

# 암호학 스터디 2주차

안녕하세요. 스터디장입니다.

다들 깜빡하고 있었겠지만, 암호학 스터디가 벌써 2주차입니다!

이번시간에는 저번 시간 내용을 복습하면서 새로운 내용을 나가려 합니다.

시험기간이니까 내용도 짧고 문제도 짧을거예요.

아참, 그리고 이번주부터 과제가 있습니다!

과제 기한은 1주일이며 안하시면 약간의 페널티(0.75아웃)가 있습니다.

하지만 과제를 잘하신분은 3분을 추첨하여 이익(어떤 이익일까요?)이 있을 예정입니다.

자 그러면 시작합니다.

## 1. 지난 시간

지난 시간에는 무엇을 배웠을까요? 그러게요.

혹시나 지난 시간 정리자료를 안 읽어보신분은 읽고 오시기를 추천합니다.

쉽게 읽으라고 일부로 쉽게 만들었으니, 다들 읽을 수 있을거예요

지난시간에는 비교적 간단한 암호 하나를 소개했습니다.

$$C = P + K \bmod 26$$

$$P = C - K \bmod 26$$

으로 표현할 수 있는 암호죠.

또한, 이 암호의 key space는 26(사실상 25)라는 것과

이 암호로 암호화된 암호문은 결국 25번만 복호화해보면 뚫린다는 것을 배웠습니다.

다시 한 번 해봅시다

이번에는 SOGM QFMDHC라는 문자열이 주어졌습니다.

한번 풀어보시고 다음 페이지로 넘어가시는 것을 추천합니다.

가능한 25개의 키로 다 돌려보면 쉽게 답을 찾을 수 있습니다.

SOGM QFMDHC <- K = 0

RNFL PELCGB <- K = 1

QMEK ODKBFA <- K = 2

PLDJ NCJAEZ <- K = 3

OKCI MBIZDY <- K = 4

NJBH LAHYCX <- K = 5

MIAG KZGXBW <- K = 6

LHZF JYFWAV <- K = 7

KGYE IXEVZU <- K = 8

JFXD HWDUYT <- K = 9

IEWC GVCTXS <- K = 10

HDVB FUBSWR <- K = 11

GCUA ETARVQ <- K = 12

FBTZ DSZQUP <- K = 13

EASY CRYPTO <- K = 14

DZRX BQXOSN <- K = 15

CYQW APWNRM <- K = 16

BXPV ZOVMQL <- K = 17

AWOU YNULPK <- K = 18

ZVNT XMTKOJ <- K = 19

YUMS WLSJNI <- K = 20

XTLR VKRIMH <- K = 21

WSKQ UJQHLG <- K = 22

VRJP TIPGKF <- K = 23

UQIO SHOFJE <- K = 24

TPHN RGNEID  $\leftarrow K = 25$

K=14일 때 "EASY CRYPTO"가 나오는 것을 볼 수 있네요

## 2. Known plaintext attack

비슷한 문제를 생각해봅시다.

SOGM QFMDHC가 암호문으로 주어지고, EASY CRYPTO가 평문으로 주어졌을 때, Key를 찾을 수 있을까요?

아까 암호방식에서

$$C = P + K \bmod 26$$

임을 알 수 있습니다.

그렇다면 평문과 암호문에 각각 첫글자인 E와 S를 대입하면

$S = E + K \bmod 26$ 이 되는 것을 알 수 있습니다.

$A = 0, B = 1, C = 2, \dots, Z = 25$ 니

E를 우변으로 넘기면

$$14 = K \bmod 26$$

이 되네요.

결국 Key는 14라는 것을 알 수 있습니다.

다음과 같이 Caesar암호에서는 암호문이 있고, 평문의 한 글자라도 알 수 있을 경우, 키를 얻을 수 있습니다.

다음과 같이 암호문과 평문의 쌍이 주어지는 경우에 Key를 찾는 공격을 Known plaintext attack이라고 합니다.

이상적인 암호라면 암호문과 평문의 쌍이 알려져있더라도 키를 알 수 없어야 합니다.

왜냐면 암호의 안전성은 오직 Key에만 의존해야 하기 때문입니다.

### 3. Kerckhoffs' principle

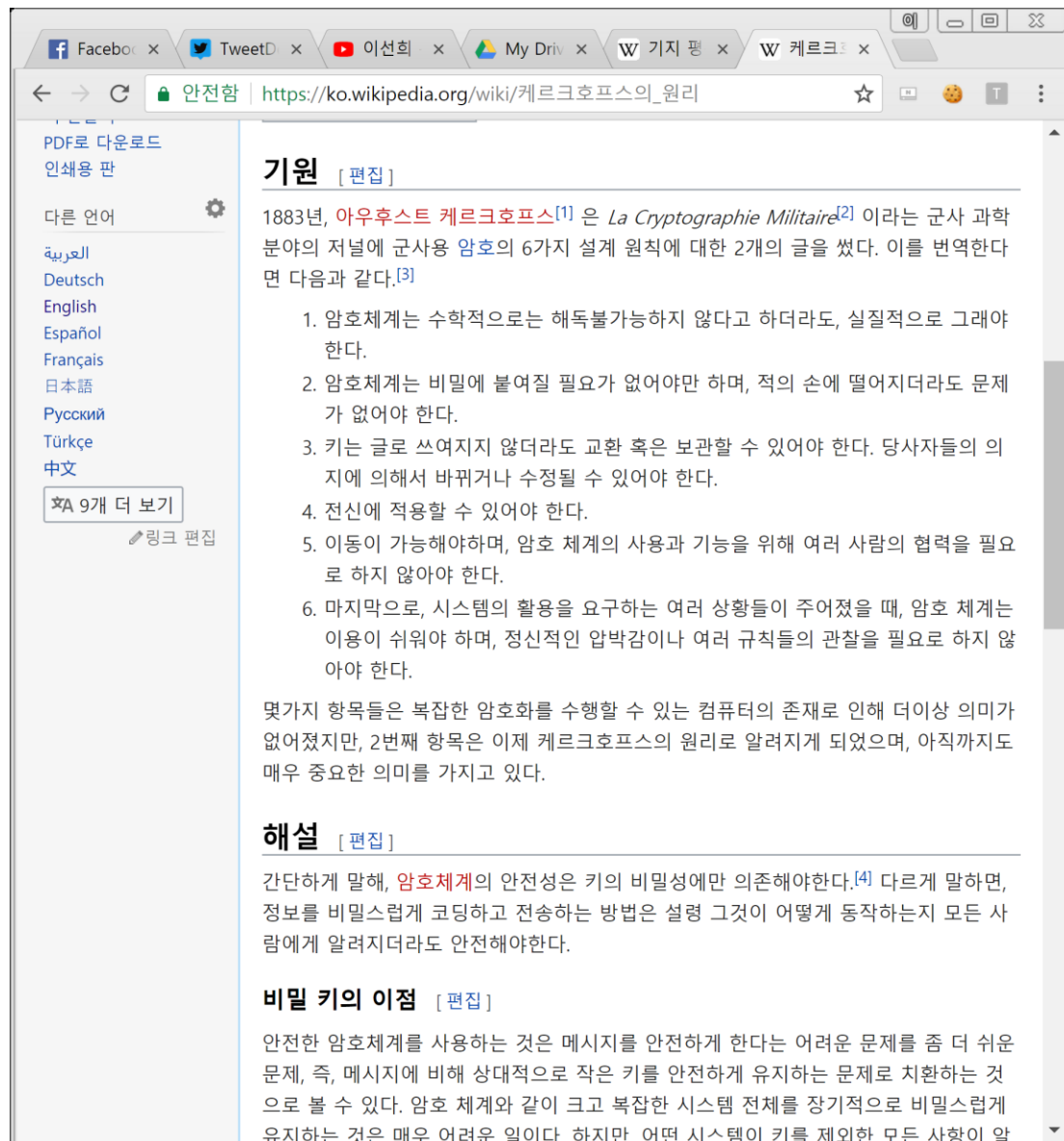
그렇다면 그냥 암호화 알고리즘을 공개하지 않으면 아까와 같이 암호문과 평문의 쌍에서 관계를 유추하지 못하는 것 아닌가요?

라는 질문이 있을 수 있습니다.

하지만 Kerckhoff 의 원리라는 것이 있습니다.

라는 원리가 있습니다.

위키백과를 참고해보죠.



The screenshot shows a web browser window with multiple tabs. The active tab is titled 'W 케르크호프스' and the address bar shows the URL 'https://ko.wikipedia.org/wiki/케르크호프스의\_원리'. The page content is in Korean and discusses Kerckhoffs' principle. It includes a list of six principles and a section on the importance of key secrecy.

**기원** [ 편집 ]

1883년, 아우구스트 케르크호프스<sup>[1]</sup> 은 *La Cryptographie Militaire*<sup>[2]</sup> 이라는 군사 과학 분야의 저널에 군사용 암호의 6가지 설계 원칙에 대한 2개의 글을 썼다. 이를 번역한다면 다음과 같다.<sup>[3]</sup>

1. 암호체계는 수학적으로는 해독불가능하지 않다고 하더라도, 실질적으로 그래야 한다.
2. 암호체계는 비밀에 붙여질 필요가 없어야만 하며, 적의 손에 떨어지더라도 문제가 없어야 한다.
3. 키는 글로 쓰여지지 않더라도 교환 혹은 보관할 수 있어야 한다. 당사자들의 의지에 의해서 바뀌거나 수정될 수 있어야 한다.
4. 전신에 적용할 수 있어야 한다.
5. 이동이 가능해야하며, 암호 체계의 사용과 기능을 위해 여러 사람의 협력을 필요로 하지 않아야 한다.
6. 마지막으로, 시스템의 활용을 요구하는 여러 상황들이 주어졌을 때, 암호 체계는 이용이 쉬워야 하며, 정신적인 압박감이나 여러 규칙들의 관찰을 필요로 하지 않아야 한다.

몇가지 항목들은 복잡한 암호화를 수행할 수 있는 컴퓨터의 존재로 인해 더이상 의미가 없어졌지만, 2번째 항목은 이제 케르크호프스의 원리로 알려지게 되었으며, 아직까지도 매우 중요한 의미를 가지고 있다.

**해설** [ 편집 ]

간단하게 말해, 암호체계의 안전성은 키의 비밀성에만 의존해야한다.<sup>[4]</sup> 다르게 말하면, 정보를 비밀스럽게 코딩하고 전송하는 방법은 설령 그것이 어떻게 동작하는지 모든 사람에게 알려지더라도 안전해야한다.

**비밀 키의 이점** [ 편집 ]

안전한 암호체계를 사용하는 것은 메시지를 안전하게 한다는 어려운 문제를 좀 더 쉬운 문제, 즉, 메시지에 비해 상대적으로 작은 키를 안전하게 유지하는 문제로 치환하는 것으로 볼 수 있다. 암호 체계와 같이 크고 복잡한 시스템 전체를 장기적으로 비밀스럽게 유지하는 것은 매우 어려운 일이다. 하지만 어떤 시스템이 키를 제외한 모든 사항이 알

2번만 중요하게 보면 됩니다.

다른 사람이 이미 암호화 알고리즘을 안다고 가정하는 상태에서 암호를 고안해야 한다는 원리입니다.

실제로 요즘 자주 쓰이는 암호(AES, RSA, ECC?는 모르겠네요)같은 것들은 다 암호화 알고리즘이 공개되어 있습니다. 찾아보면 쉽게 알 수 있습니다. 아, ECC는 빼고요.

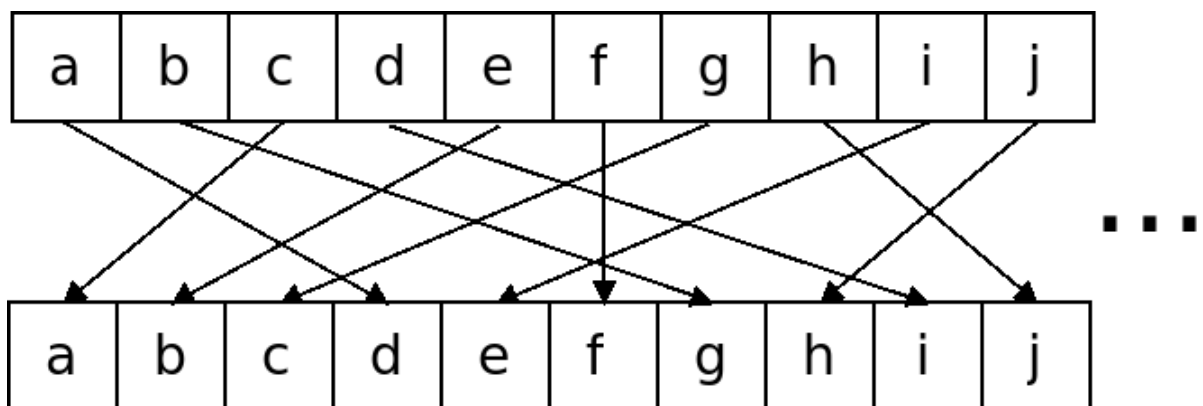
CTF에 나오는 문제 같은 경우도 보통 암호화 스크립트를 다 공개합니다.

Kerckhoff의 원리가 주는 교훈은 암호화 알고리즘을 숨긴다고 문제가 사라지지는 않는다는 것입니다.

#### 4. Substitution Cipher

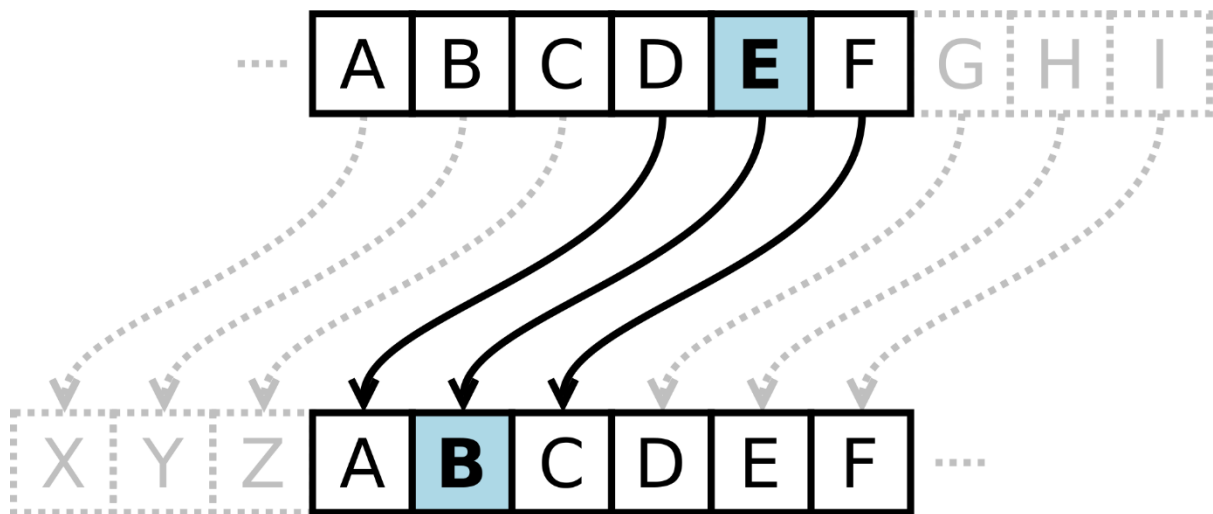
자 그러면 다음과 같은 암호를 생각해봅시다.

그림으로 표현한다면 다음과 같습니다.₩



그냥 한 글자를 자신이 원하는 다른글자에 1:1 로 대응시키는 것입니다.

지금까지 배웠던 Additive Cipher(이제는 이렇게 표현하겠습니다.)는



이런 모양이었죠.

Substitution cipher 에서의 키는 원래 알파벳과 변환된 알파벳의 1:1 관계입니다.

그렇다면 가능한 Key 의 경우는 얼마가 될까요.

A 를 다른 알파벳에 대응시키는 경우의 수 = 26

B 를 다른 알파벳에 대응시키는 경우의 수 (A 에 대응된 알파벳을 빼고)= 25

C 의 경우의 수 = 24

...

Z 의 경우의 수 = 1

다 곱하면  $26 \times 25 \times 24 \times 23 \times \dots \times 1 = 26!$ 이네요.

$\log_2(26!) \approx 86$  이니

그러면 대략 Key space 는  $2^{86}$  정도가 되겠네요.

풀기 어렵겠죠?

일단 Bruteforce Attack 으로는 힘이 많이 듭니다.

손으로 푸는거는 불가능 하고, 컴퓨터로도 조금 시간이 많이 걸리겠네요.

그렇다면 Known Ciphertext Attack 은?

가능하겠네요.

암호문과 평문의 쌍이 있으면, 그 관계에서 원래 알파벳과 바뀐 알파벳의 대응관계를 알아 낼 수 있으니, 가능합니다.

그렇다면 암호문과 평문의 쌍 없이 암호문만 주어진다면?

이번 여름학기 CTF 문제를 봅시다.

Msnjsp jf qms Pqjng (MjqP) ap h gudqakdhysn jidais ehqqds hnsih vaosj thgs osvdsjkso hio kuedapmso ey Edazzhno Siqsnqhaigsiq fjn Garnjpjfq Waiojwp hio ghrJP qmhq whp nsdshpso ji Buis 2, 2015. Qms thgs fshqunsp msnjsp fnjg Edazzhno'p fnhirmasps airduoait Whnrnhfq, Oahedj, PqhnRnhfq, Qms Djpq Vacaitp, hio Jvsnwhqrm. Qms thgs upsp ejqm fnss-qj-kdhy hio fnssgaug gjosdp hio ap pukkjqnso ey garnjkhygsiqp, wmarm rhi es upso qj kunrmhps msnjsp, vapuhd hdqsnhqajip fjn qms msnjsp ai qms thgs, hio gjuiqp. Edazzhno ojsp ijg rhdd qms thgs h "gudqakdhysn jidais ehqqds hnsih" jn hi "hrqaji nshd-qags pqnhqsty" esrhups qmsy fssd aq ap pjgsqmait oaffnsniq waqm h enjhosn kdhypqyds; qmsy nsfsn qj aq hp hi jidais "msnj enhwdsn". Msnjsp jf qms Pqjng nsjdvsp hnjuio jidais 5-vsnpup-5 ghqrmsp, jksnhqso qmnjutm Edazzhno'p jidais thgait psnvars Ehqqds.isq. Kdhysnp rhi rmijps fnjg oaffnsniq thgs gjosp, wmarm airduos kdhyait hthaiqp rjgkuqsn-rjiqnjddso msnjsp jn jqmsn kdhysnp. Aiaqahddy, ij msnjsp hns hvhadheds fjn ksnghisq ups; mjwsn, kdhysnp ghy rmijps fnjg h dapq jf msnjsp qmhq hns fnss qj ups fnjg h wsscdy njqhajip. Ey upait tjdo rjaip, qms ai-thgs runnsiry, jn qmnjutm garnjqnhiphrqajip, qmsy rhi thai ksnghisq hrrsp qj h msnj. Hp jf Ghy 2017, qmsns hns runnsiqdy 67 msnjsp ai qms thgs, oavaoso aiqj favs pskhnhqs njdsp: Hpphppai, Whnnajn, Pukkjqn, Pksrahdapq hio jis Gudqardhpp msnj. Qmsns hns runnsiqdy 13 ghkp hvhadheds qj kdhy, hdd jf wmarm mhvs oaffnsniq jebsrqavsp qj psruns, waqm pjgs mhvait oaffnsniq varqjny rjioaqajip. Sxksnasirs kjaiqp, wmarm rhi es thaiso ey esait ishney sisgy uiaqp wmsi qmsy'ns caddso, hns pmhnso hrnjpp qms siqans qshg. Wmsi h qshg nshrmsp h rsnqhai sxksnasirs kjaiqp qmnspmjdo, svsnys msnj ji qmhq qshg dsvsdp uk, hrluanait pdatmqdy hgkdafaso kjwsnp. Svsnys fsw dsvsdp, kdhysnp ghy psdsrq h qhdsiq wmarm jffsn h isw headaqy, jn hutgsiqp hi sxapqait jis. Qmap dsvsdait pypqsg sgkmhpazsp qms agkjqnhirs jf qshgwjnc hio kdhiit, pairs h kdhysnp'p hrqaji rhi hffsrq qms wmjds qshg. Kdhysnp rhi hdpj gjuiq oaffnsniq hiaghdp, purm hp mjnpsp, dazhnop, jn uiarjnip, qj airnshps qmsan gjvsgsiq pksso, huqjghqarhddy oapgjuiqait wmsi oshdait/nsrsavait ohgths jn upait hi headaqy. Hio Kdhysnp jf CUARP whnthgs rhi tsq h fdht qmnjutmq dsqqsn fnslusiry hihdypap. Aq ap "KjcKuitjPatjitApQmsEspq!"

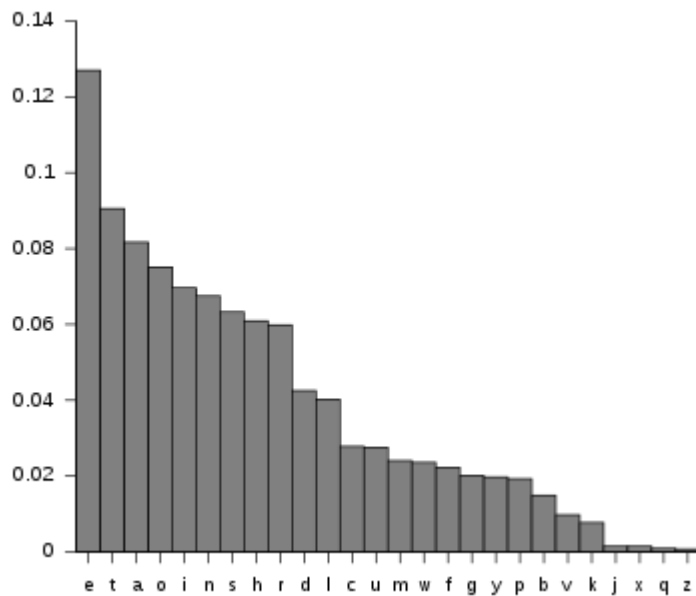


이렇게 암호문만 있으면, 쉽게 평문을 복구할 수 없습니다.

그렇다면 어떻게 해야할까요?

## 5. Statistical Attack

영어에는 다음과 같은 통계자료가 있습니다.



다음 통계자료는 영어 글자의 빈도수인데, 이 자료를 참고하면 다음과 같은 생각을 할 수 있습니다.

“저 암호문에 가장 많이 나오는 글자가 사실은 E가 아닐까?”

이렇게 알려진 통계를 이용하여 암호를 공격하는 것을 Statistical Attack, 즉 통계적 공격이라고 합니다.

실제로 영어의 글자빈도를 이용하여 암호를 해석하면,

-  
1.285 Heroes of the Storm (HotS) is a multiplayer online battle arena video game developed and published by Blizzard Entertainment for Microsoft Windows and macOS that was released on June 2, 2015. The game features heroes from Blizzard's franchises including Warcraft, Diablo, StarCraft, The Lost Vikings, and Overwatch. The game uses both free-to-play and freemium models and is supported by micropayments, which can be used to purchase heroes, visual alterations for the heroes in the game, and mounts. Blizzard does not call the game a "multiplayer online battle arena" or an "action real-time strategy" because they feel it is something different with a broader playstyle; they refer to it as an online "hero brawler". Heroes of the Storm revolves around online 5-versus-5 matches, operated through Blizzard's online gaming service Battle.net. Players can choose from different game modes, which include playing against computer-controlled heroes or other players. Initially, no heroes are available for permanent use; however, players may choose from a list of heroes that are free to use from a weekly rotation. By using gold coins, the in-game currency, or through microtransactions, they can gain permanent access to a hero. As of May 2017, there are currently 67 heroes in the game, divided into five separate roles: Assassin, Warrior, Support, Specialist and one Multiclass hero. There are currently 13 maps available to play, all of which have different objectives to secure, with some having different victory conditions. Experience points, which can be gained by being nearby enemy units when they're killed, are shared across the entire team. When a team reaches a certain experience point threshold, every hero on that team levels up, acquiring slightly amplified powers. Every few levels, players may select a talent which offers a new ability, or augments an existing one. This leveling system emphasizes the importance of teamwork and planning, since a player's action can affect the whole team. Players can also mount different animals, such as horses, lizards, or unicorns, to increase their movement speed, automatically dismounting when

```
dealing/receiving damage or using an ability.  
And Players of KUICS wargame can get a flag  
through letter frequency analysis. It is  
"PokPungofSigongIsTheBest!"
```

이런 평문을 얻을 수 있네요.

사실 Substitution Cipher 뿐 아니라 Additive Cipher 도 통계적 분석을 통하여 공격할 수 있습니다.

오늘의 이야기는 여기까지 하죠, 다들 중간고사 준비하느라 바쁘니.

# 과제

총 두문제입니다.

시험기간이기도 하고, 아직 나간게 많이 없으니 두문제만 냅니다.

쉽게 냈으니, 꼭 풀어주세요ππ

다음주 화요일 자정까지 제출해주시면 됩니다.

1. 다음 암호문에서 평문과 키를 찾으시오 (암호는 Additive Cipher라 가정)

Gur Mra bs Clguba, ol Gvz Crgref

Ornhgvshy vf orggre guna htyl.  
Rkcyvpgv vf orggre guna vzcypvg.  
Fvzcyr vf orggre guna pbzcyrk.  
Pbzcyrk vf orggre guna pbzcyvpngrq.  
Syng vf orggre guna arfgrq.  
Fcnefr vf orggre guna qrafr.  
Ernqnovyvgl pbhagf.  
Fcrpvny pnrff nera'g fcrpvny rabhtu gb oernx gur ehyrf.  
Nygubhtu cenpgvpnyvgl orngf chevgl.  
Reebef fubhyq arire cnff fvyragyl.  
Hayrff rkcyvpvgyl fvyraprq.  
Va gur snpr bs nzovthvgl, ershfr gur grzcgngvba gb thrff.  
Gurer fubhyq or bar-- naq cersrenoyl bayl bar --boivbhf jnl gb qb vg.  
Naq bs pbhefr, Synt Fubhyq or urer! Vg vf *ZnxrClgu0ater4gntn1a*  
Nygubhtu gung jnl znl abg or boivbhf ng svefg hayrff lbh'er Qhgpu.  
Abj vf orggre guna arire.  
Nygubhtu arire vf bsgra orggre guna *evtug* abj.  
Vs gur vzcyrzragngvba vf uneq gb rkcyvba, vg'f n onq vqrn.  
Vs gur vzcyrzragngvba vf mfl gb rkcyvba, vg znl or n tbbq vqrn.  
Anzrfcnprf ner bar ubaxvat terng vqrn -- yrg'f qb zber bs gubfr!

2. 다음 암호문에서 평문을 찾고, 평문을 찾는 방식을 설명하시오.

Msnjsp jf qms Pqjng (MjqP) ap h gudqakdhysn jidais ehqqds hnsih vaosj thgs osvdsjkso hio kuedapmso ey Edazzhno Siqsnqhaigsiq fjn Garnjpjfq Waiojwp hio ghrJP qmhq whp nsdshpso ji Buis 2, 2015. Qms thgs fshqunsp msnjsp fnjg Edazzhno'p fnhirmasps airduoait Whnrnhfq, Oahedj, Pqhnrnhfq, Qms Djpq Vacaitp, hio Jvsnwhqrm. Qms thgs upsp ejqm fnss-qj-kdhy hio fnssgaug gjosdp hio ap pukjinqso ey garnjkygsiqp, wmarm rhi es upso qj kunrmhps msnjsp, vapuhd hdqsnhqajip fjn qms msnjsp ai qms thgs, hio gjuiqp. Edazzhno ojsp ijg rhdd qms thgs h "gudqakdhysn jidais ehqqds hnsih" jn hi "hrqaji nshd-qags pqnhqsty" esrhups qmsy fssd aq ap pjgsqmait oaffnsiq waqm h enjhosn kdhypqyds; qmsy nsfsn qj aq hp hi jidais "msnj enhwdsn". Msnjsp jf qms Pqjng nsjdvsp hnjuio jidais 5-vsnup-5 ghqrmsp, jksnhqso qmnjutm Edazzhno'p jidais thgait psnvars Ehqqds.isq. Kdhysnp rhi rmijps fnjg oaffnsiq thgs gjosp, wmarm airduos kdhyait hthaiqp rgkuqsn-rjiqnjddso msnjsp jn jqmsn kdhysnp. Aiaqahddy, ij msnjsp hns hvhadheds fjn ksnghisq ups; mjwsn, kdhysnp ghy rmijps fnjg h dapq jf msnjsp qmhq hns fnss qj ups fnjg h

wsscdy njqhajai. Ey upait tjdo rjaip, qms ai-thgs runnsiry, jn qmnjutm garnjqnhiphrqajip, qmsy rhi thai ksnghisiq hrrspp qj h msnj. Hp jf Ghy 2017, qmsns hns runnsiqdy 67 msnjsp ai qms thgs, oavaoso aiqj favs pskhnhqs njdsp: Hpphppai, Whnnajn, Pukkjq, Pksrahdapq hio jis Gudqardhpp msnj. Qmsns hns runnsiqdy 13 ghkp hvhadheds qj kdhy, hdd jf wmarm mhvs oaffnsiq jbsrqavsp qj psruns, waqm pjgs mhvait oaffnsiq varqjny rjioaqajip.

Sxksnasirs kjaiqp, wmarm rhi es thaiso ey esait ishney sisgy uiaqp wmsi qmsy'ns caddso, hns pmhnso hrnjpp qms siqans qshg. Wmsi h qshg nshrmisp h rsnqhai sxksnasirs kjaiq qmnsprjdo, svsnj msnj ji qmhq qshg dsvsdp uk, hrluanait pdatmqdy hgkdafaso kjwsnp. Svsnj fsw dsvsdp, kdhysnp ghy psdsrq h qhdsiq wmarm jffsnp h isw headaqy, jn hutgsiqp hi sxapqait jis. Qmap dsvsdait pypqsg sgkmhpazsp qms agkjqnhirs jf qshgwjnc hio kdhiiait, pairs h kdhysn'p hrqaji rhi hffsrq qms wmjds qshg.

Kdhysnp rhi hdpj gjuiq oaffnsiq hiaghdp, purm hp mjnpsp, dazhnop, jn uiarjnip, qj airnshps qmsan gjvsgsiq pksso, huqjghqarhddy oapgjuiqait wmsi oshdait/nsrsavait ohghts jn upait hi headaqy.

Hio Kdhysnp jf CUARP whnthgs rhi tsq h fdht qmnjutmq dsqqsn fnslusiry hihdypap. Aq ap "KjcKuitjfPatjitApQmsEspq!"