

RSA

A complex network diagram with numerous nodes and edges, rendered in light blue and grey. A few nodes are highlighted in yellow and orange, and a horizontal bar with blue, red, and grey segments is positioned below the title.

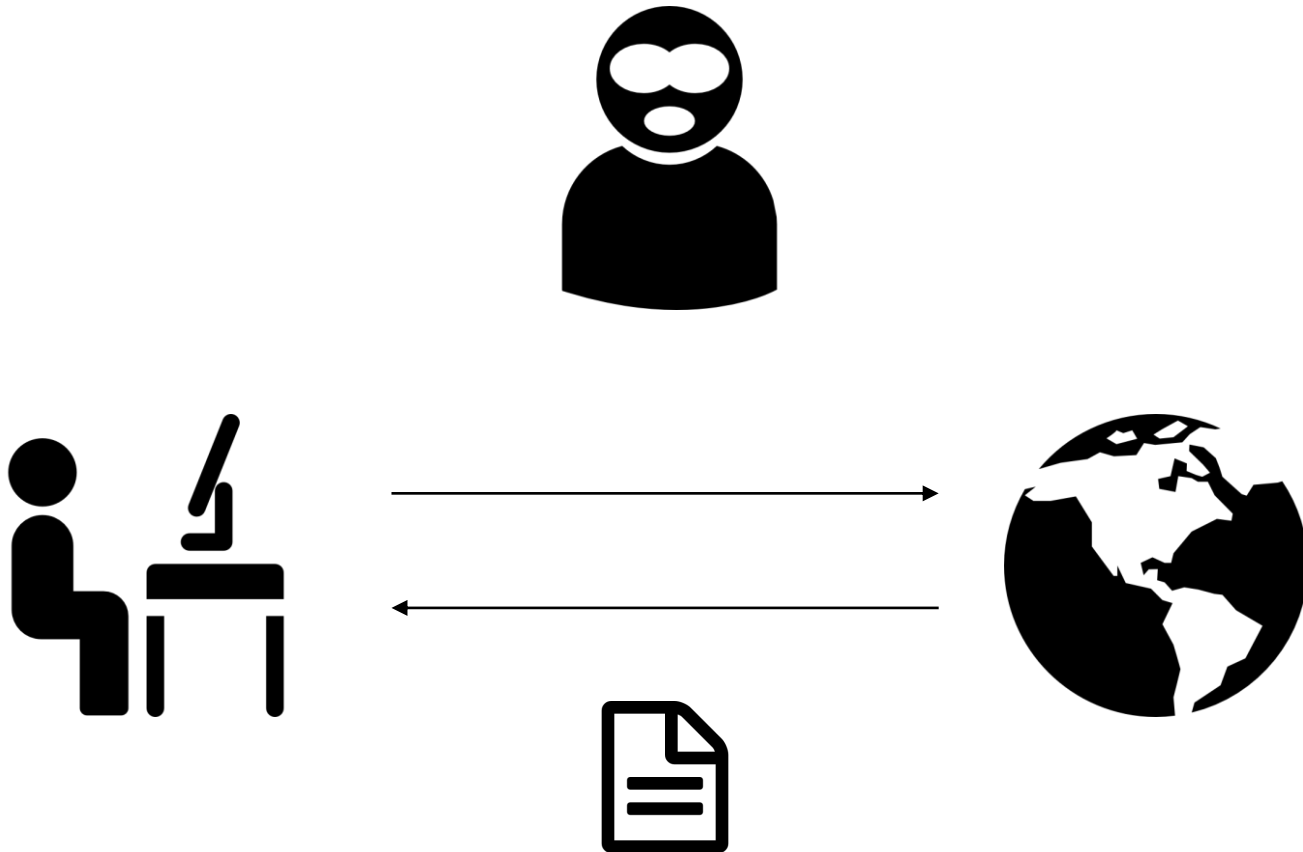
Seoul National University of Science and Technology
Computer Science and Engineering

2019-05-23

RSA Introduction

Network Environment

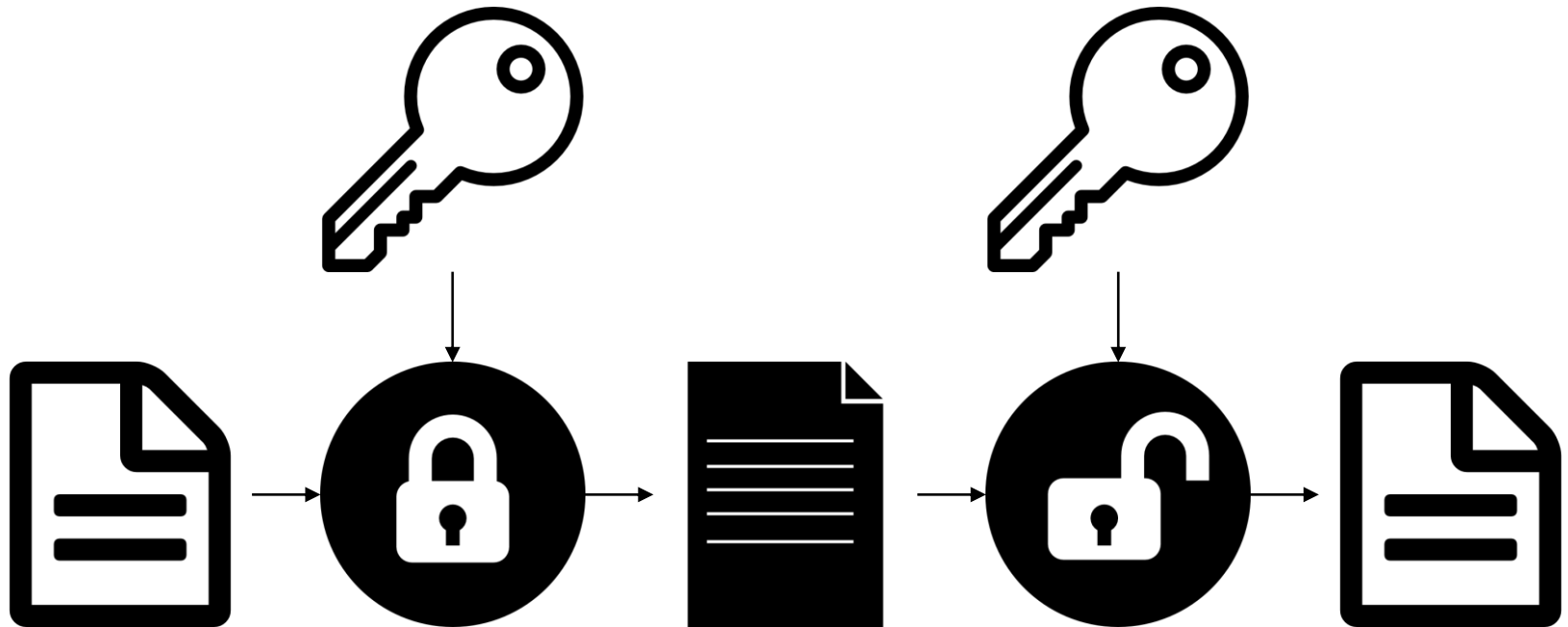
- 네트워크상의 모든 패킷 데이터는 공격자(Attacker)에게 노출될 수 있음
- 통신 과정에서 데이터를 보호하기 위해서는 암호화가 필요



RSA Introduction

Block Cipher (= Symmetric Key Cryptosystem)

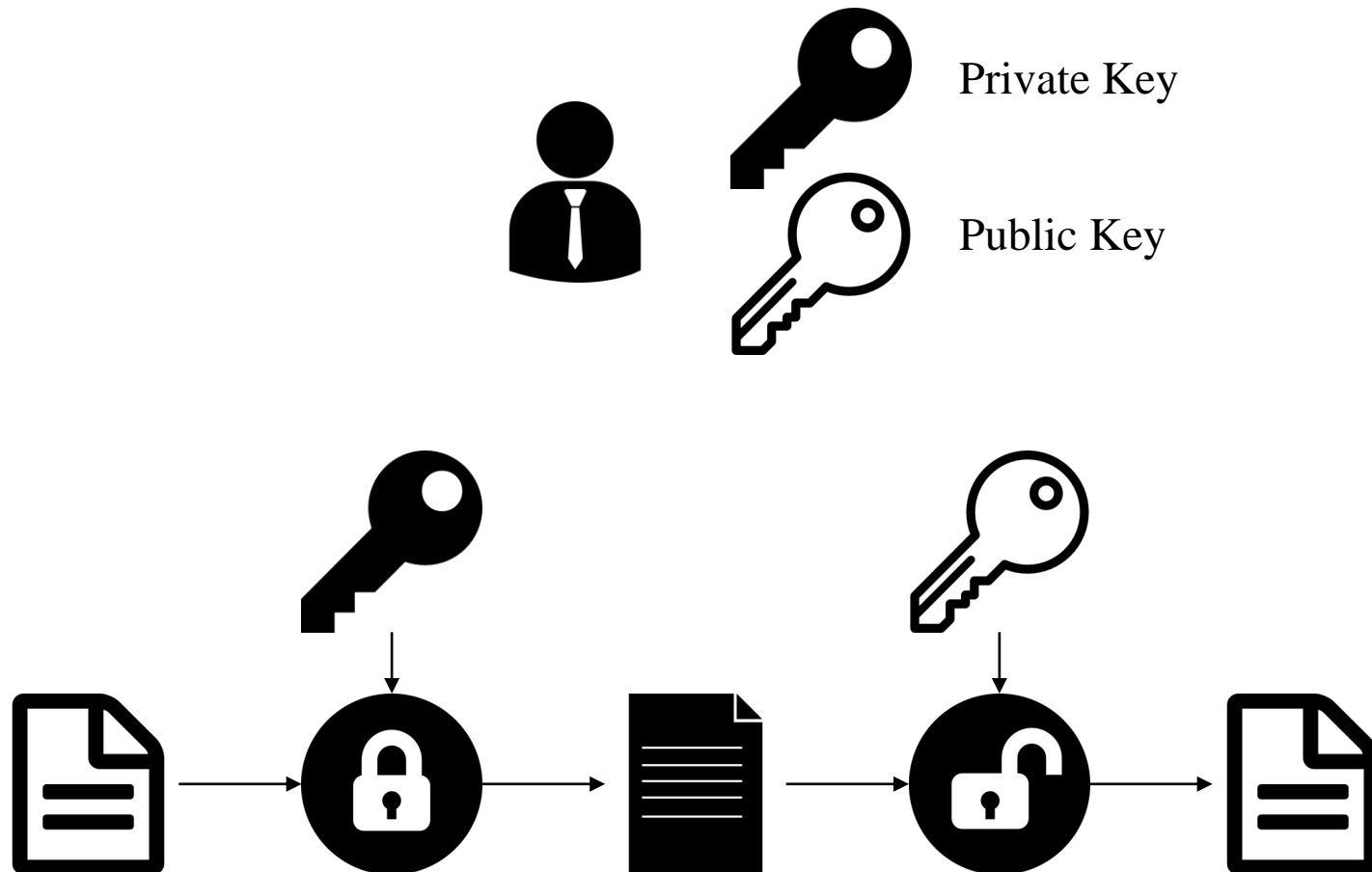
- 일반적인 데이터 암호화 알고리즘(AES, DES 등)을 수행하기 위해서는 두 통신 당사자끼리 미리 키(key)를 공유하고 있어야 함
- 키 정보 또한 상대방과 공유되는 과정에서 암호화된 상태로 전달되어야 함
- 그렇다면, 처음으로 통신을 수행하고자 하는 두 대상이 최초의 키를 어떻게 공유할 것인가?



RSA Introduction

Public Key Cryptosystem (=Asymmetric Key Cryptosystem)

- 암호화 알고리즘과 복호화 알고리즘에서 서로 다른 키를 사용하는 공개키 암호(비대칭키 암호: RSA, ECC 등) 알고리즘을 이용
- 두 암호화 키 중 하나(Public Key)는 공개되어도 상관없음



RSA Algorithm

Key Generation

1. 서로다른 두 소수 p, q 를 구한다.
Find two prime number p, q ($p \neq q$)

2. $N = pq$ 를 구한다.
Calculate $N = pq$

3. $\varphi(N) = (p - 1)(q - 1)$ 을 구한다.
Calculate $\varphi(N) = (p - 1)(q - 1)$

4. $\varphi(N)$ 보다 작고, $\varphi(N)$ 와 서로소인 정수 e 를 찾는다.
Finds an integer e that is smaller than $\varphi(N)$ and is prime to $\varphi(N)$.

5. $d \times e$ 를 $\varphi(N)$ 로 나누었을 때 나머지가 1인 정수 d 를 구한다. ($de \equiv 1 \pmod{\varphi(N)}$)
Find d (where $de \equiv 1 \pmod{\varphi(N)}$)

- Public Key: $\langle N, e \rangle$
- Private Key: $\langle N, d \rangle$

1. $p = 61, q = 53$

2. $N = 61 \times 53 = 3233$

3. $\varphi(N) = (p - 1)(q - 1) = 60 \times 52 = 3120$

4. $e = 17$

5. $17 \times 1 \pmod{3120} = 17,$
 $17 \times 2 \pmod{3120} = 34,$
 $17 \times 3 \pmod{3120} = 51,$
...
...
 $17 \times 2753 \pmod{3120} = 46801 \pmod{3120} = 1$

- Public Key: $\langle 3233, 17 \rangle$

- Private Key: $\langle 3233, 2753 \rangle$

RSA Algorithm

Encryption and Decryption

- Public Key: $\langle N, e \rangle$
- Private Key: $\langle N, d \rangle$

메시지 데이터(Plain text): p

암호화된 데이터(Cipher):

$$c = p^e \bmod N$$

복호화된 데이터(Plain text):

$$p = c^d \bmod N$$

- Public Key: $\langle 3233, 17 \rangle$
- Private Key: $\langle 3233, 2753 \rangle$

메시지 데이터(Plain text): 65

암호화된 데이터(Cipher):

$$c = 65^{17} \bmod 3233 = 2790$$

복호화된 데이터(Plain text):

$$p = 2790^{2753} \bmod 3233 = 65$$

$$2790^8 \bmod 3233 = (3671416253212328096100000000) \bmod 3233$$

$$\begin{aligned} &= (2790^2)^4 \bmod 3233 = (7784100)^4 \bmod 3233 \\ &= (7784100 \bmod 3233)^4 \bmod 3233 \\ &= (2269)^4 \bmod 3233 \\ &= (2269^2)^2 \bmod 3233 \\ &= (5148361 \bmod 3233)^2 \bmod 3233 \\ &= (1425)^2 \bmod 3233 \end{aligned}$$

```

934772766649662382134707553083402313835670595913204338449134286497412836201158026316780668839701480660675266904353173830851725485708076732240481058914495564523184436256674272296355746014291
622958166479993341839396873579239778317745051707789133784215546449931534176451102653057197630683994888478529144576217869716211520843957282083767080336902291639712559402889493508305460530406
397747292647578329629370808846888105446246734664322205811843653374793835460290366273381558603713840395530161468347254654051521982237832123727150881633320975704628138940107495451180106767456
623219290554345754891019227750603551806961131541980080816743220503641189687060703746566645384720097750832643471899819924927481006509649438671176672358601476428087142686755597023524337832552
298971068278827995585609648183862904802662868617117248477114131928198703145429364821938268724927257831358739433251361153472436981172190498227867345540240906481133290224637172484503238137308
3714520649206287295656073281665308233713090388213853720012229137713680036680921369158173048423920468254031313963319328632814364596917000316142382243303788344042648832919553147040630440999332
617023526110717704249249306436525385067847171965963909727350909060566759029290214725739310151076128819851797700083387579087855600462733765967660478947602374292284539817047198667402486878803
559156689401781096150051237170094320051623100072055663199393383390790504777323885624907112847884689926400876846771028083925757689951042982293896240176861207708670616653124236165722092078
180178704060564363023556751471324357266812256645188996827818961495565728551702078246963030962059774275394054348269760089976665725065975620894908281033248601242731471460678935036968988991
117659296481628443469306893922910728009132121463646572708909116164259658912709811572453620648477238312839123516717975889196810311956233205136808821056291031552679950396032262868386375548200
176547339636671359268425361027180323651867525273111584454301911506865887959851776793130030281513666642156726528980905481548529467387944611070432284702854206290618038613101710989263840937968
077097299215845338837615521883891735256246138252471621941965698890837770795110487986710256526364080211537071671701922328269087773232845458975422383615599647288063714281899303887222157008167
438449234792134286254600631093380549866911901749681379640589272079960664743311924531396648265015848459953360894238127925466827543805740727478164211719330561323209836633511652209520380547377
936006510846034239071572446537699822234699978294007715427082637504248658093952216254318982066828042322693414048281306266358163639251929325954580688733005557414080887974824603190192353255828
516782643007583327808205897016829088167107040024804725659841289921085792092706002514819400959596229225874897583947863250999586524967075754489281310371373817669810718241589382642311155508390
09374345267274115347583024488014625815307114272303140689204208143128996454997742320553552663730221093262814063539682216407500764453100414064555415188239572473723912296474363032440691535018
160962499817796052764636777181727806030612933796554165394730491651363903828549522750678512854082193744445220851049791730834170719141742439260227095226573949874684070636273845514101060801685
850847445627189539932196748842806758546676187417404509647969407042875720278692036472064945099698941615223202876174614046295942248392274524083685795328875203737599375082135974372781606976455
762404009212536755921136446867049627790812225927980439534784095011282141538916778916037955032558235831203029476152739585233289729453457490245028184962659383773256133386255345747542738323829
77612886774649561180303401365387302393102732479103744984724964872700426344804365622452759103416387291291028946683908719193626029362123840614551172600625112067452868288445946673940301100884
651456936952576511750853271787125374186419319565004752148946330625902901770689272546969864354653804543047041582811072593805657652966635926448591722818253849194059601540640676954965536
6296387291135361428167273944581352718740735616970964882945072502715423437352140244693120767903994974374337271974694890080594501693124468068503239747772813688616998052974800006947967323722
62428106245077976040328578677352792961995411757398197769354543220838543657148579339265682870991284470398839254554244469589586320783615791674045816150831568917021377687762994211361067950750533
086380463843072686997039997053552066456374975584934033722613175352145316378176067446835283054984079345046505578699536947446273934110868901071138616496760501880663302701045966329314389640
948759489751669814261424633249274449744809671945167501180549521365138810222260514679319171107875858294674231377645813715607966082705801588057022944244966350232770762773644662407843139207
7146758125987215674237346318421744154518945019499619981583591197809778277445958348360044691934005957060232863946118747054037025676981486040935117945446602801857439395991761342753412662372
4495111559001279893970966563377378392105488162639786254360162128373110154892722391475031734242509442193254293275058666243399203322923972780910555760203362633801859773911803602580392
9939463580967837051758906874787829911142969713805857084915619065938084635731736384324470821180755457831781208760245235178768096383620685236031363606323934987337938114605079674204440857942
36380872724977200146376838737371730644023182620744145498882054518741367803895818998319456205328621311067464947230189696072630134577337295693914279668893919466339433323172595697833853623502
4068717373628621184441302763242863517690134837405684759053576623406177708947695344274763682156123457131637282755991652102911107608711174676830018986203229447069049328321954347380586044677
260079394318685668654040812502470483227205608034878622395477268127599367770894769534427883197103459458884800710788435820091209100460061188576490287982094722849923529754840885599601191982868519
27397347170803351887474386423106312220627531114863334566034764573109304644129712069535113408884854787673903964860038133590306493044348349111668278114462093228846663848111640701634826383463
765063637898494582320693634275893285060442554275045919304407728371621136311317057301701657082091922751124460899810102652607112492566423217900987711273960802262328744526166801745686627
80367699732436666172365674382126698904890207601856851612597653400489609392609649149873329020068064793670350461845094358961085024188561887851420211973296298497945504442807857497177318874789

```

Practice

Find the original plain text

$$p = 547$$

$$q = 593$$

$$e = 17$$

Cipher text = 132637

what is the Plain text?

Thank you

