2^6$ modulo 13 = 12 (period of the key is 2!)

- The shared secret key K_{AB} lies in the intersection of the two groups

P = 13

- Example : Let $p = 13 = 2 \times 6 + 1$ and $a = 2$
  - powers of 2, 6, 7, 11 have period 12
  - powers of 3, 9 have period 3
  - powers of 5, 8 have period 4
  - powers of 4, 10 have period 6
  - powers of 12 have period 2

Example for the „safe prime"

- Example : Let p = 11 = 2 x 5 + 1 and a = 2

• powers of	2	2,4,8,5, 10,9,7,3,6,1	period 10
	6	6,3,7,9,10,5,8,4,2,1	
	8	8,9,6,4,10,3,2,5,7,1	
	7	7,5,2,3,10,4,6,9,8,1	
• powers of	4	4,5,9,3,1	period 5
	3	3,9,5,4,1	
	5	5,3,4,9,1	
	9	9,4,3,5,1	
	10	10,1	period 2

Note: only 1 element can have period 2 (show) !

Further references

- For further background on the mathematics

  - R.P. Grimaldi: Discrete and Combinatorial Mathematics