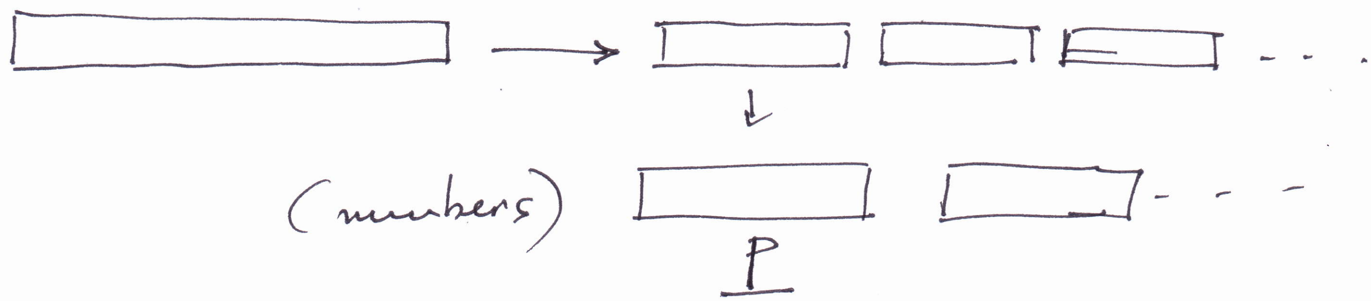
P : plaintext (1)
C : Ciphered text

Review

1) Encoding a phrase in a number



2) Caesar encryption

Key : $k \in \mathbb{Z}$

$$C = P + k \pmod{n}$$

ex

26
256
65 ...

Decryption:

$$P = C - k \pmod{n}$$

3) Exponential encryption (Deffie-Hellman encryption)

⚠ p is a prime (large), $p > 2$
and $e \in \mathbb{N}$: $\gcd(e, p-1) = 1$

(e should be chosen as a prime)

Encryption: Key: (e, p) or at least keep e

For $P < p$: $\quad C = P^e \pmod{p}$

Decryption: $\left\{ P = C^d \pmod{p} \right.$

From the Key (e,p)

$\to$ decryption key (d,p) by:

$e.d = 1 \pmod{p-1}$

3) RSA encryption (Rivest - Shamir - Adleman) (public Key)

2

⚠ . Let p, q : primes (large)

and $n = p \cdot q$ ⚠ p, q Keep Secrete

. Let choose e such that:

$$\gcd(e, \varphi(n)) = 1$$

φ : Euler function

φ : multiplicative function

i.e, since $\gcd(p, q) = 1$

$\Rightarrow \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q)$

$= (p-1) \cdot (q-1)$

The encryption Key : (e, n) (public Key)

Encryption: $C = P^e \pmod{n}$

Decryption: $P = C^d \pmod{n}$

From $n = p \cdot q \xrightarrow{\text{secrete}} \varphi(n) = (p-1)(q-1)$

$\rightarrow$ d = inverse of e mod $\varphi(n)$

$e \cdot d = 1 \mod (\varphi(n))$

2^{bis}

RSA Digital Signatures

A

Key creation

- Choose secret primes p and q

  Compute $n = p.q$

  $\varphi(n) = (p-1)(q-1)$
- Choose verification exponent e

  Such that: $\gcd(e, \varphi(n)) = 1$

  (e should be chosen as a prime)
- Publish n and e

Signing

d: Keep secrete.

- Compute d Satisfying

  $de = 1 \pmod{\varphi(n)}$
- Select a digital document D

  to sign by computing:

  $S = D^d \pmod{n}$
- Publish the document and

  signature: D and S

B and all other cannot find d of A in an acceptable time!

B

verification

- Compute $S^e \pmod{n}$

  and verify that it is equal

  to D

2ter

Key Creation

Ex: • A chooses two secret primes $p = 1223$, $q = 1987$ and $n = p \cdot q = 1223 \cdot 1987 = 2430101$

$\varphi(n) = (p-1)(q-1) = 1222 \cdot 1986 = 2426892$

• A chooses a public verification exponent

$e = 948047$

(note that: $\gcd(e, \varphi(n)) = \gcd(948047, 2426892) = 1$)

Publish

$n = 2430101$

$e = 948047$

RSA Signing

• A computes his private signing key d by $ed \equiv 1 \pmod{\varphi(n)} \Longrightarrow d = 1051235$

• A selects a digital document to sign

$D = 1070777 \qquad (1 < D < n)$

and he computes the digital signature

$S \equiv D^d \pmod{n} \equiv 1070777^{1051235} \pmod{2430101}$

$\equiv 153337 \pmod{2430101}$

• A publishes the documents and signature:

$D = 1070777$ and $S = 153337$

RSA Verification

• B uses A's public n and e to compute: $S^e \pmod{n}$

$\equiv 153337^{948047} \pmod{2430101}$

$\equiv \underbrace{1070777}_{\text{Same values as } D.} \pmod{2430101}$

!

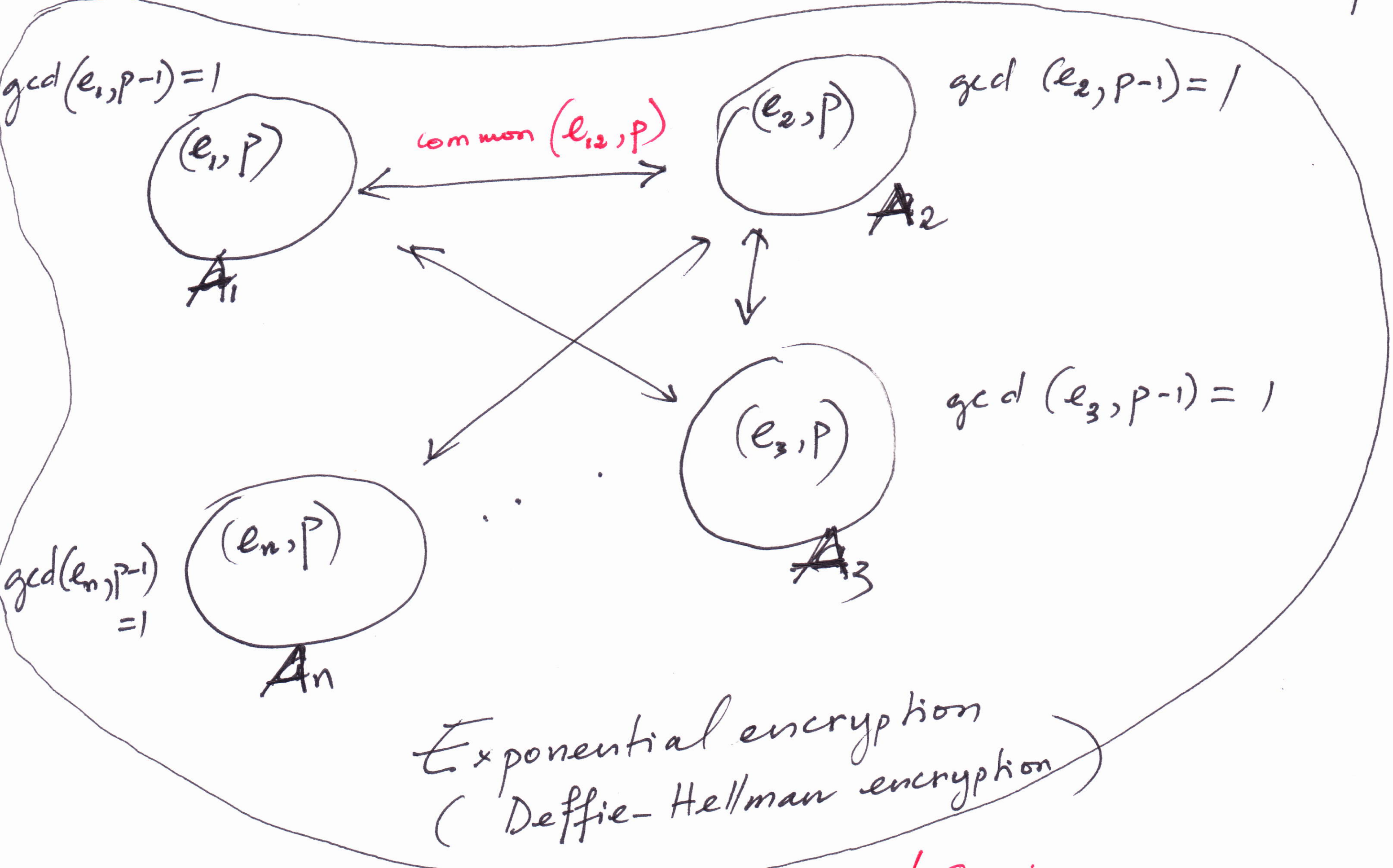
3

Encryption Schemes

- Symmetric
  - Encryption Key → Decryption Key
  - Keep Secrete
  - The time for encryption = the time for decryption.
  - ex Caesar, exponential encry.
- Asymmetric
  - encryption Key = public Key
  - From the encryption Key → decryption Key needs very large time!
  - ex RSA.

p: primes (large)

$a \in \mathbb{N}$ $\gcd(a, p) = 1$ (a should be chose as a prime)



The common Key between a_1 and a_2:

- A_1 Send to A_2 the number $y_1 = a^{e_1} \pmod p$

A_2 can find $\xrightarrow{\triangle!}$ common Key of A_1, A_2: $e_{12} = y_1^{e_2} \pmod p$

$= a^{e_1 e_2} \pmod p$

- A_2 send to A_1 the number $y_2 = a^{e_2} \pmod p$

A_1 can find the common key of A_1 A_2 by:

$e_{12} = y_2^{e_1} = a^{e_1 e_2} \pmod p$

A_2 (and all other) can not find e_1 of A_1 in an acceptable time! Similary to A_1 ...

hence the common Key of A_1, A_2:

$$e_{12} = a^{e_1 e_2} \pmod p$$

all A_i (except A_1, A_2) all cannot find e_{12}

5

⚠ If the information exchange between A_1 and A_2 is large and often,
A_1 and A_2 should change the numbers for each time they contact:
A_1 chooses a random number x and send to A_2 the number: $X = a^x$
Similarly, A_2 chooses a random number y and send to A_1 the numbers: $Y = a^y$.
Both of them can find the common key:

$$K = Y^x = (a^y)^x = (a^x)^y = X^y.$$

while the others couldn't know anything except the numbers X, Y, from these numbers, it is impossible (~~A~~ in an <u>acceptable time</u>) to find K.

→ 5 bis