Data Security and Encryption

数据安全与加密

Xitian Huang

6 August 2022

Data Leak
Shanghai National Police Database

- https://breached.to/
- Info ~1 Billion Chinese Citizens
- 10 BTC (200,000 USD or 1,300,000 RMB)

2022 - SHGA Shanghai Gov National Police database

by ChinaDan - Thursday June 30, 2022 at 08:55 AM

ChinaDan

BreachForums User

MEMBER

Posts:	5
Threads:	1
Joined:	Jun 2022
Reputation:	183

June 30, 2022, 08:55 AM (This post was last modified: July 3, 2022, 10:25 AM by Muffin. *Edit Reason: Locked by staff due to all # the spam*)

In 2022, the Shanghai National Police (SHGA) database was leaked. This database contains many TB o data and information on Billions of Chinese citizens.

Sell: Shanghai GOV (SHGA.gov.cn) National Police Database

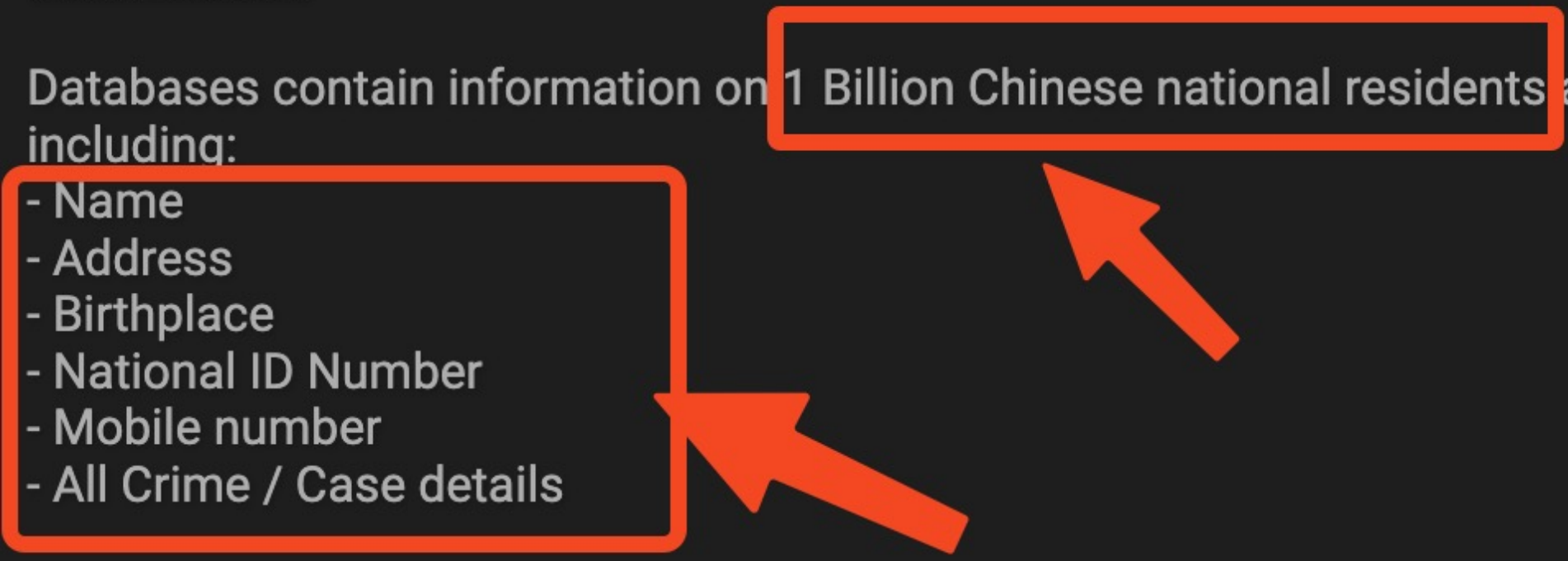
Host: http://oss-cn-shanghai-shga-d01-a.ops.ga.sh/
Data leaked from these tables:

```
----TABLES----
person_address_label_info_slave QFpD25bKTJ2eQBxcbe2Aaw 90 0 546148916 0 172.2gb
172.2gb
nb_theme_address_merge_tracks_slave -bUMVB1uRRusUbbqZepEpA 300 0 37483779369 4
22.4tb 22.4tb
nb_theme_address_case_dwd_test 7COIWTt7QU-YPwWub8z_SQ 150 0 22375506 1749307 25.2gb
25.2gb
nb_theme_address_company_dwd-total fpnmEYB9SI6WevHnZIEwIA 150 0 1842856 0 2.8gb
2.8gb
nb_theme_address_case_dwd-total 7X8oNqULQnWFLpzHDaUTbg 150 0 1214119253 0 1tb 1tb
nb_theme_address_company_dwd_test g5f6l4LGQcGL3oQ6ON2Bbw 150 0 2017931 0 4.3gb
4.3gb
person_address_label_info_master t64pp9WnS3maY9jBjzTtiw 90 0 969830088 0 282.8gb
282.8gb
```

Data Details:

Databases contain information on 1 Billion Chinese national residents and several billion case re
including:

- Name
- Address
- Birthplace
- National ID Number
- Mobile number
- All Crime / Case details



UPDATE: Per request, sample size increased to 750k (250k for each of the 3 main index): https://gofile.io/d/sCggGC
Staff update: Due to the chances of the file being reported to gofile, uploaded the sample to our servers: https://cdn.breached.to/shga_sample_750k.tar.gz

PRICE: I am selling all of this data for 10BTC ($200k USD)

省长沙市浏阳市","IDNO":"430181199712035426","IDTYPE":"01","QUERY_STRING":" 湖南省长沙市浏阳市 24 97 1997 ","R
省商丘市虞城县","EDEGREE":"初中","HEIGHT":"160","IDNO":"411425198807157221","IDTYPE":"01","NATION":"汉","PHOTO
省淮安市盱眙县","EDEGREE":"学龄前儿童","ESCU":"未服兵役","HHPLACE":"江苏省盱眙县管仲镇祖窑村井西组11号","IDNO":"32083
省天水市秦安县","HHPLACE":"甘肃省秦安县兴国镇青年西路地税局家属楼2号楼1单元502室","IDNO":"620522198601090011","IDTYPE
省白银市白银区","IDNO":"620402199005110462","IDTYPE":"01","QUERY_STRING":" 甘肃省白银市白银区 31 90 1990 ","R
壮族自治区南宁地区宾阳县","IDNO":"452123198504281021","IDTYPE":"01","QUERY_STRING":" 广西壮族自治区南宁地区宾阳县
省黄冈地区黄梅县","HEIGHT":"158","IDNO":"42213019430810196x","IDTYPE":"01","PROF":"粮农","QUERY_STRING":" 湖北
省温州市苍南县","HHPLACE":"浙江省苍南县灵溪镇联进村182-183号","IDNO":"33032719471103513","IDTYPE":"01","NATION":"
建省福州市晋安区","IDNO":"350111191001070158","IDTYPE":"01","QUERY_STRING":" 福建省福州市晋安区 111 10 1910 ",
市长宁区","EDEGREE":"高中","HEIGHT":"163.0","HHPLACE":"上海市闵行区龙吴路5599弄171号301室","IDNO":"31010519670627
省黄冈地区黄冈县","HEIGHT":"166","IDNO":"422121197102214026","IDTYPE":"01","PROF":"临工","QUERY_STRING":" 湖北
省淄博市沂源县","IDNO":"370323198709010021","IDTYPE":"01","QUERY_STRING":" 山东省淄博市沂源县 34 87 1987 ","R
省锦州市太和区","HEIGHT":"157","IDNO":"210711195210044028","IDTYPE":"01","PROF":"菜农","QUERY_STRING":" 辽宁省
西壮族自治区桂林市象山区","IDNO":"450304190302060515","IDTYPE":"01","QUERY_STRING":" 广西壮族自治区桂林市象山区 1
省六安地区六安市","HHPLACE":"安徽省六安市裕安区徐集镇裕兴村王院墙组","IDNO":"342401197804273638","IDTYPE":"01","NATI
壮族自治区河池地区凤山县","IDNO":"452727198909250029","IDTYPE":"01","QUERY_STRING":" 广西壮族自治区河池地区凤山县
省常州市金坛县","IDNO":"320422197405231111","IDTYPE":"01","QUERY_STRING":" 江苏省常州市金坛县 47 74 1974 ","R
省泰安市肥城县","IDNO":"370922197010194236","IDTYPE":"01","QUERY_STRING":" 山东省泰安市肥城县 51 70 1970 ","R
省蚌埠市五河县","ESCU":"未服兵役","HEIGHT":"156.0","IDNO":"340322192805122024","IDTYPE":"01","MARR":"丧偶","NAT
市南开区","IDNO":"120104197706054941","IDTYPE":"01","QUERY_STRING":" 天津市南开区 44 77 1977 ","RNAME":"强白
省达川地区大竹县","HHPLACE":"四川省大竹县高明乡大良村4组","IDNO":"513029199409176738","IDTYPE":"01","NATION":"汉",
省合肥市长丰县","HHPLACE":"安徽省长丰县岗集镇井沿村老庄组12号","IDNO":"340121198807208 50x","IDTYPE":"01","NATION":"
省秦皇岛市青龙满族自治县","IDNO":"130321197604014 26x","IDTYPE":"01","QUERY_STRING":" 河北省秦皇岛市青龙满族自治县
省上蔡县","IDNO":"412825198905288519","IDTYPE":"01","QUERY_STRING":" 河南省上蔡县 32 89 1989 ","RNAME":"刘义


9 52 1952 ","RNAME":"陈太全","SE
73 ","RNAME":"白利花","SEX":"女
MES":"撤逃人员 寻衅滋事案","LABS"
7号1801室","IDNO":"310106197711
RNAME":"甘继海","SEX":"男"},"_ty
":"河南封丘县","QUERY_STRING":"
1991 ","RNAME":"张萌","SEX":"
林市蛟河市 辽宁 20 01 2001 ","R
sort":[673419]}
津镇高升村大阳组16号 51 70 1970 ","RNAME":
"未婚","NPLACE":"江苏宿迁市宿城区","QUERY
S":"交通违法 实有人口 常住人口","LABS":"AB0
,"LABS":"AB000633","NATION":"汉","NPLA
","NATION":"汉","NPLACE":"上海市金山县","
-a.ops.ga.sh/shga-ryzp/CSJ/JIANGSU_JZZ
MES" "关注人员_涉毒关注人员" "LABS":"AB003
片":["http://oss-cn-shanghai-shga-d01-a
,"MARR":"已婚","NPLACE":"江苏沭阳县","PHO

10时26分,王斌(男,户籍地址:上海市徐汇区梅陇六村6号401室,现住地址:上海市闵行区罗秀路1339弄29号801室,身份证
20时许,报案人罗友军来所报案,2014年11月29日15时许,其在本市普陀区枣阳路465弄21号门口与一男子发生纠纷,被该男
3:05:57,手机号:15317001758,报警人在仓汇路1345弄东门口,称:苏A278A1 挪车","CASE_TYPE":null,"CASE_S
车驶离","CASE_TYPE":null,"CASE_STATE":null},"ORGANIZER_POLICE_TYPE":null,"ORGANIZER":{"ORGA
日16时51分,报警人王正芳使用13817262927拨打110报警称:其前夫钱龙详(身份证:310225195711201217)在外欠债,
上午9时许,报警人张丽萍110报称:于2006年1月4日晚20时至次日上午8时间,受害单位(东沟镇东塘路771号上海东际塑料制
日07时42分,报警人使用13818080572报警称:在 瑞和路168号 8号楼门口 2辆轿车相撞。双方理赔中心理赔","CASE_T
","CASE_TYPE":null,"CASE_STATE":null},"ORGANIZER_POLICE_TYPE":null,"ORGANIZER":{"ORGANIZER
日15时许,我所民警接群众匿名举报称:本市徐汇区嘉善路171弄11号棋牌室内有人以打麻将方式进行赌博。","CASE_TYPE
日7时48日许,接指挥中心110报警,龙水北路960弄15号501室纠纷。我所处警到达现场,报警人称楼上601室是群居有十几个
日1时10分吉接110报警称昆明路1266号门口夜排当吵闹.民警到现场劝阻.","CASE_TYPE":null,"CASE_STATE":nul
日09时05分,报警人使用13482626327报警称:在 龙水南路201号龙华汽配城内菜场内2号岗亭处 警察走后,有摆摊人员要
SE_TYPE":null,"CASE_STATE":null},"ORGANIZER_POLICE_TYPE":null,"ORGANIZER":{"ORGANIZER_NAME
日22时08分,报警人使用13122394577报警称:在 新源路"盛越(谐音)"宾馆301号房间 举报上址有2人正在进行卖淫嫖娼
":"310113630000","org_name":"上海市公安局宝山分局顾村派出所"},"case_address":"上海市宝山区泰和西路
日12时00分,报警人使用38821518报警称:在 浦东大道2220号1楼104室上安大厦 报警人被打rn报警人被打,带所处理。
4:28:42,手机号:13764916279,报警人在杨泰路2188号门口 通道处,称:挪车 粤GG1743","CASE_TYPE":null,"CA
日16时21分,报警人使用13918193166报警称:在金山区朱泾镇西林街51号中国农业银行门口上址有人打架,民警到场处理,
0:28:56,手机号:13052027987,报警人在天通庵路654号,称:赔偿纠纷 请民警到场处理。赔偿纠纷 ,民警到场调解,并
日12时28分,事主110报警称:杭州路宁武路电动自行车被窃。民警到现场后经了解系报警人自己未锁电动自行车停在路边后


nameinfo":[{"name":"黄*"}]}","FIRST_TIME"
[{"name":"李灵芝女士"}]}","FIRST_TIME":"154
nameinfo":[{"name":"曾**"}]}","FIRST_TIME
nameinfo":[{"name":"任**"}]}","FIRST_TIME
IL":"{"nameinfo":[{"name":"邹声虎"}]}","FI
[{"name":"田女士"}]}","FIRST_TIME":"154608
nameinfo":[{"name":"高素霞"}]}","FIRST_TIM
nameinfo":[{"name":"余世杰"}]}","FIRST_TIM
nameinfo":[{"name":"冯庆成"}]}","FIRST_TIM
nameinfo":[{"name":"贾艳芳"}]}","FIRST_TIM
:"小牛津幼儿园(航顺晓镇东南)(迎秋西里28栋3单元8号)","SI
DRESS":"宜昌市湖北省宜昌市夷陵区长江市场香山凤凰城","SR
":"西乡(金海路金海商务大厦2栋512)","SRC_ID":"0b2554
DDRESS":"广东省东莞市清溪镇清溪镇铁松铁矢岭河边东路11号
DDRESS":"山东省烟台市烟台市文昌路街道莱州中医院","SRC_
","SRC_ADDRESS":"贵州省黔东南苗族侗族自治州岑巩县大有
嘉德·金鼎广场(六号楼三单元302)","SRC_ID":"43f0348c5
ADDRESS":"江苏省连云港市海州区江苏省连云港市海州区江苏省
ADDRESS":"河南省平顶山市平顶山市文峰路龙博城","SRC_ID
ADDRESS":"山东省枣庄市枣庄市海滕机床有限司司地址:滕州市
ADDRESS":"甘肃省陇南市武都区甘肃省陇南市武都区城关镇甘肃
bile","IDENTITY_VALUE":"159****5906","LAS
,"IDENTITY_VALUE":"18926754681","LAST_TIM
obile","IDENTITY_VALUE":"135****8875","LA
obile","IDENTITY_VALUE":"183****5084","LA
TYPE":"mobile","IDENTITY_VALUE":"187985
DENTITY_VALUE":"15062048023","LAST_TIME":
mobile","IDENTITY_VALUE":"15695189162","L
mobile","IDENTITY_VALUE":"13461187266","L
mobile","IDENTITY_VALUE":"13656373688","L
mobile","IDENTITY_VALUE":"15293353385","L
"shga_wa.ods_nb_app_icpoof_delivery"},"_type"
OURCE":"shga_wa.ods_nb_app_icpoof_delivery"},
":"shga_wa.ods_nb_app_icpoof_delivery"},"_typ
_wa.ods_nb_app_icpoof_delivery"},"_type":"a","
ds_nb_app_icpoof_delivery"},"_type":"a","sort"
shga_wa.ods_nb_app_icpoof_expressdelivery"},"
s_nb_app_icpoof_delivery"},"_type":"a","sort"
p_icpoof_delivery"},"_type":"a","sort":[33198

Encryption
Cryptography 密码学

Symmetric Encryption ⟺ Private Key 私钥

Asymmetric Encryption ⟺ Public Key 公钥
Private Key 私钥

Number Theory

Mathematical Preliminaries

Modular Arithmetic 同余

Periodicity

$$a \equiv b \bmod n$$

$$a \bmod n \equiv b$$

"congruent"

$$32 \bmod 12 \equiv ?$$

$$32 \equiv 8 \bmod 12$$

$$12 \overline{)\,32} = 2 \text{ years}$$

$$24$$

$$8 \text{ months}$$

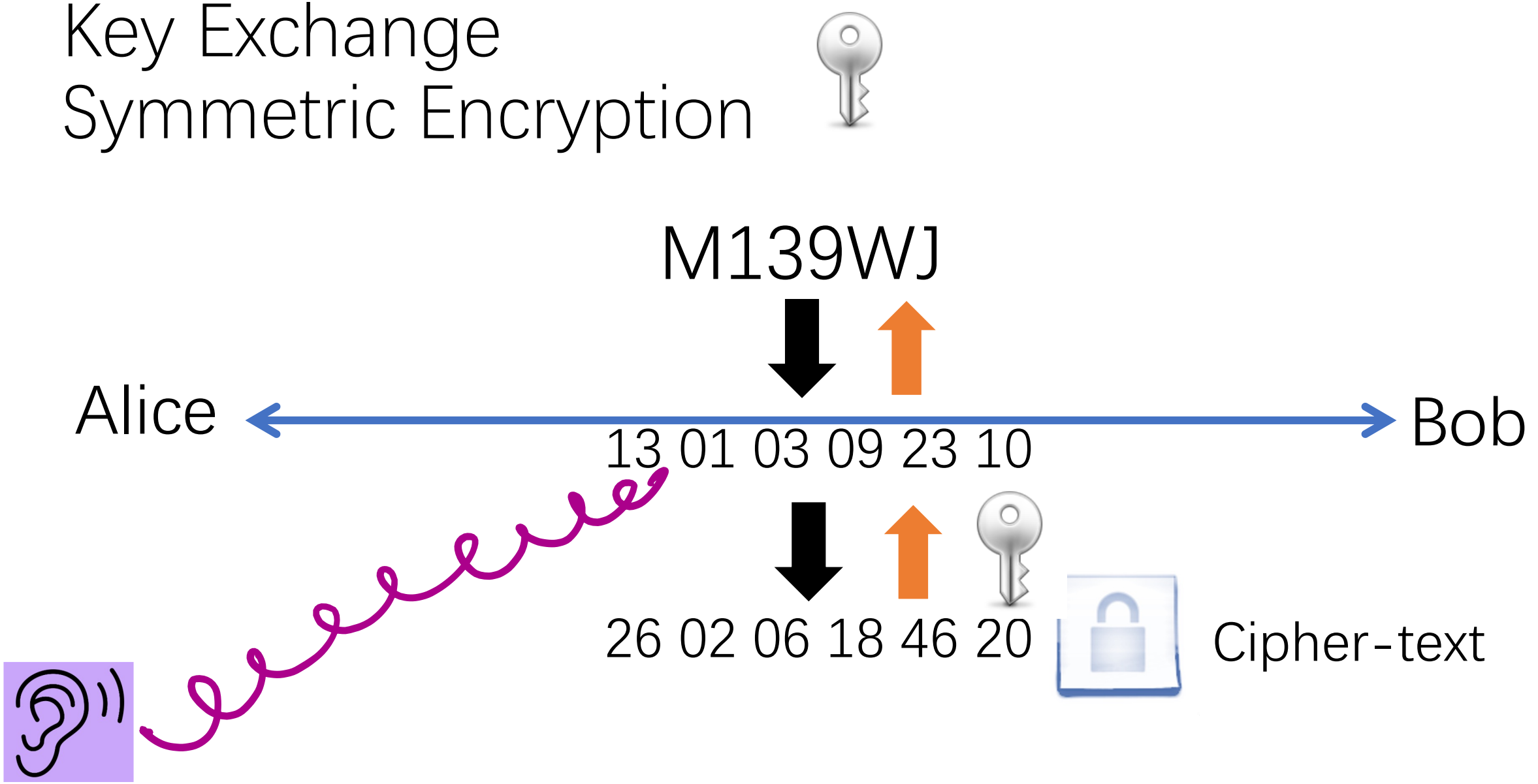
Remainder

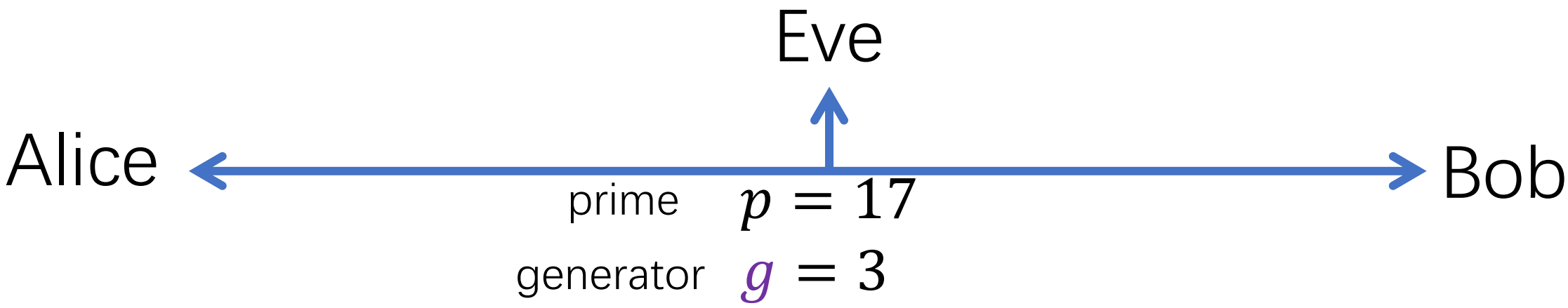
Mathematical Preliminaries
Prime number 素数/质数

1,2,3,5,7,11,13,17,19,23,29…

Infinitely many!

Key Exchange
Symmetric Encryption





$$g^{a} \bmod p = A$$

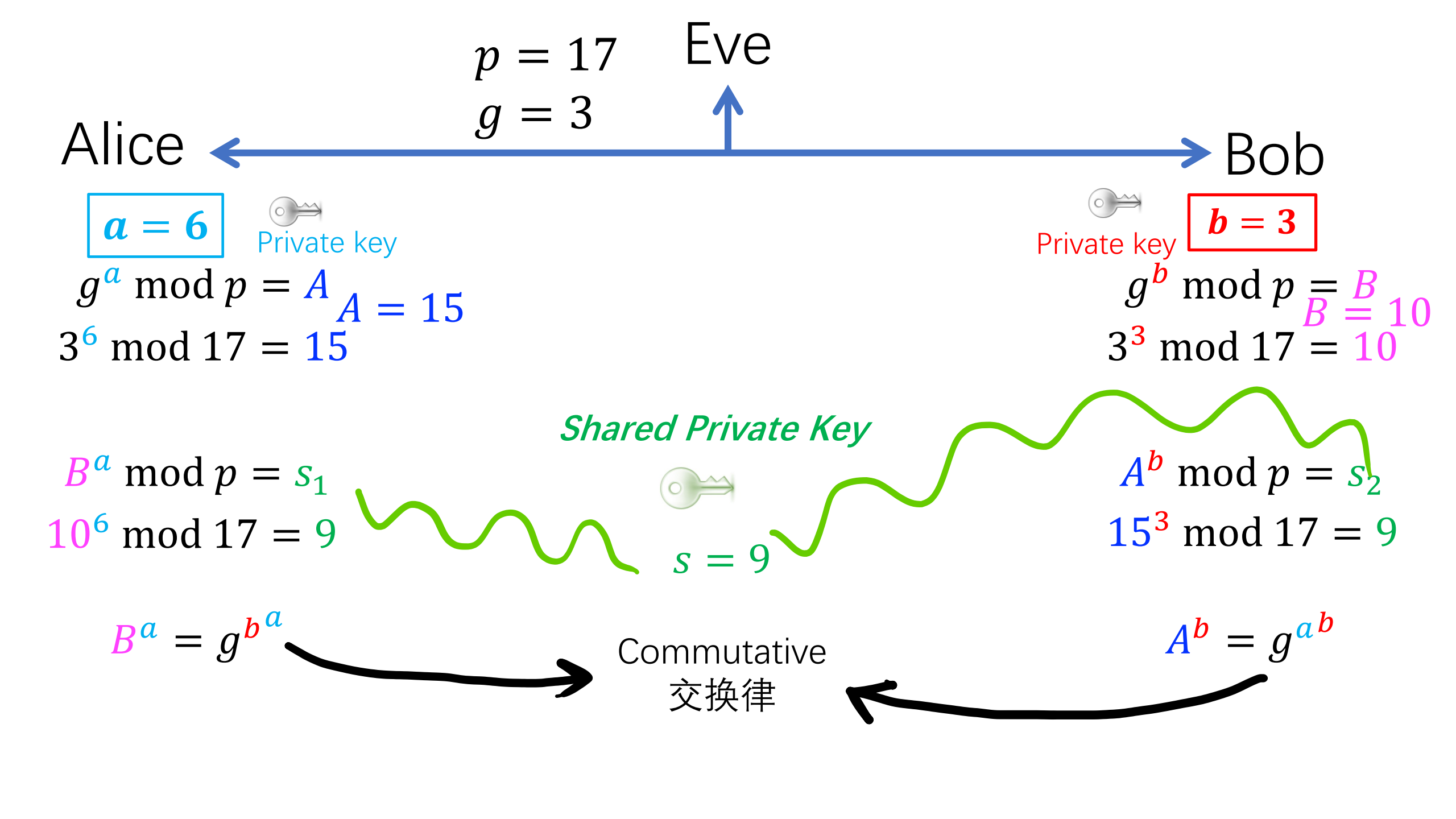
Easy

$$g^{?} \bmod p = A$$

Hard **Discrete Logarithm**

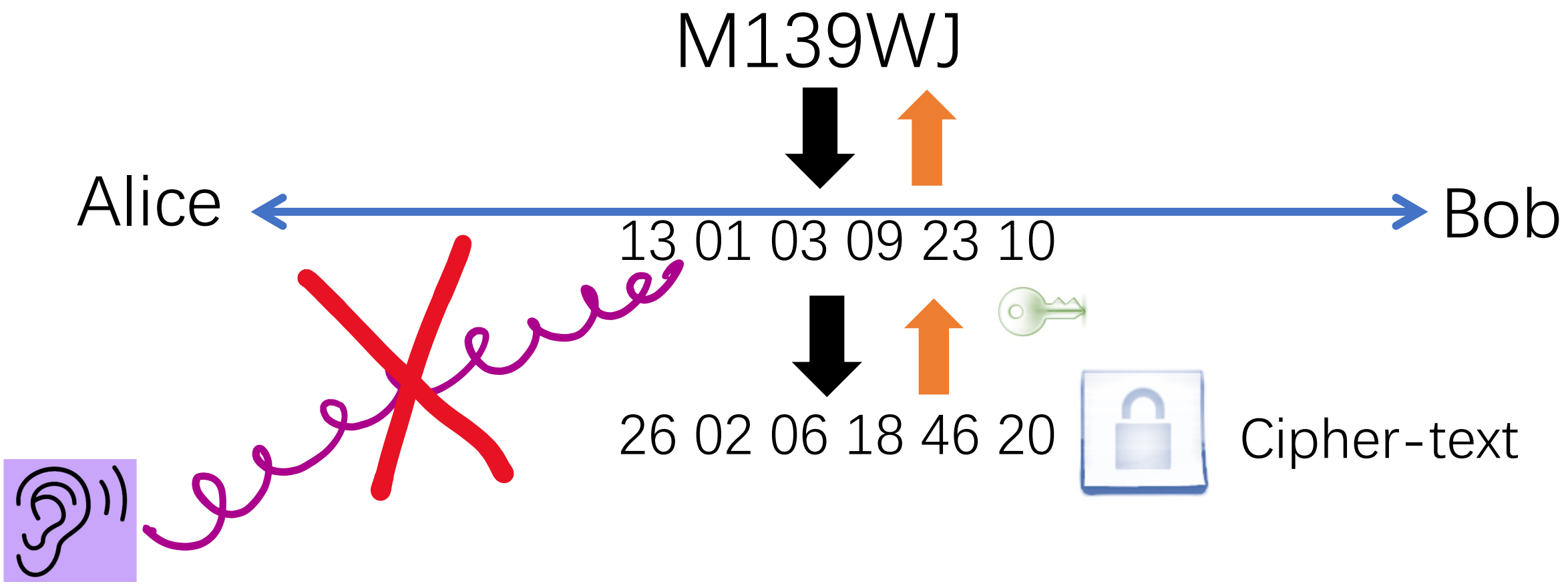
trial and error

One-way Function


$p = 17$
$g = 3$
Eve
Alice
Bob
$a = 6$
Private key
Private key
$b = 3$
$g^a \bmod p = A$
$A = 15$
$3^6 \bmod 17 = 15$
$g^b \bmod p = B$
$B = 10$
$3^3 \bmod 17 = 10$
Shared Private Key
$B^a \bmod p = s_1$
$10^6 \bmod 17 = 9$
$A^b \bmod p = s_2$
$15^3 \bmod 17 = 9$
$s = 9$
$B^a = g^{b^a}$
Commutative
交换律
$A^b = g^{a^b}$

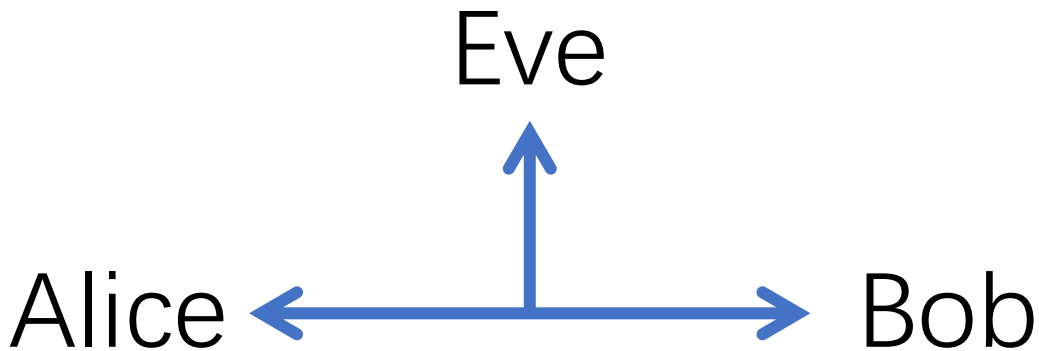
Key Exchange
Symmetric Encryption

Diffie–Hellman key exchange
1976



Key Exchange
Symmetric Encryption

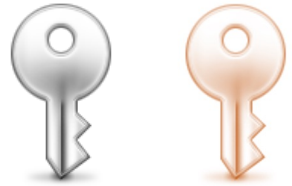
Too many keys

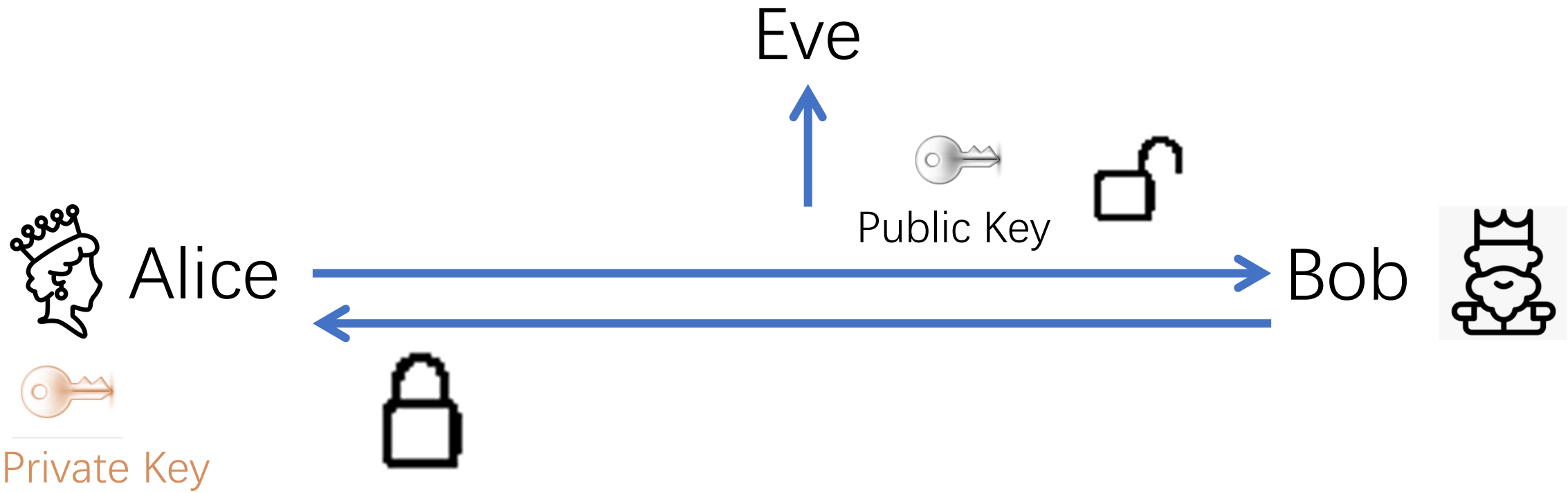


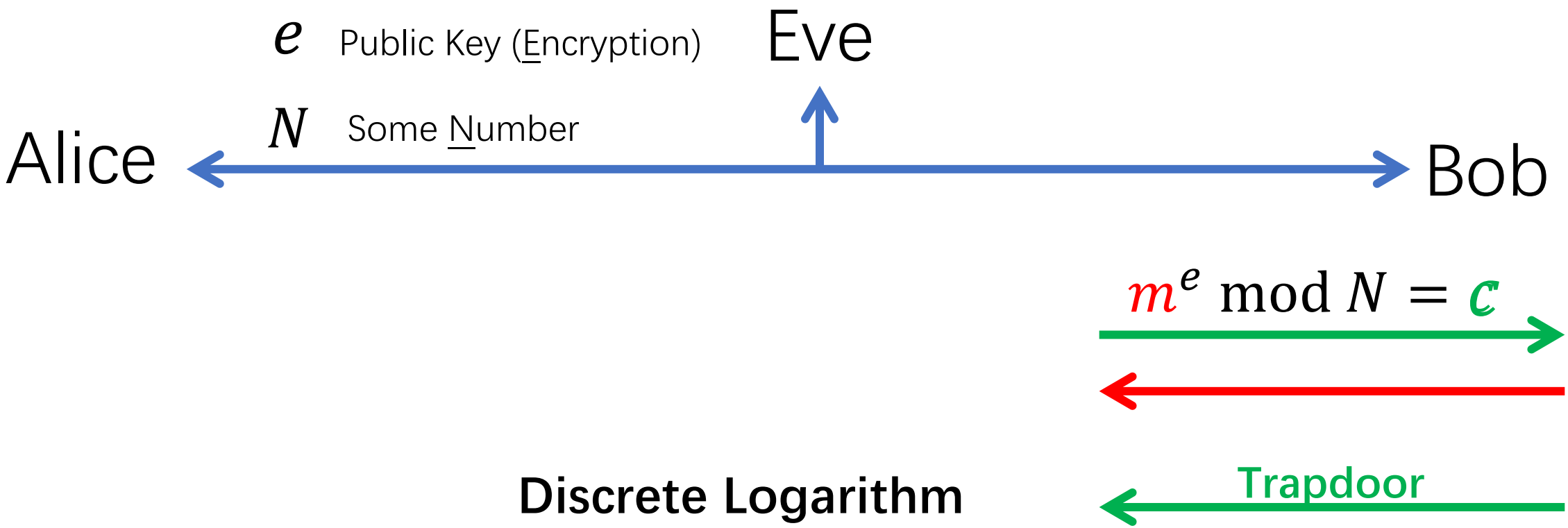
Authentication

Asymmetric Encryption

Public Key 公钥
Private Key 私钥







One-way Function

Trapdoor One-way Function

Factorization of Numbers

$$46 = 2 \times 23$$

$$6895601 = 1931 \times 3571$$

Uniquely decomposed into **prime** numbers

Fundamental theorem of arithmetic
Unique factorization theorem

Leonhard Euler

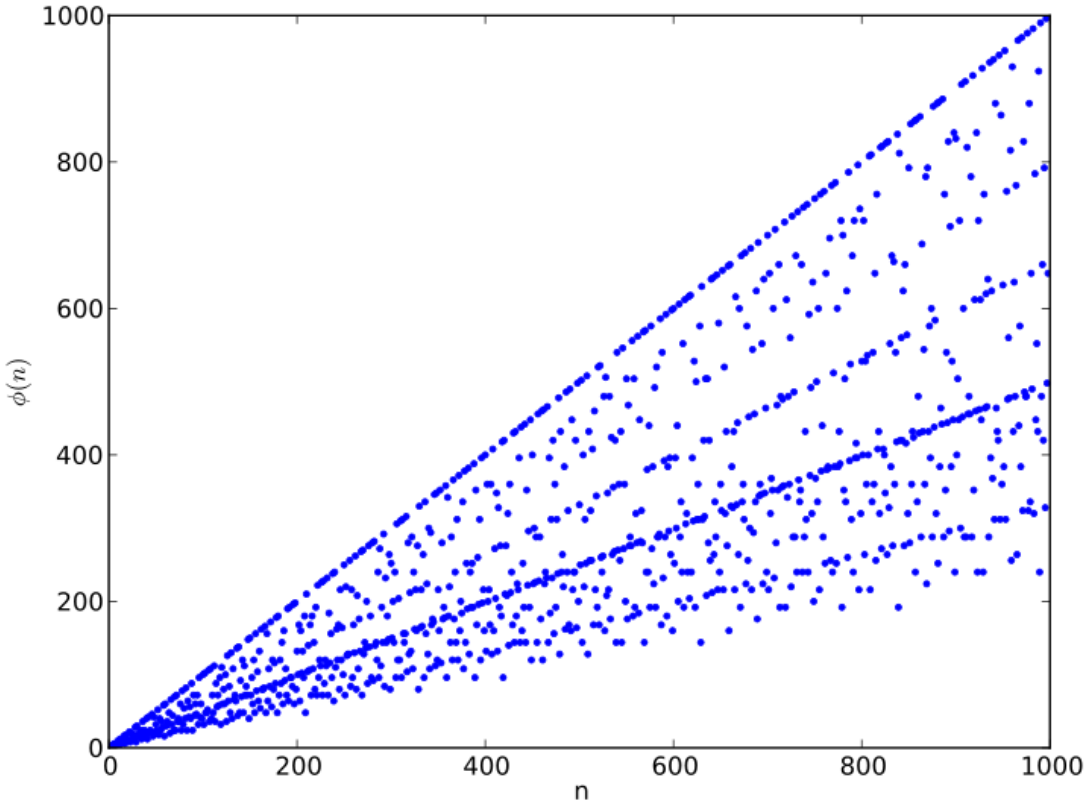
(15 April 1707 – 18 September 1783)

- Euler's function ϕ
- Euler's theorem

- Euler's function ϕ

$$\phi(9) = \#<1, 2, 3, 4, 5, 6, 7, 8, 9> = 6$$

coprime



primes p, q

$$pq = N$$

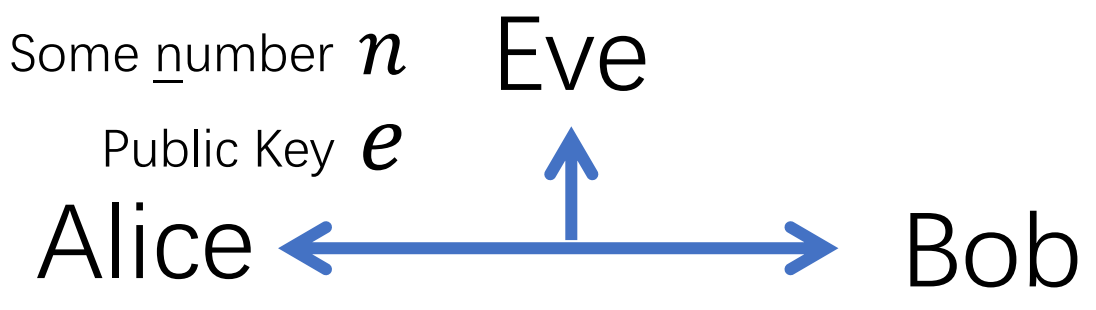
$$\phi(N) = \phi(pq) = \phi(p)\phi(q)$$
$$= (p-1)(q-1)$$

- Euler's theorem

$$m^{\phi(n)} \equiv 1 \bmod n \quad (m, n \text{ coprime})$$

$$m^{k\,\phi(n)} \equiv 1 \bmod n$$

$$m^{k\,\phi(n)+1} \equiv m \bmod n$$



$$m^{e} \equiv c \bmod n$$

$$\boxed{c^{d} \equiv m \bmod n}$$

$$(m^{e})^{d} \equiv m \bmod n$$

$$k\,\phi(n) + 1 = ed$$

$$ed \equiv 1 \bmod \phi(n)$$

Trapdoor
One-way Function

e Public Key (Encryption)

N Some Number

Eve

Alice

Bob

$N = pq$

$221 = 13 \times 17$

$\phi(N) = \phi(pq) = \phi(p)\phi(q)$
$= (p-1)(q-1)$

$\phi(221) = 12 \times 16 = 192$

$e = 5$

$m^e \bmod N = c$

$11^5 \bmod 221 = 163$

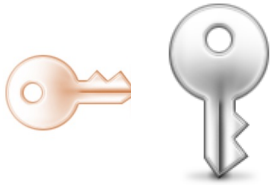
$c^d \bmod N = m$

$163^{77} \bmod 221 = 11$

$d = 77$

Private Key (Decryption)

$$ed \equiv 1 \bmod \phi(n)$$



Asymmetric Encryption

RSA Logarithm
1977
Ron **R**ivest
Adi **S**hamir
Leonard **A**dleman

Discrete Logarithm
Prime Factorization
→ **One-way Function**

Euler's Function
Euler's Theorem
→ **Trapdoor**

Edward Snowden

(1983/6/21 ---)

PRISM(棱镜计划)

Secret Documents Reveal N.S.A. Campaign Against Encryption

Documents show that the N.S.A. has been waging a war against encryption using a battery of methods that include working with industry to weaken encryption standards, making design changes to cryptographic software, and pushing international encryption standards it knows it can break. Related Article »

Excerpt from 2013 Intelligence Budget Request | Bullrun Briefing Sheet

Diffie–Hellman key exchange
1976

RSA Logarithm
1977

1969 at GCHQ
James Ellis
Clifford Cocks
Malcolm Williamson

1973 at GCHQ
Clifford Cocks

(Revealed in 1997)


CENTRAL INTELLIGENCE AGENCY
UNITED STATES OF AMERICA


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

GCHQ

MATHS

Number Theory

No Privacy On Internet