**REPORT**

**[ Assignment 1: 단일치환암호 분석 ]**



|  |  |
| --- | --- |
| 과 목 명 | 정보보호론 |
| 교 수 명 | 김 효 승 |
| 학 번 | 20237107 |
| 작 성 자 | 하 태 영 |
| 제 출 일 | 2025.03.21 |

**한림대학교**

**목차**

1. 서론

2. 빈도 분석 및 방법

3. 키와 평문 도출

4. 결론

1. **서론**

**치환 암호**

* 알파벳 대칭 표를 이용하여 문자를 치환
* 사용 가능한 키의 개수 26!(약 2의 88승가지)
* 전수 키 조사가 불가능 함

**치환 암호 분석**

* 암호문의 빈도수를 찾아 평문을 추측하여 대입

1. **빈도 분석 및 방법**

**암호문**

**D**S-BVHFV E**D**M LUTH VH Y**O**G**O**H **N**U **D** TVR**J** A**D**GVSY

**D**M E**O**SS **D**M Q**J**VSUMUQ**J**Y, **JO** EUTB**O**F VH **D**M**N**TUHUGY, **D**SR**JO**GY, G**DNJO**G**DN**VRM, G**O**FVRVH**O**, P**O**UPT**D**Q**J**Y, **D**HF G**D**HY U**NJO**T **N**UQVRM.

**JO** L**O**R**D**G**O** **D** G**O**GL**O**T UA **D** MRV**O**H**N**VAVR QS**D**R**O** UA M**N**ZFY R**D**SS**O**F **NJO** **J**UZM**O** UA EVMFUG.

**J**VM **N**T**ODN**VM**O**M UH GZMVR E**O**T**O** **NJ**UZP**JN** **N**U L**O** **NJO** L**O**M**N** EUTBM UH **NJO** MZLI**O**R**N** UA GZMVR VH **D**T**D**LVR.

**자주 등장하는 주요 단어**

**NJO** -> the

**D** -> a

**빈도수**

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

1. **키와 평문 도출**

**NJO → the (N → t, J → h, O → e)**

DS-BVHFV EDM LUTH VH YeGeH tU D TVRh ADGVSY

DM EeSS DM QhVSUMUQhY, he EUTBeF VH DMtTUHUGY, DSRheGY, GDtheGDtVRM, GeFVRVHe, PeUPTDQhY, DHF GDHY UtheT tUQVRM.

he LeRDGe D GeGLeT UA D MRVeHtVAVR QSDRe UA MtZFY RDSSeF the hUZMe UA EVMFUG.

hVM tTeDtVMeM UH GZMVR EeTe thUZPht tU Le the LeMt EUTBM UH the MZLIeRt UA GZMVR VH DTDLVR.

**한자리 수로 올 수 있는 단어(i, a)**

**D → a**

aS-BVHFV EaM LUTH VH YeGeH tU a TVRh AaGVSY

aM EeSS aM QhVSUMUQhY, he EUTBeF VH aMtTUHUGY, aSRheGY, GatheGatVRM, GeFVRVHe, PeUPTaQhY, aHF GaHY UtheT tUQVRM.

he LeRaGe a GeGLeT UA a MRVeHtVAVR QSaRe UA MtZFY RaSSeF the hUZMe UA EVMFUG.

hVM tTeatVMeM UH GZMVR EeTe thUZPht tU Le the LeMt EUTBM UH the MZLIeRt UA GZMVR VH aTaLVR.

**a로 시작하는 두 글자 단어(an, at, as, aw)**

**aM → as (M → s)**

aS-BVHFV Eas LUTH VH YeGeH tU a TVRh AaGVSY

as EeSS as QhVSUsUQhY, he EUTBeF VH astTUHUGY, aSRheGY, GatheGatVRs, GeFVRVHe, PeUPTaQhY, aHF GaHY UtheT tUQVRs.

he LeRaGe a GeGLeT UA a sRVeHtVAVR QSaRe UA stZFY RaSSeF the hUZse UA EVsFUG.

hVs tTeatVses UH GZsVR EeTe thUZPht tU Le the Lest EUTBs UH the sZLIeRt UA GZsVR VH aTaLVR.

**tU → to (U → o)**

aS-BVHFV Eas LoTH VH YeGeH to a TVRh AaGVSY

as EeSS as QhVSosoQhY, he EoTBeF VH astToHoGY, aSRheGY, GatheGatVRs, GeFVRVHe, PeoPTaQhY, aHF GaHY otheT toQVRs.

he LeRaGe a GeGLeT oA a sRVeHtVAVR QSaRe oA stZFY RaSSeF the hoZse oA EVsFoG.

hVs tTeatVses oH GZsVR EeTe thoZPht to Le the Lest EoTBs oH the sZLIeRt oA GZsVR VH aTaLVR.

**otheT → other (T → r)**

aS-BVHFV Eas LorH VH YeGeH to a rVRh AaGVSY

as EeSS as QhVSosoQhY, he EorBeF VH astroHoGY, aSRheGY, GatheGatVRs, GeFVRVHe, PeoPraQhY, aHF GaHY other toQVRs.

he LeRaGe a GeGLer oA a sRVeHtVAVR QSaRe oA stZFY RaSSeF the hoZse oA EVsFoG.

hVs treatVses oH GZsVR Eere thoZPht to Le the Lest EorBs oH the sZLIeRt oA GZsVR VH araLVR.

**hVs → his (V → i)**

aS-BiHFi Eas LorH iH YeGeH to a riRh AaGiSY

as EeSS as QhiSosoQhY, he EorBeF iH astroHoGY, aSRheGY, GatheGatiRs, GeFiRiHe, PeoPraQhY, aHF GaHY other toQiRs.

he LeRaGe a GeGLer oA a sRieHtiAiR QSaRe oA stZFY RaSSeF the hoZse oA EisFoG.

his treatises oH GZsiR Eere thoZPht to Le the Lest EorBs oH the sZLIeRt oA GZsiR iH araLiR.

**oH → on, iH → in (H → n)**

aS-BinFi Eas Lorn in YeGen to a riRh AaGiSY

as EeSS as QhiSosoQhY, he EorBeF in astronoGY, aSRheGY, GatheGatiRs, GeFiRine, PeoPraQhY, anF GanY other toQiRs.

he LeRaGe a GeGLer oA a sRientiAiR QSaRe oA stZFY RaSSeF the hoZse oA EisFoG.

his treatises on GZsiR Eere thoZPht to Le the Lest EorBs on the sZLIeRt oA GZsiR in araLiR.

**Eas → was, Eere → were**

aS-BinFi was Lorn in YeGen to a riRh AaGiSYLorn

as weSS as QhiSosoQhY, he worBeF in astronoGY, aSRheGY, GatheGatiRs, GeFiRine, PeoPraQhY, anF GanY other toQiRs.

he LeRaGe a GeGLer oA a sRientiAiR QSaRe oA stZFY RaSSeF the hoZse oA wisFoG.

his treatises on GZsiR were thoZPht to Le the Lest worBs on the sZLIeRt oA GZsiR in araLiR.

**Lorn → born, Le → be, Lest → best**

aS-BinFi was born in YeGen to a riRh AaGiSY

as weSS as QhiSosoQhY, he worBeF in astronoGY, aSRheGY, GatheGatiRs, GeFiRine, PeoPraQhY, anF GanY other toQiRs.

he beRaGe a GeGber oA a sRientiAiR QSaRe oA stZFY RaSSeF the hoZse oA wisFoG.

his treatises on GZsiR were thoZPht to be the best worBs on the sZbIeRt oA GZsiR in arabiR.

**oA → of**

aS-BinFi was born in YeGen to a riRh faGiSY

as weSS as QhiSosoQhY, he worBeF in astronoGY, aSRheGY, GatheGatiRs, GeFiRine, PeoPraQhY, anF GanY other toQiRs.

he beRaGe a GeGber of a sRientifiR QSaRe of stZFY RaSSeF the hoZse of wisFoG.

his treatises on GZsiR were thoZPht to be the best worBs on the sZbIeRt of GZsiR in arabiR.

**anF → and**

aS-Bindi was born in YeGen to a riRh faGiSY

as weSS as QhiSosoQhY, he worBed in astronoGY, aSRheGY, GatheGatiRs, GediRine, PeoPraQhY, and GanY other toQiRs.

he beRaGe a GeGber of a sRientifiR QSaRe of stZdY RaSSed the hoZse of wisdoG.

his treatises on GZsiR were thoZPht to be the best worBs on the sZbIeRt of GZsiR in arabiR.

**as weSS as → as well as**

al-Bindi was born in YeGen to a riRh faGilY

as well as QhilosoQhY, he worBed in astronoGY, alRheGY, GatheGatiRs, GediRine, PeoPraQhY, and GanY other toQiRs.

he beRaGe a GeGber of a sRientifiR QlaRe of stZdY Ralled the hoZse of wisdoG.

his treatises on GZsiR were thoZPht to be the best worBs on the sZbIeRt of GZsiR in arabiR.

**riRh → rich**

al-Bindi was born in YeGen to a rich faGilY

as well as QhilosoQhY, he worBed in astronoGY, alcheGY, GatheGatics, Gedicine, PeoPraQhY, and GanY other toQics.

he becaGe a GeGber of a scientific Qlace of stZdY called the hoZse of wisdoG.

his treatises on GZsic were thoZPht to be the best worBs on the sZbIect of GZsic in arabic.

**becaGe → became GeGber → member**

al-Bindi was born in Yemen to a rich familY

as well as QhilosoQhY, he worBed in astronomY, alchemY, mathematics, medicine, PeoPraQhY, and manY other toQics.

he became a member of a scientific Qlace of stZdY called the hoZse of wisdom.

his treatises on mZsic were thoZPht to be the best worBs on the sZbIect of mZsic in arabic.

**worBs → works**

al-kindi was born in Yemen to a rich familY

as well as QhilosoQhY, he worked in astronomY, alchemY, mathematics, medicine, PeoPraQhY, and manY other toQics.

he became a member of a scientific Qlace of stZdY called the hoZse of wisdom.

his treatises on mZsic were thoZPht to be the best works on the sZbIect of mZsic in arabic.

**familY→ family**

al-kindi was born in yemen to a rich family

as well as QhilosoQhy, he worked in astronomy, alchemy, mathematics, medicine, PeoPraQhy, and many other toQics.

he became a member of a scientific Qlace of stZdy called the hoZse of wisdom.

his treatises on mZsic were thoZPht to be the best works on the sZbIect of mZsic in arabic.

**Qlace → place**

al-kindi was born in yemen to a rich family

as well as philosophy, he worked in astronomy, alchemy, mathematics, medicine, PeoPraphy, and many other topics.

he became a member of a scientific place of stZdy called the hoZse of wisdom.

his treatises on mZsic were thoZPht to be the best works on the sZbIect of mZsic in arabic.

**mZsic → music, hoZse → house**

al-kindi was born in yemen to a rich family

as well as philosophy, he worked in astronomy, alchemy, mathematics, medicine, PeoPraphy, and many other topics.

he became a member of a scientific place of study called the house of wisdom.

his treatises on music were thouPht to be the best works on the subIect of music in arabic.

**PeoPraphy → geography, thouPht → thought**

al-kindi was born in yemen to a rich family

as well as philosophy, he worked in astronomy, alchemy, mathematics, medicine, geography, and many other topics.

he became a member of a scientific place of study called the house of wisdom.

his treatises on music were thought to be the best works on the subIect of music in arabic.

1. **결론**

텍스트, 폰트, 라인, 스크린샷이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

**최종 평문**

al-kindi was born in yemen to a rich family

as well as philosophy, he worked in astronomy, alchemy, mathematics, medicine, geography, and many other topics.

he became a member of a scientific place of study called the house of wisdom.

his treatises on music were thought to be the best works on the subIect of music in arabic.

**평문 해석**

알킨디는 예멘의 부유한 가정에서 태어났습니다.

철학뿐만 아니라 천문학, 연금술, 수학, 의학, 지리학 등 다양한 분야에서 활동했습니다.

그는 지혜의 집이라는 과학 연구소의 회원이 되었습니다.

음악에 관한 그의 논문은 아랍어로 된 음악의 하위 분야에 관한 최고의 작품으로 여겨졌습니다.