Tugas 2
IF4020 Kriptografi

Oleh:

Willy Wilsen 13520160

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2022/2023

Kriptanalisis pada Cipher Abjad-Tunggal

Cipherteks

XBMVHRWROMLAHZEAHUCMRGAEXBEHXRCEALFAVEYILFORGXBMVHRWROMTECLA
XUAAHTRPYLFKBYFXZEAXBMVHROBYVZMLAXRFXEBFECTLHZHZETBLHLFORGPEAA
YOEALFAEXBEHXRCEYFCHZEXBEYHLRFRGHZEAEPEHZRCATZLWEXBMVHYFYWMAL
ALAXRFXEBFECTLHZBEYCLFOEFXBMVHECPEAAYOEAKMKBEYILFOAEXBEHXRCEAY
FXLEFHHLPEAAYTPYFMEDYPVWEARGXBMVHROBYVZMRNEBHZBEEHZRUAYFCMEY
BAYOREOMVHLYFAXBLKEAPYCEUAERGZLEBROWMVZLXHBYFAGRBPYHLRFAHRRKA
XUBEHZEPEYFLFORGTBLHHEFPEAAYOEAPEARVRHYPLYFYFCKYKMWRFLYFAXBLKE
AEPVWRMECALPLWYBHEXZFLQUEAHRBEFCEBXUFELGRBPHYKWEHAUFBEYCYKWE
HRHZEUFLFLHLYHECHZEOBEEIAEPVWRMECXBMVHROBYVZMYFCHZEXWRAEWMBE
WYHECAHEOYFROBYVZMTZLXZLAXRFXEBFECTLHZXRFXEYWLFOHZEEDLAHEFXER
GXRPPUFLXYHLRFBYHZEBHZYFXRFHEFHGRBPLWLHYBMYFCHYXHLXYWVUBVRAEA
ENEFHZEIYPYAUHBYRGYFXLEFHLFCLYHRUXZEARFXBMVHROBYVZMWLAHLFOAEXB
EHTBLHLFOYARFERGHZEALDHMGRUBGUFCYPEFHYWYBHAZUFCBECARGRHZEBED
YPVWEARXXUBLFYFXLEFHXLNLWLSYHLRFALFAZRBHXBMVHROBYVZMZYAYVVEYBE
CPRBERBWEAAAVRFHYFERUAWMLFENEBMXUWHUBELFTZLXZWLHEBYXMZYAKEXR
PETLCEAVBEYCXBMVHYFYWMALARFHZERHZEBZYFCHRRIXRFALCEBYKWMWRFOEB
HRCENEWRVYAYBLORBRUAAUKJEXHRGAHUCMHZEEYBWLEAHAUBNLNLFOCEAXBL
VHLRFARGAMAHEPYHLXPEHZRCARGXRCEKBEYILFOXRPEGBRPGLGHEEFHZXEFHU
BMLFHZEYBYKLXEFXMXWRVECLYAUKZYWYAZYLHOLNEAHZEGLBAHIFRTFTBLHHEF
CEAXBLVHLRFRGHZEHEXZFLQUERGGBEQUEFXMYFYWMALATZEBEHZEGBEQUEFXL
EARGWEHHEBAYFCWEHHEBOBRUVLFOARGYWYFOUYOEYBEUAECHRUFBYNEWAEX
BEHXRCEAXBMVHRWROMZYAVWYMECYBRWELFVRWLHLXYWYFCPLWLHYBMPYHHE
BAGBRPPECLENYWHLPEAHZBRUOZHZEXEFHUBMVEBZYVAPRAHGYPRUALAHZEXB
MVHRWROLXEGGRBHRGOBEYHKBLHYLFYFCHZEUFLHECAHYHEACUBLFOTRBWCTY
BLLHZEEGGRBHARGHZLBHMHZRUAYFCEPVWRMEEAYHKBLHYLFAKWEHXZWEMVYB
ILFXBMVHYFYWMSLFOOEBPYFMAEFLOPYHBYFAPLAALRFALAAYLCHRZYNEAZRBHE
FECHZETYBKMAENEBYWMEYBAYFCLHWECHRHZECENEWRVPEFHRGHZEGLBAHCL
OLHYWXRPVUHEBXRWRAAUAALPLWYBEGGRBHALFHZEUFLHECAHYHEAHRKBEYIJY
VYFEAEXRCEAYLCECYPEBLXYFLFHEWWLOEFXELFHZETYBXRFNLFXLFOYPEBLXYF
YUHZRBLHLEARGHZELPVRBHYFXERGXBMVHRWROLXEDVEBHLAEYFCENEFHUYWW
MWEYCLFOHRHZEEAHYKWLAZPEFHRGHZEFYHLRFYWAEXUBLHMYOEFXMLFTLHZH
ZEBLAERGCLOLHYWXRPVUHEBFEHTRBIALFHZEAEXUBLFOXRPPUFLXYHLRFKEXYP
EYFLFXBEYALFOWMLPVRBHYFHHYAILFHZEVBLNYHEAEXHRBYATEWWHZEFEECARG
HZEKYFILFOLFCUAHBMLFVYBHLXUWYBGRBAEXUBECLOLHYWXRPPUFLXYHLRFKEX
YPEEAVEXLYWWMUBOEFHCENEWRVPEFHAYHLKPWECHRHZECEALOFRGWUXLGEB
RFERGHZEGLBAHVUKWLXXLVZEBAGRBXRPVUHEBXRPPUFLXYHLRFAHZEFYHLRFY
WAEXUBLHMYOEFXMRGGEBECAENEBYWLPVBRNEPEFHAHRWUXLGEBYFCLFHZEFY
HLRFYWKUBEYURGAHYFCYBCAVBEAEFHECHZEPRCLGLECNEBALRFYAHZECYHYEF
XBMVHLRFAHYFCYBCRBCEAHZUAHZEGLBAHVUKWLXAHYFCYBCGRBEFXBMVHLRFK
EOYFHROYLFTLCEAVBEYCUAEYPEHZRCRGAEXUBLFOXRPPUFLXYHLRFLAXYWWEC
YXBMVHRAMAHEPHZEAEFCEBEFXBMVHARBEFXLVZEBAYPEAAYOEUALFOYFEFXBM
VHLRFYWORBLHZPHROEHZEBTLHZYAEXBEHIEMHZLAVBRCUXEAYXLVZEBHEDHTZL
XZLAAEFHHRHZEBEXLVLEFHHZEBEXLVLEFHTZRYWARVRAAEAAEAYIEMBEXELNEAH

ZEXLVZEBHEDHYFCCEXBMVHARBCEXLVZEBAUALFOHZEIEMHRBEXRNEBHZERBLOL
FYWPEAAYOEXYWWECHZEVWYLFHEDHLFHZEZLAHRBMRGXBMVHRWROMUVHRYW
WXBMVHRAMAHEPABEQULBECHZEAEFCEBYFCHZEBEXELNEBHRYOBEEKEGRBEZY
FCRFHZEAYPEIEMYIEMHZYHZYCHRKEBLORBRUAWMVBRHEXHECGBRPEDVRAUBEH
RYFYCNEBAYBMHZLALAIFRTFYAAMPPEHBLXRBAEXBEHIEMXBMVHROBYVZMYBBYF
OLFOHRAZYBEYAEXBEHIEMKEHTEEFHTRVYBHLEALARGHEFYCLGGLXUWHVBRKWE
PYFCCREAFRHAXYWETEWWHRAXEFYBLRALFTZLXZPYFMLFCLNLCUYWARBXRPVUH
EBAPLOZHXRPPUFLXYHETLHZEYXZRHZEBLFPYBHLFZEWWPYFYVBRGEAARBYHAH
YFGRBCUFLNEBALHMYFCTZLHGLEWCCLGGLEYOBYCUYHEAHUCEFHLFHBRCUXEC
HZEXRFXEVHRGYAMPPEHBLXRBVUKWLXIEMXBMVHROBYVZMLFHZELBAEPLFYWVY
VEBFETCLBEXHLRFALFXBMVHROBYVZMHZEMAVEXUWYHECHZYHYPEHZRCRGEFXB
MVHLRFPLOZHEDLAHLFTZEBEHZEEFXBMVHLRFIEMCLGGEBECGBRPHZECEXBMVHL
RFIEMLFAUXZYAXZEPEYUAEBAEFXBMVHLRFIEMXRUWCKEYFFRUFXECHRHZEVUKW
LXYFMRUHALCEBXRUWCRKHYLFHZLAVUKWLXEFXBMVHLRFIEMYFCUAELHHRAEFC
EFXBMVHECPEAAYOEAHRHZEUAEBALFXERFWMHZEUAEBTRUWCVRAAEAHZECEXB
MVHLRFIEMRFWMAZEXRUWCRKHYLFHZECEXBMVHLRFRGHZEPEAAYOEVUKWLXIE
MXBMVHROBYVZMYWARRVEFECCRRBAGRBPYFMRHZEBYVVWLXYHLRFAAUXZYACL
OLHYWALOFYHUBEAYFCEWEXHBRFLXXYAZHZEXRFXEVHRGVUKWLXIEMXBMVHRO
BYVZMXLBXUWYHECLFHZEBEAEYBXZXRPPUFLHMGRBARPEHLPEKEGRBEHZEGLBA
HVBYXHLXYWVBRVRAYWGRBAUXZYAXZEPETYAPYCELFYUOUAHHZEBAYVUKWLXIE
MXBMVHRAMAHEPFYPECYGHEBLFNEFHRBABRFBLNEAHYCLAZYPLBYFCWEFYCWE
PYFTYALFHBRCUXECLFPYBHLFOYBCFEBAXRWUPFRFPYHZEPYHLXYWOYPEALFAXL
EFHLGLXYPEBLXYFHZEBAYXBMVHRAMAHEPRUHWLFECLFAEXHLRFZYAAUBNLNECR
NEBHTEFHMMEYBARGAHUCMKMXBMVHYFYWMAHALFHZEVUKWLXAEXHRBYFCLHL
AHZEPRAHTLCEWMUAECVUKWLXIEMXBMVHRAMAHEPLFHZETRBWCLHLAUAECYPR
FORHZEBVWYXEALFHZEAEHVBRHRXRWGRBAEXUBEXBECLHXYBCHBYFAYXHLRFAY
FCHZEAAWVBRHRXRWGRBAEXUBEXRPPUFLXYHLRFRFHZELFHEBFEHVUKWLXCLAX
UAALRFYFCBEAEYBXZLFXBMVHROBYVZMLFKUALFEAAYFCYXYCEPLYAHYBHECLFH
ZEWYAHQUYBHEBRGHZE20HZXEFHUBMYFCXRFHLFUEAYHYGUBLRUABYHEFETPEH
ZRCAGRBEFXBMVHLRFYBEVUKWLXWMYFFRUFXECBEAEYBXZEBAHZEFAHUCMHZE
AEPEHZRCAGRBTEYIFEAAEAKMYVVWMLFOHZEHRRWARGXBMVHYFYWMALA2RFW
MYGHEBLFHEFAEVUKWLXAXBUHLFMCREAYFETXBMVHRAMAHEPOYLFYAEFAERGW
EOLHLPYXMAHUCMLFOYFCUALFOPEHZRCAGRBKBEYILFOXBMVHRAMAHEPALAYFE
AAEFHLYWAHEVLFHZECENEWRVPEFHRGFETCEALOFAGRBPRBEAEXUBEXBMVHRA
MAHEPAKMWEYBFLFOZRTHZLFOAKBEYITEWEYBFZRTHRPYIEHZEPAHBRFOEBLHLAL
FHZLAAVLBLHHZYHHZLAHZEALALATBLHHEFHZLATRBIUAEAPYHZEPYHLXYWHRRWA
HRAHUCMHZEBAYVUKWLXIEMXBMVHRAMAHEPYFCAENEBYWNYBLYFHATEUAEHRR
WAGBRPFUPEBLXYWYWOEKBYYFCHZEOERPEHBMRGFUPKEBAHROEHRUBBEAUW
HAYWOEKBYLXXBMVHYFYWMALAZYAVBRNEFHRKERFERGHZEPRAHEGGEXHLNEPE
HZRCALFHZEAHUCMRGVUKWLXIEMXBMVHRAMAHEPA

Langkah-langkah

1. Mencari tabel frekuensi kemunculan huruf, bigram, dan tigram dalam Bahasa Inggris

Letter frequency	E: 610, H: 466, A: 377, L: 366, Y: 353, B: 350, R: 348, F: 347, X: 248, Z: 203, C: 174, M: 169, W: 163, V: 153, U: 144, P: 137, G: 104, O: 101, K: 61, T: 52, I: 37, N: 36, D: 10, Q: 6, S: 2, J: 2

Bigram frequency	HZ: 131, ZE: 110, LF: 94, EA: 84, YF: 79, EB: 75, HR: 74, AH: 69, BE: 69, EF: 68, XB: 64, AE: 63, HL: 63, FH: 63, RF: 60, HE: 60, BM: 58, EX: 55, VH: 54, MV: 53, EC: 53, RB: 51, LX: 48, RG: 46, PE: 45, AL: 44, YW: 44, FC: 42, YH: 42, EH: 41, LH: 41, YB: 41, XR: 40, FX: 40, BL: 40, EY: 39, LA: 38, BY: 38, CE: 37, AY: 37, HY: 37, FO: 34, LR: 34, BA: 34, FY: 33, EP: 32, AA: 30, UA: 28, WL: 28, CL: 27, NE: 27, BR: 27, XY: 27, YA: 27, FA: 26, XE: 26, FE: 25, BH: 25, UB: 25, RA: 25, PY: 24, WE: 24, AR: 24, RP: 23, GR: 23, FL: 23, RO: 22, CH: 22, WM: 22, MA: 22, ZY: 22, YV: 21, OE: 21, RU: 21, KW: 21, EM: 21, AX: 20, ZL: 20, VU: 20, IE: 20, RC: 19, YP: 19, UF: 19, WR: 18, XU: 18, XZ: 18, VZ: 18, XL: 18, OB: 17, ZR: 17, RH: 17, UK: 17, RW: 16, GH: 16, ER: 16, EW: 16, CA: 15, LE: 15, WY: 15, HA: 15, HU: 14, YC: 14, HH: 14, AU: 14, MY: 14, VB: 14, LO: 14, ML: 13, YO: 13, EE: 13, KE: 13, MX: 13, AM: 13, EG: 13, AV: 12, YL: 12, ZM: 12, ET: 12, FR: 12, PV: 12, XH: 12, HB: 12, PL: 12, CY: 12, LB: 12, BX: 11, EL: 11, PP: 11, YX: 11, EN: 11, LN: 11, GL: 11, OL: 11, WA: 11, CU: 11, YI: 10, KB: 10, VW: 10, LY: 10, RV: 10, VR: 10, OY: 10, AZ: 10, UW: 10, MH: 10, EV: 10, CR: 10, MR: 9, HX: 9, VE: 9, HT: 9, TL: 9, TZ: 9, LP: 9, ED: 9, EU: 9, AG: 9, LG: 9, UH: 9, UX: 9, PR: 9, LV: 9, GG: 9, WW: 9, UC: 8, CM: 8, OR: 8, TE: 8, BF: 8, ME: 8, PU: 8, LC: 8, BC: 8, IL: 7, GX: 7, TR: 7, AP: 7, RR: 7, RK: 7, HM: 7, WH: 7, FT: 7, GB: 7, WC: 7, GE: 7, XI: 7, GA: 6, ZH: 6, AT: 6, LW: 6, AK: 6, KM: 6, FM: 6, EO: 6, BP: 6, YK: 6, QU: 6, NL: 6, XM: 6, VY: 6, EK: 6, FI: 6, HV: 6, OM: 5, FK: 5, CT: 5, TB: 5, RN: 5, FP: 5, MW: 5, UE: 5, OH: 5, VL: 5, UY: 5, TY: 5, PA: 5, CP: 4, OA: 4, PH: 4, FB: 4, EI: 4, ZX: 4, WV: 4, GY: 4, DH: 4, XX: 4, BW: 4, OX: 4, HI: 4, RT: 4, OZ: 4, WX: 4, YU: 4, WO: 4, RY: 4, CC: 4, ZB: 3, MK: 3, RE: 3, LK: 3, RM: 3, CX: 3, XW: 3, HG: 3, BV: 3, CB: 3, RX: 3, MZ: 3, VV: 3, AW: 3, IF: 3, EQ: 3, GW: 3, CW: 3, MP: 3, NY: 3, BI: 3, VP: 3, ZP: 3, MU: 3, OF: 3, WU: 3, XA: 3, CG: 3, BT: 3, AB: 3, FZ: 3, FW: 3, WG: 3, PF: 3, YG: 3, UP: 3, FU: 3, MT: 2, TP: 2, DY: 2, OW: 2, CK: 2, KY: 2, ZF: 2, LQ: 2, IA: 2, MB: 2, DL: 2, MG: 2, BG: 2, GU: 2, ZU: 2, ZW: 2, BZ: 2, BN: 2, TF: 2, BO: 2, UV: 2, OU: 2, YN: 2, FV: 2, UO: 2, HK: 2, AC: 2, OP: 2, BK: 2, HW: 2, HC: 2, FN: 2, DV: 2, AI: 2, KU: 2, CN: 2, WP: 2, EZ: 2, BB: 2, TC: 2, MC: 2, FF: 2, KH: 2, CV: 2, GV: 2, GF: 2, TH: 2, GP: 1, YT: 1, GZ: 1, KA: 1, GT: 1, IY: 1, YR: 1, LD: 1, LS: 1, SY: 1, RI: 1, IX: 1, KJ: 1, JE: 1, OC: 1, XP: 1, PG: 1, KL: 1, KZ: 1, HO: 1, YM: 1, VA: 1, GO: 1, OT: 1, LL: 1, MS: 1, SL: 1, OO: 1, RZ: 1, IJ: 1, JY: 1, GC: 1, KP: 1, PW: 1, WK: 1, UR: 1, YE: 1, UL: 1, AF: 1, FG: 1, CF: 1, MM: 1, XC: 1, HQ: 1, BU: 1, TX: 1, PO: 1, IT: 1, IU: 1, WN: 1, YY: 1, PK: 1
Trigram frequency	HZE: 96, BMV: 49, MVH: 49, XBM: 48, YFC: 32, LRF: 32, VHR: 30, LFO: 29, HLR: 29, EFH: 29, FHZ: 25, LFH: 24, ZEB: 23, GRB: 21, AEX: 20, ALF: 19, EFX: 19, LXY: 19, IEM: 19, EXB: 17, YHL: 17, EBA: 17, FXB: 16, KWL: 16, WLX: 16, EAA: 15, EAE: 15, EHZ: 15, AHE: 15, VUK: 15, UKW: 15, ZEA: 14, EAH: 14, HRO: 14, BEY: 14, HYF: 14, VHL: 14, XRP: 14, HRA: 14, AHZ:

	13, BEH: 13, OBY: 13, BYV: 13, BLH: 13, CHZ: 13, RGH: 13, FYW: 13, ALA: 13, MAH: 13, ROB: 12, YVZ: 12, VZM: 12, FXE: 12, GHZ: 12, PEH: 12, ARG: 12, EYB: 12, RHZ: 12, UFL: 12, YPE: 12, HEB: 12, XBE: 11, CEA: 11, HLF: 11, PEA: 11, HZR: 11, YFY: 11, HEC: 11, NEB: 11, UAE: 11, ECH: 11, AMA: 11, HEP: 11, XRF: 10, AAY: 10, YOE: 10, AYF: 10, RFA: 10, XUB: 10, ZEP: 10, YHE: 10, ENE: 10, EBE: 10, MLF: 10, EBL: 10, RAM: 10, EAL: 9, ECL: 9, BYF: 9, LHL: 9, EAY: 9, EBH: 9, ERG: 9, UBE: 9, HEF: 9, RBE: 9, ZLA: 9, RPP: 9, XYW: 9, ZYA: 9, MHZ: 9, AHY: 9, AEF: 9, EXU: 9, VBR: 9, BEX: 9, EMX: 9, MXB: 9, LAH: 8, AHU: 8, HUC: 8, YLF: 8, LHZ: 8, AYO: 8, FCH: 8, ZEX: 8, EPE: 8, ZRC: 8, YWM: 8, PYF: 8, BAY: 8, PYH: 8, AHR: 8, YBH: 8, FCE: 8, PPU: 8, PUF: 8, FLX: 8, XYH: 8, LHY: 8, EBY: 8, EXH: 8, HZL: 8, RBA: 8, HRW: 7, RWR: 7, UCM: 7, RCE: 7, LFA: 7, EYI: 7, ILF: 7, RGX: 7, AXB: 7, RFX: 7, WMA: 7, CLF: 7, RUA: 7, AGR: 7, ECA: 7, HRH: 7, MYF: 7, HLX: 7, BEC: 7, UBL: 7, BLF: 7, RBH: 7, EXR: 7, CHR: 7, HRG: 7, LNE: 7, BAH: 7, ZEC: 7, RFY: 7, YWA: 7, XLV: 7, BEA: 7, LXI: 7, XIE: 7, WRO: 6, RGA: 6, XRC: 6, LAX: 6, YFX: 6, EBF: 6, BFE: 6, FEC: 6, TLH: 6, RCA: 6, TZL: 6, VHY: 6, FXL: 6, LEF: 6, EAR: 6, EUA: 6, HHE: 6, BHE: 6, HRB: 6, HZY: 6, RFH: 6, FHE: 6, XHL: 6, AEA: 6, PEF: 6, LFY: 6, LCE: 6, EPY: 6, XEF: 6, ZEG: 6, LBA: 6, ECY: 6, LFX: 6, ECE: 6, FHR: 6, BXR: 6, BLX: 6, EFY: 6, BAE: 6, AAE: 6, MRG: 5, EHX: 5, HXR: 5, GXB: 5, XZE: 5, TBL: 5, EYF: 5, AEP: 5, MAL: 5, EYC: 5, OEF: 5, KBE: 5, XLE: 5, YFM: 5, PVW: 5, RNE: 5, YFA: 5, ZLX: 5, RBP: 5, HRR: 5, FLF: 5, LHH: 5, BEF: 5, EFC: 5, CEB: 5, WEH: 5, EHR: 5, ZEU: 5, FOH: 5, ZEE: 5, VRA: 5, FHL: 5, FCL: 5, FOY: 5, FCY: 5, HYW: 5, YWY: 5, YBE: 5, YFE: 5, XUW: 5, HUB: 5, ELF: 5, LFT: 5, RPE: 5, AVB: 5, CEN: 5, NEW: 5, WRV: 5, GBR: 5, BRP: 5, EGL: 5, GLB: 5, UAL: 5, LOL: 5, OLH: 5, BHL: 5, AEY: 5, YWW: 5, ZEF: 5, EXL: 5, LVZ: 5, VZE: 5, YBC: 5, CEX: 5, EPA: 5, RFI: 5, FIE: 5, EVU: 5, ROM: 4, YIL: 4, FOR: 4, UAA: 4, EAX: 4, AXR: 4, ZHZ: 4, ZET: 4, OEA: 4, FAE: 4, RFR: 4, FRG: 4, LAL: 4, YCL: 4, FOA: 4, FHH: 4, HLP: 4, LYF: 4, XBL: 4, HBY: 4, FAH: 4, FYF: 4, PLW: 4, WYB: 4, QUE: 4, EBX: 4, YKW: 4, KWE: 4, FLH: 4, OYF: 4, LXZ: 4, YHZ: 4, WLH: 4, AEN: 4, NEF: 4, UXZ: 4, FER: 4, FAL: 4, EWR: 4, YBL: 4, BRU: 4, AAU: 4, LEA: 4, FOX: 4, GHE: 4, FHU: 4, LXE: 4, FXM: 4, AZY: 4, NEA: 4, CYB: 4, RAH: 4, EGG: 4, HYL: 4, HEA: 4, TRB: 4, LAA: 4, EFE: 4, CLH: 4, WEC: 4, CLO: 4, RPV: 4, PVU: 4, VUH: 4, UHE: 4, XRW: 4, FEA: 4, PEB: 4, XYF: 4, EWW: 4, YBX: 4, HLA: 4, FYH: 4, LHM: 4, YFH: 4, ZEV: 4, CUA: 4, GEB: 4, BRF: 4, EPR: 4, CLG: 4, ARB: 4, YWO: 4, HED: 4, HHZ: 4, WAR: 4, HBR: 4, XEC: 4, FET: 4, RUW: 4, UWC: 4, AVE: 3, ORG: 3, CLA: 3, AXU: 3, HTR: 3, KBY: 3, ZML: 3, XEB: 3, ECT: 3, CTL: 3, HZB: 3, FOE: 3, ECP: 3, AKM: 3, LPE: 3, WEA: 3, BHZ: 3, BEE: 3, MEY: 3, YBA: 3, HLY: 3, FAX: 3, EAP: 3, APY: 3, YCE: 3, AER: 3, EBR: 3, BPY: 3, PEY: 3, YFL: 3, RVR: 3, RFL: 3, EPV: 3, VWR: 3, WRM: 3, RME: 3, MEC: 3, HEX: 3, EUF: 3, OBE: 3, ZMY: 3, RAE: 3, WYH: 3, CAH: 3, XZL: 3, HZX: 3, OHZ:

	3, XER: 3, BYH: 3, ZYF: 3, LWL: 3, HYB: 3, YBM: 3, YXH: 3, YWV: 3, RGY: 3, LFC: 3, HRU: 3, ARF: 3, EHT: 3, RFE: 3, CYP: 3, BHA: 3, CBE: 3, CAR: 3, LNL: 3, ZRB: 3, MZY: 3, AYV: 3, YVV: 3, RBW: 3, WML: 3, LFE: 3, UWH: 3, FTZ: 3, LHE: 3, KEX: 3, TLC: 3, EAV: 3, VBE: 3, RFO: 3, OEB: 3, BHR: 3, BLO: 3, ORB: 3, XHR: 3, GAH: 3, CMH: 3, AUB: 3, EKB: 3, OXR: 3, EEF: 3, UBM: 3, BEQ: 3, EQU: 3, LAT: 3, RGW: 3, CWE: 3, AEC: 3, RUF: 3, WAE: 3, VWY: 3, BAG: 3, PPE: 3, OZH: 3, EXE: 3, VEB: 3, PRA: 3, GGR: 3, TYB: 3, HAR: 3, EEA: 3, AYH: 3, VYB: 3, AAL: 3, ALR: 3, ETY: 3, BYW: 3, RVP: 3, VPE: 3, YWX: 3, WXR: 3, RAA: 3, AUA: 3, HAL: 3, HRK: 3, XEL: 3, RBL: 3, ZEL: 3, LPV: 3, WEY: 3, LAZ: 3, HMY: 3, RFK: 3, FKE: 3, EXY: 3, XYP: 3, RBY: 3, TEW: 3, OLF: 3, FCU: 3, UAH: 3, UWY: 3, FHA: 3, ALO: 3, LOF: 3, AHV: 3, HVU: 3, LXX: 3, GGE: 3, GLE: 3, BAL: 3, FYA: 3, YAH: 3, YHY: 3, RBC: 3, LXA: 3, YAE: 3, EHI: 3, HIE: 3, EMH: 3, BRC: 3, RCU: 3, CUX: 3, UXE: 3, AYX: 3, EDH: 3, YIE: 3, HRY: 3, ZYH: 3, BRH: 3, FYC: 3, EHB: 3, LGG: 3, HVB: 3, FPY: 3, EPL: 3, AUX: 3, XZY: 3, AEB: 3, XRU: 3, RFW: 3, FWM: 3, BXZ: 3, WGR: 3, CAG: 3, EFA: 3, RRW: 3, RWA: 3, MLA: 2, CMR: 2, GAE: 2, VEY: 2, XUA: 2, AHT: 2, RPY: 2, LFK: 2, HZH: 2, EYH: 2, ATZ: 2, WEX: 2, ZBE: 2, VHE: 2, CPE: 2, EAK: 2, OAE: 2, EDY: 2, DYP: 2, YPV: 2, VWE: 2, ZRU: 2, UAY: 2, BLK: 2, LKE: 2, KEA: 2, PYC: 2, OWM: 2, WMV: 2, XHB: 2, FAG: 2, ARV: 2, HYP: 2, YPL: 2, PLY: 2, KMW: 2, MWR: 2, WRF: 2, CAL: 2, ALP: 2, LPL: 2, LWY: 2, EXZ: 2, XZF: 2, ZFL: 2, FLQ: 2, LQU: 2, UEA: 2, BXU: 2, HYK: 2, HAU: 2, UFB: 2, LYH: 2, ZEO: 2, CXB: 2, XWR: 2, WRA: 2, EWM: 2, MBE: 2, EWY: 2, EOY: 2, ZXR: 2, YWL: 2, WLF: 2, EDL: 2, DLA: 2, GXR: 2, RFB: 2, FBY: 2, BMY: 2, ZEI: 2, YAU: 2, CLY: 2, WLA: 2, AHL: 2, HMG: 2, MGR: 2, RUB: 2, UFC: 2, FHY: 2, FCB: 2, AZR: 2, YAY: 2, PRB: 2, ERB: 2, AAV: 2, UAW: 2, AWM: 2, XZW: 2, BYX: 2, YXM: 2, PET: 2, ETL: 2, LAR: 2, ZER: 2, EBZ: 2, BZY: 2, ALC: 2, BYK: 2, WMW: 2, RVY: 2, AYB: 2, LOR: 2, RBR: 2, AUK: 2, AHA: 2, UBN: 2, BNL: 2, NLN: 2, NLF: 2, BLV: 2, LVH: 2, EGB: 2, ZXE: 2, BML: 2, ZEY: 2, RVE: 2, LYA: 2, WYA: 2, YAZ: 2, IFR: 2, FRT: 2, RTF: 2, ZEH: 2, RGG: 2, GBE: 2, UEF: 2, TZE: 2, GWE: 2, EHH: 2, FCW: 2, VLF: 2, WYF: 2, YFO: 2, YNE: 2, YAV: 2, LFV: 2, YHH: 2, AGB: 2, PEC: 2, YWH: 2, YPR: 2, PRU: 2, ROL: 2, OLX: 2, YHK: 2, HKB: 2, KBL: 2, HYH: 2, BWC: 2, CEP: 2, MAE: 2, APL: 2, AYL: 2, YLC: 2, OYP: 2, FYU: 2, HLE: 2, PVR: 2, VRB: 2, BHY: 2, EDV: 2, LAE: 2, UYW: 2, WWM: 2, MWE: 2, OHR: 2, MYO: 2, FTL: 2, FEH: 2, RBI: 2, EYA: 2, YAL: 2, BLN: 2, ATE: 2, WWH: 2, FOL: 2, AHB: 2, HBM: 2, LXU: 2, VEX: 2, LYW: 2, WMU: 2, HAY: 2, WUX: 2, UXL: 2, XLG: 2, LGE: 2, RBX: 2, CAE: 2, BRN: 2, NEP: 2, HAH: 2, RWU: 2, EYU: 2, LGL: 2, CNE: 2, BCE: 2, OYL: 2, YCU: 2, RCR: 2, CRG: 2, AXY: 2, WWE: 2, CYX: 2, YXB: 2, PHZ: 2, VHA: 2, AYP: 2, ROE: 2, OEH: 2, EBT: 2, LAV: 2, XEA: 2, HTZ: 2, HHR: 2, LVL: 2, VLE: 2, FHT: 2, RYW: 2, ELN: 2, FCC: 2, BAU: 2, EIE: 2, BMR: 2, LBE: 2, YOB: 2, EKE: 2, KEG: 2, EGR: 2, EMY: 2, RKE: 2, KEB: 2, ECG: 2, CGB: 2, YAA: 2, AMP: 2,

	MPP: 2, HBL: 2, LXR: 2, XRB: 2, HTE: 2, GGL: 2, GLX: 2, WEP: 2, CCR: 2, CRE: 2, REA: 2, WHR: 2, FYB: 2, BLR: 2, CUY: 2, PLO: 2, LOZ: 2, LFP: 2, PYB: 2, ZEW: 2, BRG: 2, RGE: 2, CEF: 2, FHB: 2, XEV: 2, EVH: 2, PLF: 2, ETC: 2, RFP: 2, YAX: 2, AXZ: 2, YFF: 2, FFR: 2, FRU: 2, UFX: 2, FMR: 2, RUH: 2, WCR: 2, CRK: 2, RKH: 2, KHY: 2, ERF: 2, VVW: 2, CEW: 2, EWE: 2, RGV: 2, GVU: 2, BAR: 2, WVB: 2, AYW: 2, TYA: 2, YVU: 2, YGH: 2, FRF: 2, AEH: 2, EHV: 2, RHR: 2, HRX: 2, RXR: 2, RWG: 2, FAY: 2, ZLF: 2, WMY: 2, WAH: 2, RGF: 2, YBF: 2, ZRT: 2, RTH: 2, FUP: 2, WOE: 2, OEK: 2, OML: 1, FAV: 1, OMT: 1, MTE: 1, TEC: 1, AAH: 1, TRP: 1, PYL: 1, FKB: 1, FXZ: 1, ETB: 1, RGP: 1, GPE: 1, CEY: 1, CAT: 1, ZLW: 1, LWE: 1, KMK: 1, MKB: 1, HHL: 1, AYT: 1, YTP: 1, TPY: 1, FME: 1, MED: 1, ZMR: 1, MRN: 1, EEH: 1, FCM: 1, CME: 1, YOR: 1, ORE: 1, REO: 1, EOM: 1, OMV: 1, CEU: 1, RGZ: 1, GZL: 1, ZLE: 1, LEB: 1, BRO: 1, ROW: 1, MVZ: 1, VZL: 1, LXH: 1, RRK: 1, RKA: 1, KAX: 1, RGT: 1, GTB: 1, EFP: 1, FPE: 1, APE: 1, VRH: 1, RHY: 1, FCK: 1, CKY: 1, KYK: 1, YKM: 1, FLY: 1, XUF: 1, UFE: 1, FEL: 1, ELG: 1, LGR: 1, BPH: 1, PHY: 1, EHA: 1, AUF: 1, FBE: 1, YCY: 1, CYK: 1, LFL: 1, EOB: 1, EEI: 1, EIA: 1, IAE: 1, ECX: 1, EXW: 1, AEW: 1, WMB: 1, BEW: 1, HEO: 1, YFR: 1, FRO: 1, ZMT: 1, MTZ: 1, XEY: 1, EYW: 1, EED: 1, FXR: 1, FHG: 1, HGR: 1, BPL: 1, CHY: 1, HYX: 1, WVU: 1, VUB: 1, UBV: 1, BVR: 1, EIY: 1, IYP: 1, YPY: 1, PYA: 1, AUH: 1, UHB: 1, BYR: 1, YRG: 1, GYF: 1, YHR: 1, RUX: 1, ZMW: 1, MWL: 1, HTB: 1, OYA: 1, YAR: 1, ALD: 1, LDH: 1, DHM: 1, GRU: 1, UBG: 1, BGU: 1, GUF: 1, HAZ: 1, AZU: 1, ZUF: 1, RGR: 1, GRH: 1, BED: 1, ARX: 1, RXX: 1, XXU: 1, FHX: 1, HXL: 1, XLN: 1, NLW: 1, WLS: 1, LSY: 1, SYH: 1, FAZ: 1, BHX: 1, HXB: 1, ZMZ: 1, VVE: 1, CPR: 1, BER: 1, BWE: 1, AAA: 1, AVR: 1, VRF: 1, ERU: 1, FEN: 1, EBM: 1, BMX: 1, MXU: 1, WHU: 1, BEL: 1, ZWL: 1, XMZ: 1, YAK: 1, AKE: 1, YCX: 1, ERH: 1, RRI: 1, RIX: 1, IXR: 1, KWM: 1, HRC: 1, VYA: 1, UKJ: 1, KJE: 1, JEX: 1, EEY: 1, YBW: 1, BWL: 1, WLE: 1, FOC: 1, OCE: 1, FAR: 1, GAM: 1, LXP: 1, XPE: 1, CEK: 1, PEG: 1, RPG: 1, PGL: 1, GLG: 1, LGH: 1, HEE: 1, YBY: 1, YKL: 1, KLX: 1, XMX: 1, MXW: 1, VEC: 1, UKZ: 1, KZY: 1, ZYW: 1, ZYL: 1, YLH: 1, LHO: 1, HOL: 1, OLN: 1, AHI: 1, HIF: 1, TFT: 1, FTB: 1, EHE: 1, UER: 1, GGB: 1, XMY: 1, EBO: 1, BOB: 1, OBR: 1, RUV: 1, UVL: 1, OAR: 1, GYW: 1, FOU: 1, OUY: 1, UYO: 1, OEY: 1, BEU: 1, BYN: 1, EWA: 1, OMZ: 1, AVW: 1, WYM: 1, YME: 1, YBR: 1, BRW: 1, RWE: 1, WEL: 1, FVR: 1, VRW: 1, RWL: 1, FCP: 1, CPL: 1, BMP: 1, MPY: 1, CLE: 1, LEN: 1, ENY: 1, NYW: 1, WHL: 1, ZBR: 1, RUO: 1, UOZ: 1, MVE: 1, ZYV: 1, YVA: 1, VAP: 1, APR: 1, AHG: 1, HGY: 1, GYP: 1, XEG: 1, RGO: 1, GOB: 1, EAC: 1, ACU: 1, CUB: 1, FOT: 1, OTR: 1, WCT: 1, CTY: 1, BLL: 1, LLH: 1, EEG: 1, ZLB: 1, LBH: 1, BHM: 1, HMH: 1, MEE: 1, FAK: 1, AKW: 1, HXZ: 1, ZWE: 1, WEM: 1, EMV: 1, MVY: 1, YBI: 1, BIL: 1, WMS: 1, MSL: 1, SLF: 1, FOO: 1, OOE: 1, EBP: 1, FMA: 1, EFL: 1, FLO: 1, LOP: 1, OPY: 1, YHB: 1, FAP: 1, PLA: 1, LCH: 1, HRZ: 1, RZY: 1, ZYN: 1, EAZ: 1, YBK: 1, BKM: 1, KMA: 1, WME:

	1, LHW: 1, HWE: 1, AHC: 1, HCL: 1, BEG: 1, RKB: 1, YIJ: 1, IJY: 1, JYV: 1, YVY: 1, VYF: 1, CEC: 1, HEW: 1, WWL: 1, WLO: 1, LOE: 1, RFN: 1, FNL: 1, XLF: 1, YUH: 1, UHZ: 1, ELP: 1, XED: 1, DVE: 1, HUY: 1, AZP: 1, ZPE: 1, XML: 1, BLA: 1, RGC: 1, GCL: 1, BIA: 1, IAL: 1, FOW: 1, MLP: 1, HHY: 1, HYA: 1, YAI: 1, AIL: 1, EVB: 1, VBL: 1, LNY: 1, NYH: 1, BYA: 1, YAT: 1, WHZ: 1, FEE: 1, EEC: 1, ZEK: 1, EKY: 1, KYF: 1, YFI: 1, FIL: 1, FVY: 1, YBG: 1, BGR: 1, PEE: 1, XLY: 1, MUB: 1, UBO: 1, BOE: 1, FHC: 1, HCE: 1, HLK: 1, LKP: 1, KPW: 1, PWE: 1, OFR: 1, GWU: 1, XXL: 1, XMR: 1, WLP: 1, PVB: 1, YWK: 1, WKU: 1, KUB: 1, YUR: 1, URG: 1, BCA: 1, CAV: 1, PRC: 1, RCL: 1, LEC: 1, ECN: 1, CYH: 1, HYE: 1, YEF: 1, BCR: 1, CRB: 1, HZU: 1, ZUA: 1, XAH: 1, BCG: 1, CGR: 1, KEO: 1, ROY: 1, EYP: 1, FLA: 1, EPH: 1, OEU: 1, FEF: 1, WOR: 1, HZP: 1, ZPH: 1, PHR: 1, BTL: 1, YXL: 1, DHT: 1, TZR: 1, ZRY: 1, AYI: 1, EMB: 1, DHY: 1, CCE: 1, MHR: 1, XRN: 1, YWP: 1, WPE: 1, OEX: 1, EVW: 1, WYL: 1, DHL: 1, ZEZ: 1, EZL: 1, RBM: 1, OMU: 1, MUV: 1, UVH: 1, WWX: 1, WXB: 1, PAB: 1, ABE: 1, QUL: 1, ULB: 1, RYO: 1, EEK: 1, BEZ: 1, EZY: 1, FCR: 1, CRF: 1, PEI: 1, MYI: 1, ZYC: 1, YCH: 1, MVB: 1, RHE: 1, XHE: 1, PED: 1, DVR: 1, RAU: 1, RYF: 1, YCN: 1, BMH: 1, LAI: 1, AIF: 1, TFY: 1, AAM: 1, MYB: 1, YBB: 1, BBY: 1, RAZ: 1, ZYB: 1, EMK: 1, MKE: 1, KEH: 1, TEE: 1, TRV: 1, WHV: 1, BRK: 1, RKW: 1, EAF: 1, AFR: 1, FRH: 1, RHA: 1, HAX: 1, YWE: 1, WET: 1, ETE: 1, RAX: 1, AXE: 1, LRA: 1, RAL: 1, XZP: 1, ZPY: 1, FML: 1, CLN: 1, NLC: 1, LCU: 1, BAP: 1, ZHX: 1, HET: 1, EYX: 1, YXZ: 1, XZR: 1, ZRH: 1, LFZ: 1, FZE: 1, WWP: 1, WPY: 1, FYV: 1, YVB: 1, GEA: 1, AAR: 1, YHA: 1, YFG: 1, FGR: 1, BCU: 1, CUF: 1, FLN: 1, ALH: 1, FCT: 1, CTZ: 1, ZLH: 1, LHG: 1, HGL: 1, LEW: 1, EWC: 1, WCC: 1, CCL: 1, LEY: 1, EYO: 1, BYC: 1, UYH: 1, UCE: 1, GYA: 1, YAM: 1, RBV: 1, BVU: 1, ELB: 1, WVY: 1, VYV: 1, YVE: 1, TCL: 1, CLB: 1, ZMH: 1, ZEM: 1, EMA: 1, MAV: 1, GEF: 1, FPL: 1, ZHE: 1, EMC: 1, MCL: 1, RPH: 1, EML: 1, FAU: 1, YUA: 1, MXR: 1, WCK: 1, CKE: 1, KEY: 1, MRU: 1, UHA: 1, AVU: 1, AEL: 1, ELH: 1, WMH: 1, BTR: 1, TRU: 1, WCV: 1, CVR: 1, EMR: 1, MRF: 1, MAZ: 1, AZE: 1, OEV: 1, MYW: 1, ARR: 1, RRV: 1, VEF: 1, ECC: 1, CRR: 1, RRB: 1, MRH: 1, VWL: 1, FAA: 1, YAC: 1, ACL: 1, WAL: 1, OFY: 1, YHU: 1, XXY: 1, XYA: 1, AZH: 1, ZMX: 1, MXL: 1, XLB: 1, LBX: 1, XZX: 1, ARP: 1, EHL: 1, PEK: 1, VBY: 1, BRV: 1, RAY: 1, YWG: 1, YAP: 1, CEL: 1, YUO: 1, UOU: 1, OUA: 1, AHH: 1, EPF: 1, PFY: 1, FYP: 1, CYG: 1, LFN: 1, FNE: 1, BAB: 1, ABR: 1, FBL: 1, HYC: 1, ZYP: 1, PLB: 1, LBY: 1, WEF: 1, YCW: 1, YFT: 1, FTY: 1, OYB: 1, BCF: 1, CFE: 1, FEB: 1, BAX: 1, WUP: 1, UPF: 1, PFR: 1, WOY: 1, AXL: 1, HLG: 1, UHW: 1, HWL: 1, RFZ: 1, FZY: 1, NEC: 1, ECR: 1, CRN: 1, BHT: 1, TEF: 1, FHM: 1, HMM: 1, MME: 1, CMK: 1, MKM: 1, KMX: 1, XAE: 1, HTL: 1, MUA: 1, ECV: 1, CVU: 1, ETR: 1, WCL: 1, LAU: 1, PRF: 1, ORH: 1, EBV: 1, BVW: 1, WYX: 1, YXE: 1, LHX: 1, HXY: 1, XYB: 1, BCH: 1, CHB: 1, AAW: 1, AWV: 1, LXC: 1, XCL: 1, FKU: 1, KUA: 1, YXY: 1, XYC: 1, AHQ: 1, HQU: 1, QUY: 1, UYB: 1, FCX: 1, CXR: 1,

	LFU: 1, FUE: 1, HYG: 1, YGU: 1, GUB: 1, LRU: 1, UAB: 1, ABY: 1, ETP: 1, TPE: 1, BEV: 1, LXW: 1, XWM: 1, ECB: 1, RBT: 1, BTE: 1, TEY: 1, YIF: 1, IFE: 1, KMY: 1, MYV: 1, VWM: 1, MYG: 1, AEV: 1, XAX: 1, XBU: 1, BUH: 1, UHL: 1, LFM: 1, FMC: 1, MCR: 1, ETX: 1, TXB: 1, EPO: 1, POY: 1, WEO: 1, EOL: 1, LPY: 1, PYX: 1, XMA: 1, CML: 1, FOP: 1, OPE: 1, RBK: 1, BKB: 1, OXB: 1, PAL: 1, LAY: 1, HEV: 1, EVL: 1, GFE: 1, TCE: 1, OFA: 1, BPR: 1, PAK: 1, BFL: 1, FOZ: 1, OZR: 1, THZ: 1, OAK: 1, AKB: 1, YIT: 1, ITE: 1, BFZ: 1, FZR: 1, THR: 1, HRP: 1, PYI: 1, IEH: 1, PAH: 1, AVL: 1, VLB: 1, LBL: 1, ATB: 1, ATR: 1, BIU: 1, IUA: 1, FCA: 1, YWN: 1, WNY: 1, NYB: 1, BLY: 1, HAT: 1, TEU: 1, WAG: 1, RPF: 1, PFU: 1, UPE: 1, WYW: 1, BYY: 1, YYF: 1, EOE: 1, OER: 1, ERP: 1, GFU: 1, UPK: 1, PKE: 1, UBB: 1, BBE: 1, EAU: 1, AUW: 1, WHA: 1, BYL: 1, YLX: 1, XXB: 1, KER: 1, HEG: 1, GEX: 1, HLN: 1

2. Melakukan trial dan error dalam bentuk iterasi

Iterasi	Analisis
Iterasi-1	Berdasarkan huruf yang paling sering muncul pada letter frequency (E), bigram frequency (HZ), dan trigram frequency (HZE), dapat dilakukan pemetaan sebagai berikut. H -> t Z -> h E -> e
Iterasi-2	thYt dipetakan menjadi th*t, kemungkinan Y -> a
Iterasi-3	Atate dan theAe dipetakan menjadi state dan these, kemungkinan A -> s
Iterasi-4	aFC dapat dipetakan menjadi and, kemungkinan F -> n C -> d
Iterasi-5	Jumlah LF dan L cukup besar diduga L -> i
Iterasi-6	XRntent dipetakan menjadi content dan jumlah R cukup besar, kemungkinan X -> c R -> o
Iterasi-7	TitheachotheB dipetakan menjadi witheachother, kemungkinan T -> w B -> r

Iterasi-8	VrodUces dipetakan menjadi produces, kemungkinan V -> p U -> u
Iterasi-9	crMpto dipetakan menjadi crypto, kemungkinan M -> y
Iterasi-10	GundaPentaW dipetakan menjadi fundamental, kemungkinan G -> f P -> m W -> l
Iterasi-11	cryptoloOy dipetakan menjadi cryptology, kemungkinan O -> g
Iterasi-12	Kranches dipetakan menjadi branches, kemungkinan K -> b
Iterasi-13	eDistence dipetakan menjadi existence, kemungkinan D -> x
Iterasi-14	oNer dipetakan menjadi over, kemungkinan N -> v
Iterasi-15	techniQue and subJect dipetakan menjadi technique dan subject, kemungkinan Q -> q J -> j
Iterasi-16	cryptanalyS dan codebrealing dipetakan menjadi cryptanalyst dan codebreaking, kemungkinan S -> t l -> k

Plainteks

Hasil dekripsi sebelum diedit	Hasil dekripsi setelah diedit
cryptologyisthestudyofsecretcodesinspeaking ofcryptologywediscusstwomainbranchescrypt ographyisconcernedwiththewritingofmessage sinsecretcodeandthecreationofthesemethods whilecryptanalysisisconcernedwithreadingenc ryptedmessagesbybreakingsecretcodesancie nttimessawmanyexamplesofcryptographyover threethousandyearsagoegyptianscribesmade useofhieroglyphictransformationstoobscureth emeaningofwrittenmessagesmesopotamiana	Cryptology is the study of secret codes. In speaking of cryptology, we discuss two main branches: cryptography is concerned with the writing of messages in secret code and the creation of these methods, while cryptanalysis is concerned with reading encrypted messages by breaking secret codes. Ancient times saw many examples of

ndbabylonianscribesemployedsimilartechniquestorendercuneiformtabletsunreadabletotheuninitiatedthegreeksemployedcryptographyandthecloselyrelatedsteganographywhichisconcernedwithconcealingtheexistenceofcommunicationratherthancontentformilitaryandtacticalpurposeseventhekamasutraofancientindiatouchesoncryptographylistingsecretwritingasoneofthesixtyfourfundamentalartshundredsofotherexamplesoccurinancientcivilitationsinshortcryptographyhasappearedmoreorlessspontaneouslyineveryculturewhichliteracyhasbecomewidespreadcryptanalysisontheotherhandtookconsiderablylongertodevelopasarigoroussubjectofstudytheearliestsurvivingdescriptionsofsystematicmethodsofcodebreakingcomefromfifteenthcenturyinthearabicencyclopediasubhalashaitgivesthefirstknownwrittendescriptionofthetechniqueoffrequencyanalysiswherethefrequenciesoflettersandlettergroupingsofalanguageareusedtounravelsecretcodescryptologyhasplayedaroleinpoliticalandmilitarymattersfrommedievaltimesthroughthecenturyperhapsmostfamousisthecryptologiceffortofgreatbritainandtheunitedstatesduringworldwariitheeffortsofthirtythousandemployeesatbritainsbletchleyparkincryptanalytinggermanysenigmatransmissionsissaidtohaveshortenedthewarbyseveralyearsanditledtothedevelopmentofthefirstdigitalcomputercolossussimilareffortsintheunitedstatestobreakjapanesecodesaidedamericanintelligenceinthewarconvincingamericanauthoritiesoftheimportanceofcryptologicexpertiseandeventuallyleadingtotheestablishmentofthenationalsecurityagencyinwiththeriseofdigitalcomputernetworksinthesecuringcommunicationbecameanincreasinglyimportanttaskintheprivatesectoraswellthenedsofthebankingindustryinparticularforsecuredigitalcommunicationbecameespeciallyurgentdevelopmentsatibmledtothedesignofluciferoneofthefirstpublicciphersforcomputercommunicationsthenationalsecurityagencyofferedseveralimprovementstoluciferandinthenationalbureauofstandardspresentedthemodifiedversionasthedataencryptionstandardordesthusthefirstpublicstandardforencryptionbegantogainwidespreaduseamethodofsecuringcommunicationiscalledacryptosystemthesenderencryptsorencipherasamessageusinganencryptionalgorithmtogetherwithasecretkeythisproducesaciphertextwhi

cryptography. Over three thousand years ago, Egyptian scribes made use of hieroglyphic transformations to obscure the mean- ing of written messages. Mesopotamian and Babylonian scribes employed similar techniques to render cuneiform tablets unreadable to the uninitiated. The Greeks employed cryptography (and the closely related steganography, which is concerned with concealing the existence of communication rather than content) for military and tactical purposes. Even the K¯ama-su¯tra of ancient India touches on cryptography, listing secret writing as one of the sixty-four fundamental arts. Hundreds of other examples occur in ancient civilizations; in short, cryptography has appeared more or less spontaneously in every culture in which literacy has become widespread [45].

Cryptanalysis, on the other hand, took considerably longer to develop as a rigorous subject of study. The earliest surviving descriptions of systematic methods of code-breaking come from fifteenth century, in the Arabic encyclopedia S. ubh. al-a ‘sha [45]. It gives the first known written description of the technique of frequency analysis, where the frequencies of letters and letter groupings of a language are used to unravel secret codes.

Cryptology has played a role in political and military matters from medieval times through the 20th century. Perhaps most famous is the cryptologic effort of Great Britain and the United States during World War II. The efforts of thirty thousand employees at Britain’s Bletchley Park in cryptanalyzing Germany’s Enigma trans- missions is said to have shortened the war by several years [45], and it led to the development of the first digital computer, Colossus. Similar efforts in the United States to break Japanese codes aided American intelligence in the war, convincing American authorities of the importance of cryptologic expertise and eventually lead- ing to the establishment of the National Security Agency in 1952.

chissenttotherecipienttherecipientwhoalsopossesesakeyreceivestheciphertextanddecryptsordeciphersusingthekeytorecovertheoriginalmessagecalledtheplaintextinthehistoryofcryptologyuptoallcryptosystemsrequiredthesenderandthereceivertoagreebeforehandonthesamekeyakeythathadtoberigorouslyprotectedfromexposuretoanadversarythisisknownassymmetricorsecretkeycryptographyarrangingtoshareasecretkeybetweentwopartiesisoftenadifficultproblemanddoesnotscalewelltoscenariosinwhichmanyindividualsorcomputersmightcommunicatewitheachotherinmartinhellmanaprofessoratstanforduniversityandwhitfielddiffieagraduatestudentintroducedtheconceptofasymmetricorpublickeycryptographyintheirseminalpapernewdirectionsincryptographytheyspeculatedthatametthodofencryptionmightexistinwheretheencryptionkeydifferedfromthedecryptionkeyinsuchaschemeausersencryptionkeycouldbeannouncedtothepublicanyoutsidercouldobtainthispublicencryptionkeyanduseittosendencryptedmessagestotheusersinceonlytheuserwouldpossesthedecryptionkeyonlyshecouldobtainthedecryptionofthemessagepublickeycryptographyalsoopeneddoorsformanyotherapplicationssuchasdigitalsignaturesandelectroniccashtheconceptofpublickeycryptographycirculatedintheresearchcommunityforsometimebeforethefirstpracticalproposalforsuchaschemewasmadeinaugustthersapublickeycryptosystemnamedafterinventorsronrivestadishamirandlenadlemanwasintroducedinmartingardnerscolumnonmathematicalgamesinscientificamericanthersacryptosystemoutlinedinsectionhassurvivedovertwentyyearsofstudybycryptanalystsinthepublicsectoranditisthemostwidelyusedpublickeycryptosystemintheworlditisusedamongotherplacesinthesetprotocolforsecurecreditcardtransactionsandthesslprotocolforsecurecommunicationontheinternetpublicdiscussionandresearchincryptographyinbusinessandacademiastartedinthelastquarterofthe20thcenturyandcontinuesatafuriousratenewmethodsforencryptionarepubliclyannouncedresearchersthenstudythesemethodsforweaknessesbyapplyingthetoolsofcryptanalysis2onlyafterintensepublicscrutinydoesanewcryptosystemgainasenseoflegitimacystudyingandusingmethodsforbreakingcryptosystemsisanessentialstepinthedevelopmentofnewdesignsformor

With the rise of digital computer networks in the 1970s, securing communication became an increasingly important task in the private sector as well. The needs of the banking industry, in particular, for secure digital communication became especially urgent. Developments at IBM led to the design of Lucifer, one of the first public ciphers for computer communications. The National Security Agency offered several improvements to Lucifer, and in 1975 the National Bureau of Standards presented the modified version as the Data Encryption Standard, or D.E.S. Thus the first public standard for encryption began to gain widespread use.

A method of securing communication is called a cryptosystem. The sender en- crypts (or enciphers) a message using an encryption algorithm together with a secret key. This produces a ciphertext which is sent to the recipient. The recipient, who also possesses a key, receives the ciphertext and decrypts (or deciphers) using the key to recover the original message, called the plaintext.

In the history of cryptology up to 1975, all cryptosystems required the sender and the receiver to agree beforehand on the same key, a key that had to be rigorously protected from exposure to an adversary. This is known as symmetric or secret key cryptography. Arranging to share a secret key between two parties is often a difficult problem, and does not scale well to scenarios in which many individuals or computers might communicate with each other.

In 1976, Martin Hellman, a professor at Stanford University, and Whitfield Diffie, a graduate student, introduced the concept of asymmetric or public key cryptography in their seminal paper New Directions in Cryptography. They speculated that a method of encryption might exist in where the encryption key differed from the decryption key. In such a scheme, a user’s encryption key could be announced to the public; any outsider could obtain this public encryption

esecurecryptosystemsbylearninghowthingsbreakwelearnhowtomakethemstrongeritisinthisspiritthatthisthesisiswrittenthisworkusesmathematicaltoolstostudythersapublickeycryptosystemandseveralvariantsweusetoolsfromnumericalalgebraandthegeometryofnumberstogetourresultsalgebraiccryptanalysishasproventobeoneofthemosteffectivemethodsinthestudyofpublickeycryptosystems	key and use it to send encrypted messages to the user. Since only the user would posses the decryption key, only she could obtain the decryption of the message. Public key cryptography also opened doors for many other applications, such as digital signatures and electronic cash. The concept of public key cryptography circulated in the research community for some time before the first practical proposal for such a scheme was made.1 In Au- gust 1977 the RSA public key cryptosystem, named after inventors Ron Rivest, Adi Shamir, and Len Adleman, was introduced in Martin Gardner's column on Math- ematical Games in Scientific American [32]. The RSA cryptosystem, outlined in Section 3.1, has survived over twenty years of study by cryptanalysts in the public sector, and it is the most widely used public key cryptosystem in the world. It is used, among other places, in the SET protocol [84] for secure credit card transactions and the SSL protocol [30] for secure communication on the Internet. Public discussion and research in cryptography in business and academia started in the last quarter of the 20th century, and continues at a furious rate. New methods for encryption are publicly announced; researchers then study these methods for weaknesses by applying the tools of cryptanalysis.2 Only after intense public scrutiny does a new cryptosystem gain a sense of legitimacy. Studying and using methods for breaking cryptosystems is an essential step in the development of new designs for more secure cryptosystems. By learning how things break, we learn how to make them stronger. It is in this spirit that this thesis is written. This work uses mathematical tools to study the RSA public key cryptosystem and several variants. We use tools from numerical algebra and the geometry of numbers to get our results. Algebraic crypt- analysis has proven to be one of the most effective methods in the study of public key cryptosystems.

	https://theory.stanford.edu/~gdurf/durfee-thesis-phd.pdf

Metode Kasiski

Cipherteks

VOIVVCBAJMBLGUKWAOMDABTAPPZSECQFQWAOPKSBRCQMVOGKUIEQXDWFZSGN
ELRHHBGIZSAZJLHIGMPOGZBTKHPUBFMDFARTVLWHNLTUKVRJFLXSPRVUKQUKJVS
URCKTGCYZGIEBQEVSLVFUPQYZLYVMZSPZCYIDYYBAXZNTFPRPNXLGFUNZVOEHG
SUQLVRXGDEGBXTKGBRLCJYZGILQXOPANAIWGFIZLSPNPPWQUOEQLSAYEOEDNXL
AFZLUPLQOWYZZSARRAKIOSNMQDWAMFLVKRQMZOOGKTISIJDPQWGGGDSMGUW
MZLCSZJPWSAQQZWSEOPNWQUYWXOOFZQMYZSSTXLVRTGLHGBPBQUVAOEHPDR
BAAFBRRQYIBTSVQWFFJWLXCGRMAMHOXGHOCSDPQXWEYVDSFYNEMJHUKHPVG
GKKMVSZOEFIOEYNFZPNTFBRUJKAGFWDAGIIQNEAQLVOGPKYBTYVXQUBZUAYRRX
BESBQZYVSTGRMYSFROPKSBRCQMFARGPDLWYOBTWFRCGYIDEYNQKGBXUHXHU
OJQYWATKUKCSPWGJMRGTZPOGOZAFHJKNCIGGELQFHFMTHHINDMPXFBSVOFOA
NCZYHUHCUHIAQEMKOOOLGSBQOZQKQUUQSAVVMPXSHRXEOEBTOLULGFZCAYGN
CIELOGKQDRSQMIYHIFUPQYZLDPQLVNTPPZSECIDQCSZJIEBQEVSKHHJGUXGTBIPM
OGKFHWSAQQZWSEYCUHCSDPQEOEKKUHCAOAUSBGNCAQCZOVFAGEKOHVYRNIE
LVRLKYWHGSUQABQUPLWWNXMZYWAKGYWVNFMSJOQACAIRSBWYLVOGPKYBTYC
DXCHTFPRUSKBTWFVXUVIYNBVAOOFUPLSTGRMSJOQACAIGYKBQJVRHGJEARDPQ
XWEYVWVSFSLQFHBLVOIFRZCNDWPUHPRRBXMEAOQATPRUGRMVSDNTGZICPMCB
SHVUPPRHUMPMFURJKAWBNWMFGPNTFBRUXYOKGRNOIHOIOULMFROKEHQSOKV
PMBTZGJLBVMIXUCYRGNIGRUWXSVGOPNKWGOSZAYOGPKYBTKNFWFVTFVRSFSIE
ABQKRLRRRXKQXIEZJLVABBMUFGGZDHRRHXOTSRZUXLHHBIWSQOXGTAEOFCBFT
OAJWUKWATWSBOJNKJLZNDMDTSPGOLKOQTITEOQGWUMJRBAULMHMOVRXHXME
LHOGPKYBTMPMFURJKAWBNWMUFHBAPPZSECQFWWGBCUMBQYVQKWRAPKIFGR
MOGBGXQSSTASKMOWGNHHGIYDMULJNTVLGVASAOZSJKVLRGPRIBSBQLCJYZGOQ
FNOAKZHGHRGMFWBFIJHTKUSKTOSEKGZXOOVQEZSQRCAIFNPBQJOYUPNWHBBG
UFIAOXLVGVDMULJNTKUHCAOAUWXBOPLHIASDQJGVZAVJWANWZWGVGCZJOPETF
QCSKPNMBROZUFUNTFMEQHVBKGTAGVBVOYCKUWBPKULRQBEZMYSQHAPHSNCIZ
VPRRKLJGOKAQVCAOPKSBRCQMFGFZTBKUYOBAYSGOPKIDRXLQFQRGPKSIELZUY
VGLWAYFRDPQABQUPLWWNXOANSETOLRHVXIGYIEGVLHHUOMELOORKZLARXBAXP
NTFBRUVXAFAHHZGVJHRMPZGZBMAVRANBKTABPUPAVOFDBALVRLKCIDEODUGIFK
PNMBROZUFUFIJVSZBXBTWGNSGJEACEAUFGGOVBXHRUVADCTODHRRHXOISGOUT
UMBNXIFECFVJLVSSETXGTQEPHQWPCKMJFLOPNXVRWQEKWBTQMHSIYBUGBGUUJ
MSAMMMFRGKEORCYYOKSBQHWPPRVXOMVSIKNVTSQQMZWFNZKVRTBBBTWTHZ
WYIRHBQZYHUKHPVGGNMOSRRUHALSVDJNWUNTVVJCFDMDMDNTFKIJRVWBAHFK
NMAWGRBTWGGGVBXSFNCDABTZJPWDRBQAVDEKRHVOGSWZKKRXGTERRBMSSF
QOPNXVROLGUOGOQUEZNXLFWOPNKUKCEQIZANNZKVRGJRQXWOYYQMYZSSTXA
BTZJLRIZLMDGTGKCJLWAQAFSTSGPKMBPBMMKWAMVOIWECSUDZOECZWWTXQZY
HUKOASGGELKSPEUCKHIESVSLVRYGJSBQNMOSRRUHALSVDJISGZAFKPSQGQFZRV

LHPGIYDGFZOGGTVWSGYEMJRFZJLJWECBBWFVUFALSNMIPWAVIWUMHGRIFZOQH
GLRTBBUQVKNYVYEBFPWDESQOPASOJYZWMBVZVOEHNVAAUCAIWYVSADTKXIAIVP
SBFKAMKCPOQLGCAYUUUIAOVALOGSAXAAVZGKXCOOQZYOFKOPEIGYVAECHYKUW
HVDCFACAZJLPSIOTAXOPGFLQWPCEMKWAITLEGVXONMHGNGHWGVQVYWBGZQZX
IQIINJCNJYHWRRMZQSGVTIPRHRBVMDTNIKSMHVOAMFRFZCAYHRCEQJSVTEYIOFS
VSDMHZKSMNRNLGJWAMVOIHUSZPVSPGFLSTGRMULPFOOWVCIOUQFHVYOHVYRN
JKLVRSQCIARXBAXHUKUAEHHDMESBQZGHGVVXOXWOETKUKDEYKQKGGUYHVRFK
UAVSETGYEHUKBISGRWWPTDRNEULVZUTLGOZZCEXOPONPXWRCBTWBHSDLVCSQ
ZMVINZGZMBPBMMKSQGPKTCFDODSRHGVLTFBQZMEGUGFHPGBLMSMBGUUAEFG
DPUKGVZWHXWBXEMKGHVRVVHRNJKLVROOWVCIOUQFHBLVOIQBEVFJMFYQJMCC
YTULWPGNHRRRMWZGAVIIYSKGRLGJWAMVOITBEZFZRRICKICSDPQLVRKPNMBROZ
UFUHTKCIFFSBKLVNZRYMCEVGAFZLNCKSBRNMBSFGSGUXBBGWRXSEYVDIBGIAUP
PNIJLPCEZZAYFNSFLTOEDUQFHFOPJPIQSVSLVRJGWEFGWMZLCSYQJMCGOKTFCY
UIFEZBXOIAHUZJPVHLPWGJANYVLVDEYODSAFGPKXVEOMPGQGUTHPGGELUWGGN
GZIDEYODSAFOPJPIQOBTWSYKOLRHFYNEUWRTELXSPRVADCTECYXPHCQZWGFGP
KLIZKVULWRYVOMGQOKMVSYKFPXPGYIZWKPKPAYFLDPMLWFSCYOSQLGFZSRSGY
KSAMMAXPRZVLVQBXKQHHFGPKMRRKARGFVZUKIJRVWBESAZRYSQRCAEGARUHA
LSZSVODIQKVOEHGRMDSDVJIYSKGRWRABSUTTEHVYVRDCJOPALSAOEOWBGATFA
WYVLQEOAJCUIRHMIFACAZJHXWFKKOWZRXCAIRGSUQDMVTVLKFNDMPKIFZCPRO
OVMMFRGNGIIGGSVHWGGSGUXSSPWDLFRRCAIRGYBTAGVZDPWKVVTUFUGUDBMZ
QSBETOPNGSSFCBWSJOZUPHWCYSLRGIAJCAMCAYNNSGVIUJMSAMMBJCSOEPIBPI
AALVNZKAWUEKLGSHRYYPPZOOINDSGUCKEDGDWDSDVJGUZWEYVYWBGGNJLOA
QMEESNTYOMZRDPQHCFZIYERHKBQHFBMTHQWFDPQHWBTGLVHBOVTSBPOPNUIN
VQFQOAJSBEBGSBKWTSOEPIBPIIZVSSLGJXWIOVQKGNYYLPZNCQFKFRRGCEBPOB
AOOEJUALSAOMPKGBZJHXWGLAOGBGXKIYHVYVFGHUKPHXWBXIXVSIKNVTARXBIA
ZYHGNVSNDMDSBQSQYIARKVUFUSANALOGDPQHFBLKJMSAMGMFRQKXLPCCWMZL
CSYEPIBPOIZVHRIJUSZBQGYMGGHGJEFESMPGIGOPAEQGKVPABGKIYEHRNIEABGN
GYSZRYNDWGRGTJLOANLQNSYURTIBGEVUNSEYKACWGLAPWJRRQWQSADQZKQV
KPJIOANBQUVAUNVKMVCJMKSQUPALSCEZBGGRZQISCFDBTWBNZKVRGQODQDCC
SGUXDYKVFZSEKHVVSVDJIAZYJGCIZBZQFKSYLKUVSFOIDUVNTFTEBHPIOLIEKEVQA
HXQOSHVUPHRRVXNAJANZKVRHRMPZGZBMASEBQCMMSBQGGYSGCKKQLFNTUWS
FGKBUGBRTXPVCAWMZLOAJDPSHRMPZGZBMAHRROSWEUWRTELWHUKBFZSZOUZ
MCAYNOGAZAPPXMFOZHAQROULBDRMBQVHBHGHFZRDWNMWYJDBWWAOAEABFO
IOXGVXBAABQKRLRRRXKQOVVIJPWHUOQZAHVGNJEDVDIXXCEZJLQOVXBQFOAIGV
JVVQPQJSQAEHXWBXIGLCAUOFFIFSVQKGVTUPKVGPWDABQKRLRRRXKQAGQOTLG
HRNBAJSNIJHGHVYVMTZRGEOMSIOUQFHNTFALSQEBKGTRJWJEHVYVMFRNICKIAV
MIEZWTNCZTCFCQNDSGNCAXVRNMHWZBVOLRHBPQFTKVRNIIPNCMPGBGNGZXFR
XOFZGBLVOIWACBULIGOQUMBGRMRGFZUHVTHVWCYMGRUHPRTBBUMLWBTVOIAN
SVFWBNTELSTPYUBWHRTVAIOPRQZYGGGHMAWGRPUYVDACSMHLCSUDZFGPKLW
TRLQNCGOQUMBGOODSHRJGKYQNDQAFGLYVLQOANKXGGRIQSPOOYZMLWBTYPX
VTYDQJBZKPAMBQEAFJMEKULEFPRQZKHVZWAMCACIEOSYRCZHCZOAFAQNTFVZS
ECMMKSQAEHXWBXQZKHVZWAMCACBTWRRBGSSDZOVFAGRDRLGHRNBATSZUPPX
CEOLMFRZKCZYFRNAAAHVYKUPWAOEULVGNGALFROXUDZNXUVJVVQPQJSQAEHX
WBXLQNSYURTIBGYNTMANTTLWCHBKQKTNIKSMHVOAELOAJCYHOANEAJYCXQJIRH
BMESGJKNSEGGRMQUCAUOPGGBMQAUIYZWYEZNXLESTRZAKIJRVWBESAZVOEHG
RMIAZYOPNRSFCBAVSIKNVTWGLQEJSSRGJXSQLGFZSRDEPXSZOVFSBQSKUHGRD
WRSZYOVIWHNUMTGZQKTZAVBKKWFCJRGKKSGRMZSHHXGVJGPSMZLWSOEMEQG
DPMLHUKUJMSADQRAQEKCSMHLMIZTSEKCJLSQLGATGRXXHXWBXNADZBCGKFMY
YOUUOYYVBHMGRIFLVRJKZGCIOZKGTFIKLRHVPQOLFHZJPWHUOZUYVGUHLZSEIPG
EOAHGPRUFCWFZOGYEPIBPOIZVHRIJUSZBQGOSBOKWZIRGYQYHFBBGOYANXEQD

```
TNXGPRHUOEAJZQKUWIQVKTXQWAOPKSBRCQMABGNGMMTGRLQUOQKQMXVRSV
ELWGAVAIYAYTAYWOGPKYBTCTQYOYYVHXIFGIEKSGZQIIGGKBQGKAKFBRWIOZEAH
LGEJSFQSVSLCGNGNSJRBVYWBGXGNYZNDQAFBBUHVRRRMMYTSEYVHXSBGVQVI
AOXLVGVDQQKKRXGZSARDPUFUHTKXYSNXLZWKOEVOIBGRQETSTGPDMHUDPQAG
FACUGSBPOANSETOLRHEOOGDOGOQURCBPWZLVRKUAEPYSATESAZQMWHNDMAO
BRJWUMJRBAULWRYCZPSTKTNGRLLQSPCJOLNQHUKKZWINXKQGTTUXLVBZOVFJST
ANHXWBXVAGTBTVOISFDINDWFNOLRHBPQZKHVZWAXSXXWXGUVHCUHIAQIEKHNZ
GVABRNCZAJRXUPXMGRCEOWGNVOIWFCCMFQRUHALSYKBFWFEKIBPOGSWZAHO
NCZPSTKTXQPRIQTIOYOOMDPBJAALWFWMMFGVZDOERGRMDAUUZVVGOEBGAMH
YKIHPOPDQAFGNYNVRUNCNADZBCKUKJNVQPJSTANHXWBXAIAHUZJLMGFEIZUSBLI
VZSEXUQFHEKIBPOGSWZFCBLTPZOYBGNWHJKGUYBVFMDKWGOGZAVVMPISGQXK
CIBOIOXGPNRKGEHVYVNWQNSGALSSSZELQBTUPHSEKBUGBFUVVFCBCBOGACKVP
XWIOVQKGVTFVRSFSIZWSQYWUMJRBAULWRYVOEHPKVOJSNZGKIABMZMLWPOPKI
DRXLQFHPOVPDSACBTSHPGPJSACOBQYZBHCSPMVXWDVSEZQHGVVODQLVNZWU
MJRBAULWRYKUGZHNQZYWGHPLIRGYJQABQKRLRRRXBMMHBTQTSIFKVPLVHYJHZ
WAQJUYURXTLWDBXAUTWYOVPIGBXRGDMVZDJIZRLZMLSFOVZ100XVLOIDSBAOXLV
GNBGZGKVZDOEGTBIPMOGKFHPIZXQIZCUGXLWWTXQRAQNTVYSZRCQZVSIKNVTW
AQBTWQBAPAVMVDJZGKUGUMEQHVBUWGFIJVSZFCBGVMCXQNVOZCZQKSNXEOKF
BEXEUSAZGYWFRCMMJQUIGUXSECIZVQRTVLVGBPMJUSYRGUGSPEZDWBGRAPXP
UKAYGFRZJHRHUYCESBQGEAMJRCBGVSAZUHGOQOUUUGGGHMWOANXDGTRYUV
VGVDJZGKUGUAACZKQZUOZVWZKOAOAMUOZVWZEBQTIFABNTIVVQNWXGKWGHJH
WOYCWNWQBSGALSYOIPABTTCAMCAKTGFWIKTZMHLKVPSZRGFLVWADPQVSIKNVT
ARXBAXFRYGHVQUDMOZBBRQNCOANIDLGVTKUHCAOAUS
```

Langkah-langkah

1. Mencari semua kriptogram yang berulang di dalam cipherteks

   Contoh:

   ```
   WUMJRBAULWRY -> [96, 444, 540]
   VQP: [528, 1009, 1537]
   ```

2. Hitung jarak antara kriptogram yang berulang

   ```
   WUMJRBAULWRY -> [444 - 96, 540 - 96, 540 - 444] -> [348, 444, 96]
   VQP: [1009 - 528, 1537 - 528, 1537 - 1009] -> [481, 1009, 528]
   ```

3. Hitung semua faktor (pembagi) dari jarak tersebut

   ```
   348 -> [1, 2, 3, 4, 6, 12, 29, 58, 87, 116, 174, 348]
   444 -> [1, 2, 3, 4, 6, 12, 37, 74, 111, 148, 222, 444]
   96 -> [1, 2, 3, 4, 6, 8, 12, 16, 24, 32, 48, 96]
   481 -> [1, 13, 37, 481]
   1009 -> [1, 1009]
   528 -> [1, 2, 3, 4, 6, 8, 11, 12, 16, 22, 24, 33, 44, 48, 66, 88, 132, 176, 264, 528]
   ```

4. Menentukan irisan dari himpunan faktor pembagi tersebut. Nilai yang muncul di dalam irisan menyatakan angka yang muncul pada semua faktor pembagi dari jarak-jarak tersebut. Nilai tersebut mungkin adalah panjang kunci.

Dilakukan irisan pada himpunan faktor pembagi dari 348, 444, 96, 481, 1009, dan 528. Didapat irisan dari himpunan faktor pembagi tersebut adalah 1. Hal ini dikarenakan jumlah faktor pembagi yang sangat banyak. Artinya, nilai irisan yang diambil adalah nilai yang paling banyak muncul dalam semua faktor pembagi. Dari seluruh himpunan faktor pembagi yang ada, kemungkinan panjang kunci adalah 12.

5. Kelompokkan cipher setiap kelipatan key, dimulai dari huruf cipherteks pertama, kedua, dan seterusnya, kemudian dipecahkan dengan metode analisis frekuensi

Group	Cipher	Huruf paling sering muncul
1	VGPPUEJKVFJGPCFVGCNPEPAFTDJPQGEQWGVHEF GPUYPPGUKTNTVCLQECQPPJGFCKCOKPGCPFUPC GVVHTGPKFIEGGPPFRJDXTWKOWOPKPCPQHVVCZJ GCPXKPACPFVUAKPTPPWPOVKFGAPKPJGVDTJPPQ UEWNKWHHVFNVJRGPQKKQJCPVCOCGHFHTJFWGV PVWVQVGOKJFTGQYIKCEKVFOOQUGKYGWTNDGPV FUWROVQNIVCPKRCGVJFPGQIJVPTGPOECPVFPCG VPURHVITPTCJCVCGGCDDGPCUEKYCGNYITGPSEG YGUJKPNGQNKXEJGPIGTRKQPNPQKGHGKFEPKAGU XDAEUPUGDIRJNJGEOURTJEFWCCCONGVQHHVEVH CPQGVQYPUWCFEWGRPCKGUERTKCQNOWAVPNGE KVTGGEUCCXGVKKJHGEJWGGUPGQVPVQFEGGHVX GKVPCOQUQWCQKXNVOWCGUVHICQADVINKNJIITG GKKGUVVFWVGPVPCQWKPRQJTVDVBKOCQSQKGM SSQQSBFBSGTKOOBWQBWZSFBG	G
2	OUPKILLHLLVIQYPODJAPOLKLISPNMLHYLHDPFBIKAV KDYHUZCHOUGSOADQPIUHUUAHYLYAKPVLAJWOPP ZPABHHJNNKVLLHLAUJLUVKAPUKSHLLJHHZANLULV ZNMBLPLKBKKALLLZBVVACNVJBHULHNMJOPVVYPAV KMBPHTNUUVMLJKOZAKJAKPVLAULYAOYPLAKPULLL HZHPSAYSOLWHCAHUHYPLPLZKLHAHVWOJHYOKNC YKUDLLJWJFPLKHZJLLYKOPAYYLKKYAOYTAFUHALPI UAPBSHAJPAPKUJOYHLNBPJLCAHIHVNYAJLPUJAYYJ TAWJVAIVUVCUTVHVSYWPPHLZPLHBOLPJLVHFPLLH OAJKZALIZOUVPOLAMSKUKLSPALAZVHASLPZUAVHT LSYJSPYKONVJPUIZKVMJSJHKBZLPLPPUZOPWKMM AKHIBJNNVHLZXODULUAMUZSZLHOLAUVPOABZTAO VHVUHLVBPUZCGAPVPVUOKKPJSHUULLTHLPJZAVG UNIBUFCNAURYGRQAGRUZZNGBTIRIRBV	L

3	IKZSERHPWXSEYIREEYIWEQIVSMWWYHPIXOSVIRIY YSSLIXKPIHFHSAEYRYZEXWHHQVWWWIYRISIEVIRRI RWROQLIKYRRVRHEKLKMRYWZMISGGRYGTXIWVHH JJMEVRHJSKISYWRHLRJRVIMSEXRMVQXHMRPTRIVL JIAXWVEXEKRYRLMIWSHSLPGWJLMRESEVSGLXEW PQEWXWRMYIMISVVIEGKVETGXVMTTPEXVVIMRSIIM IMSXIPTPEMEVVXPIPRXXLMXYOKVMISLESELAIXIKRI XIWMSWMMIWPEZLMEQVUEIXPELXYXTVILMPISEEES LICQIKLSRXVIVEQRRESSVSRWMXBFWXRWEQJXFKR GGMLEITXRIXIMTRISIAMLMYQPXMEMHZXMSGXYPLJ XIWMHIEGEIERTXXHWAKJEMMLXFHGRWZRISIYRISM XIYXIRSSYRXVSYIMGRREWMPPWVXIRXHAXILPPILE GPRKXMZPZYAIELHFXRMEIIDSPGMGIRSZWII1OZKGT KAGIXXZITRRZGZGYGVVTHSTKGKYRT	I
4	VWSBQHIUHSUBZDPHGZWQDOOKIGSQZGDBCCFGO UQBRTBWDHCOGIOIBVBGSZSBGSCCCYHWVRBUYT GASFRUCHBUISBGWBSRARHOWZOJXBBSBFTIVGZH KOFHGCIWOBQOQSGBUDIFWHHAUHAODBZAHRBSW VSSCRSTRGSCJWSDORVZCGZIWBWWGIBSSISWSHT BOHSBCOCIHSWGGIRHHHONHTCYAHVDRHDOWCBC FGFWHCQCRKTCBFCBBBCOIFCZHDVGDIHSPIGPFSS QRJQSHKHSWRWRFOGSRKZFCCSBUZDWOZRWHIBB WZBSWHWASAOSCBZFQHZOBWSOMSCGDSZSBARH BGFCHRHCMDZWGRHDOVWIVRHHSSHACVHPFWBH TATOWHWBQOOVBFCCSWCDHCFWFVWBCHORGGZJ HSWSSGHVSGQSHSWMMCHHSUBZRAHQBTVYBIGW FJZRSGASBHSHCPHJSCIBWSHSIBMWSOSOWROOUJ WGSOOBVBHSSCWSJHADSAMVJZRRIWDGZ0XDFXV NPUJQEGGVGAJEUHUUWWIJGCTFNGQK	S
5	VAERXHGBNPRQLYNGBGGUNWSRJUAUSBRTGSYGE JNTRGRYEUSGGNAAQVTNQLEQTASAZRGNNSTSNGY RFRBGPUNXOOVRGTFRBHBFANQRHTNEQGAYAPGR UONBVAAAPRHYBNORYRERNVURVRNFERBCRHNSP RIAYVQBHGVFRGFRGRRNEJSZAPETGEQVQYGENGB FJNAFAGOGVIPVVQRRVRFRUGIRRHVEFURZRSPFBB GBRIBCRGBSRFERBGEEQGGBLEEGEQFPHZQGLQAB RRRZGGVAYHFGNOGSGVQCYAAPEOGEARHFBNGPI NPAGVBRNRGACPBEGRRAGGAAVCFQYVBFHHVRQC GAROUAFRRAVRUVVVBFGRRVIQVVFRBNRAGVBNPP GLTGNAOTQPAZEBAZRERARVBGHVAHGBNRGFGQZR NBGPGALQBYGIVUEFPBGNUVRGRATFGIQRNRBVRN GUBEBYNRTJNZBFBXARGFYGTYFGEPNNBFEGYVVO VSEBIFRPBRACVVRHGRFABBR0LOHLYVAMVNOYULU PHAHMVAZZVHAAZLVHNU	R
6	COCCDBMFLRCEYYXSXIFOXYNQDWQYSPBSRDNKY KEYXRCOYOPOEDNQOMOCMDCEBQDOONSXFBYKB RKDSZXRMMWYUKMUOKSXBXICTDTBXMWCYRSDSR	O

	OGSVPBDOSNEOVCECKCOXLDXXOXXMBDOOXEUXX ECWYMYXQBBNDDVRNBSBOXQRSLQBCXESNDGDY CMRBPYVDKYSOYDOCXQIMBOCSNSRONXDXYKKNZ CQBDQLDXNOEYMREDOSVNGIZDSWOXPYOEYOYRC KOYDLMXKVCSRRYOVMKSDVSPYVSBSYMIKODYQDK DOVSIOCOOLYXXDKDMWOQSKNYNELDNCEDOKDZO PXXMCKKWMSKYOMDOXXODXQXSPXNYOEYMCNPC XCRWBSYRRCRODNYYERCOCXCONONOOQXYBONB RMXVRCLLODUKRSDDMLXYROPOICOQYXOKCRSYC GKOSBDMGDDXRDPOPSDBKOXOXDPXQNRCKSKOW RBDCVXEXSBFMIYSKCOSBKMXCOXOBNYXKQXXLXV EPWSTVESVKWXVGXRMGWVAKEVWLMMVTVCH	
7	BMQQWGPMTVKVVBLUTLIELZMMPMQWTBAVMPEKN AAVBMQBNJWZLMCEZPLIIPIVIQPAVIUMMWCBVMBPL CMMCPMOLVIWSNIKMOWBWMIAMPMQVMKMAIQMKQ BGMADWTZBKZIAQBLZPOIMBAPKBDZBAVOITKQBMO OMBQMJMWBCQWMLLIQTMAMSQLVMJQGEBIIUWZAT AUAQVCTEOVIZVAEVLZMUJBMOKUBECBZMOZMPEJ UVTWLZPZBGMWAZUVMKOWOMLOBNVQVKIPGMKA WAVMWVELIKUMMVWBTBWLNMALIWVMPBPVQBIVQ BMAVIBMVPGMIGMVINLVAQBJZBDVJQIIQNPMKBMPW BNZBWABKQIBPIVWKBVUBVIQMQMOBMCUVUQPSLO QKZDAQIAMQBVBLAEXPLNKAEMMQLWMBQGVWMKM MPQIGNOIZQZPWIGQEETQLVTTIBZVVQMVQPLQPOO WAMATLKVVIQWICCCBWTOMMGQNQAIUWGMPOVZB BVIAVZLBBWDAQJBVJARZVGGIWZWMQZOFFSGSPHJ OOGCOBQOSCHWAQOC	M
8	ADFMFIODUUTSMAGQKQZQAZQZQZZXXQAQAQMMF GQXEYMTQQGAQPZMQXUEYQDSPZQUFEQZSYDTAS QQQNEVBMFKMPXXZFEQUTSFSDTUEMUFQOMUOBF FTEQUUUQZFUKUMZQMAQUQAGEAFZTAUUTUAIFXM EUMKMZTZONDBTDAZSGFZXXDFMUZKSOIFFMBPFQ DWAKMUXZAFAMNYNQMMQSGPUQKAEXQAIUETMM DMSUMKQFUZGFQUKABRUAQSZTIGDPUDTEAZUMZ MFAQRBEODRROQFOQPMHDTUESRNBAGNDYEQQQ TFKZQFAPOFXIDUQMZZYPPEDQUPZQMBTQFIFDOOA ZMQUZZEFOHQNEAQZXQQGQDQAMQKMENHFPFUR YMFBZUUQDAXMQFZEFMZTFAMAUUQQTQEAEQAEBI AEFFRTWZZMRZAAUFKOUGFZOYQAXMQEAQEQESY AYQQUZEQAGZTAUNNQFANZXEZEMFZXMMDAAAPIZ QZNDIXNEUOQZUOMQTQDQUZQMPUUGMLNTZTRAV HFZBREBPUURQAVZAQNYYALARUAA	Q
9	JAQVZZGFKKGLZXFLGXLLFSDOWLWOLUFWMXJVZFL QSSFWKYJFFXYKKSLLHLQKMWESALAYJLXWOJJXFD ASSFGGFMUSAWAXFSQTBTELLFFWKGOLZSNWOZJF LWJWQFGWYVVFYFYANYLXAGALGFWFDSEGJKGFSV WWYSWMAWAVKSUWAWAGSKDYSLSSZZJWWZVEMU	L

	XKUAYEAXKMWJSDFJDJVLFLXSWKVSLXWVKSEMKK LFJLGJZLFLFSXPYFLLFAJSGWSWUDWLVWLZXHGEG DSADWEAWDKFWLAFTJGSJLSDSWEHHHSQWVKKOK GGVASFHFLVMGAAWNNWKUKGWDZAKULSJGSLGLG UZGAVMAAOAXFJLKAAJTFGFZDWTGZLGMLWWYYDN SFGLJJKOAKKWATFALDJNMKLJSUUSEAVJZSSGFSLL ATTDULGLYEZVSHDJQAULYYKGALWFTVKFWTANDLE OLGQGJGDKGKAOFWAQDFAMFDJAUFFWKSGWLGGK WLJLFSYVLLYAMLYTDLOBBXXCQDVCCECCPEKYCON DKOTWCOKKDXDNO	
10	MBWOSSZAVQCVSZUVBOSSZAWOGCSOVVBFHWHS PWVUBFAFGWMHHFHOQHGOIVCHOSOBGVBWOVCF OOVWHWODHUPRRBCVYFBIGROOOSOMHUHWWBW JSBOBSSOIJXGGCUTBSPCGSQVBSIOPHZBVIUGGCG CTFWBRBSFTHRUDHGBDKFOONOBTTWZHPVRGROR FAOKSBCICIAOCCOWHBCGTRSMWSPHVHBOGSGVO BISRGBGGVHMWAWRVUVZFSPFHVCCHAAQGASWCG WSKWSPHFSAIDBCBOCZMIRGFGUOOIGCVHSDBSCF WBOTSGFOGBHSZBUFRCHGIBBGSSJQVSGBCSZSVI HAZBFBOZWSAQHWBBVHCOSCGBGSZHTRWSZKBGI FGWBHGVZCHGGWBMHSQSHRGSRHVZSSATOYGCIT SZSSSBZZCHWHQSGZOVTFVOOHBFTZWBOWWOSK HCBBSIKUKSGSOVSBWRHTSTWHUHJWQFHPPGUHG ZSHSHCHWGPQQBAGSWSWHHZSVWWBHVUWMSIGI QQQBJBBZXMIMZACBUXJQAIXWITVPBMIA	S
11	BTAGGABRRUYFPNNRRPPALRAGGSEFRARFOEUZND OBQRRRBARJFBUOURFGFNSHGEEGERQAQOHVFQR EBPQNVRNNOTYGOVQEGZXAJPQHORBGRGGNJQAF EQYANBVVSNAPQRAFGRGQEEONHBPRFFNGTOFQL BGGQINHURNNFGTERQGPNYTGSAOUERRZVGFVVQ NQVAAPAVFHAPAGGNVNFVHAPFVRUQEGERZPHNQH UGVHRBFPVARRHNLGENNFRSYUNFGGFYRTFRYPFR RFVARQVSJGAARVFGGRVGPZAVSNRGVGNFBBPASS NREBGUIYQSBQSRGGGGRYERVAQRNCEYYNEVNBQ NRABRZZRBYFQVVEAQAVQQNRNRNTGBVGBGZRBN RGDFGRLRBZEVYNQVRRZZVGNQYNNACJAYRAYISR QYQJHSUEERBYRFHGAGROBNQAGQGOYGALGGBEA RHOTFEGRARRLUTTBFVVNRGREORBVUYNBTUBEBJ GQNNBFCVQRNPPPBENRGQBHRYVFDZPIRZTZUGQE MZJDYEGUDZZMFGNPGPQAODU	R
12	LAOKNZTTJKZUZTZXLANYURMKGZOZTORJXYKOTAG ZZOGCXTGKMSHOUXZKUTZJKYKNKLUKAGTXUAHYL UATUJTOKZROGTKZZUGJNGGMGJABAXNTKLKIKRUO TOZGKTGKHROZOGLUTGRTZMULKISOOUVEOTUKHK ZZKUTTKGZKXOONZYZKGMEKUYUALGZUIHYOZIIOO ZKYZGINZJTIZTZMGOYSKZTUTWUOSZGGGUZVOLYGI MIKTZNSYISOJYUZYGUNOKTEGYKKSSZGZZUKJUOAJ	Z

	ZXTZNSRZUNUJIOZYUJGTZMTOJOLYRJZXKKHSALKYI HOKNGUYRKUUZZSKJLTKUZMGTTJMTOAOHJOKIGZI AUTKOIGTJINNVRNLOUUTTTGAGOJYITKKZRTAZBDU KYNXAUTIJXKUZZZOKRDSOKRXOKKKXCYJIZUHYIKB XKONKAGYZKGNXUYOXTEGATOKZJYLKUATNZHZXN UKNIJZZKYCAZLKLKOXRSTUKTYYZOOGHZZYHKTYX OZOSGMZAVWGWVKUJVUWGSVUGGUUAKWAFSVXZ LS	

6. Mencari huruf kunci dengan menerka dan menguji coba

Group	Huruf plainteks	Huruf cipherteks	Huruf kunci	Keterangan
1	E	G	C	Apabila G merupakan e, maka huruf ke-1 dari teks cipher: V -> t
2	E	L	H	Apabila L merupakan e, maka huruf ke-2 dari teks cipher: O -> h
3	E	I	E	Apabila I merupakan e, maka huruf ke-3 dari teks cipher: I -> e
4	E	S	O	Apabila S merupakan e, maka huruf ke-4 dari teks cipher: V -> h
5	E	R	N	Apabila R merupakan e, maka huruf ke-5 dari teks cipher: V -> i
6	E	O	K	Apabila O merupakan e, maka huruf ke-6 dari teks cipher: C -> s
7	E	M	I	Apabila M merupakan e, maka huruf ke-7 dari teks cipher: B -> t
8	E	Q	M	Apabila Q merupakan e, maka huruf ke-8 dari teks cipher: A -> o
9	T	L	S	Karena sudah terbentuk thehisto, maka huruf ke-9 dari teks cipher: J -> r

				dengan kunci S
10	E	S	O	Karena sudah terbentuk thehistor, maka huruf ke-10 dari teks cipher: M -> y dengan kunci O
11	E	R	N	Apabila R merupakan e, maka huruf ke-11 dari teks cipher: B -> o
12	E	Z	G	Karena sudah terbentuk thehistoryo, maka huruf ke-12 dari teks cipher: L -> f dengan kunci G

Didapatkan key = CHEONKIMSONG

Plainteks

Hasil dekripsi sebelum diedit	Hasil dekripsi setelah diedit
THEHISTORYOFENGINEERINGUNIVERSITYININDONESIADATESBACKTOTHETHCENTURYWHENTHEDUTCHCOLONIALGOVERNMENTESTABLISHEDDETECHNISCHEHOOGESCHOOLTEBANDUNGTHSONJULYONAHECTAREPLOTOFLANDINBANDUNGATTHATTIMETHEREWASONLYONEFACULTYDEFACULTEITVANTECHNISCHEWETENSCHAPANDONLYONEMAJORNAMELYDEAFDEELINGDERWEGENWATERBOUWTHEESTABLISHMENTOFTHISENGINEERINGSCHOOLWASTOFULFILLTHENEEDSOFTECHNICALPERSONNELORENGINEERSDUETOTHEOUTBREAKOFTHEFIRSTWORLDWARTHEFIRSTACADEMICYEAROFTHBANDUNGWASUNIQUEBECAUSETHBANDUNGONLYGOTSTUDENTSANDTWOOFTHEMAREINDONESIANMEANWHILETHEREWEREPROFESSORSATTHEBEGINNINGOFFOURYEARSLATERONTWELVESTUDENTSGRADUATEDFROMTHBANDUNGTHBANDUNGWASABIJZONDERESCHOOLWHICHLATERCHANGEDITSSTATUSASASTATEOWNEDCAMPUSONJULYTHETHANNIVERSARYOFTHBANDUNGSTUDENTSGRADUATEDASENGINEERSAN	The history of engineering university in Indonesia dates back to the 20th century, when the Dutch colonial government established De Technische Hoogeschool te Bandung (THS) on July 3, 1920, on a 30-hectare plot of land in Bandung. At that time, there was only one faculty, de Faculteit van Technische Wetenschap and only one major, namely de afdeeling der We gen Waterbouw. The establishment of this engineering school was to fulfill the needs of technical personnel or engineers due to the outbreak of the First World War. The first academic year of TH Bandung, 1920-1921, was unique because TH Bandung only got 28 students, and two of them are Indonesian. Meanwhile, there were 12 professors at the beginning of 1922. Four years later, on July 4, 1924, twelve students graduated from TH Bandung. TH Bandung was a Bijzondere School, which later changed its status as a state-owned campus. On July 3, 1926, the 6th Anniversary of TH

DOFTHEMAREINDONESIANTHATMOMENT ISREMARKEDASTHEFIRSTTIMEINDONESI ANENGINEERSHAVEGRADUATEDFROMT HBANDUNGOURFOUNDINGFATHERIRSOE KARNOWASONEOFTHEGRADUATESLATE RHEBECAMETHEFIRSTPRESIDENTOFTHE REPUBLICOFINDONESIADURINGTHEJAPA NESEOCCUPATIONINTHCHANGEDITSNA METOBANDUNGKOGYODAIGAKUBKDAND BECAMEBANDUNGTECHNICALCOLLEGES EKOLAHTINGGITEKNIKBANDUNGAFTERI NDONESIASINDEPENDENCEFURTHERMO REINSTTBANDUNGHADMOVEDTOYOGYA KARTAASSTTBANDUNGINJOGJAWHICHLA TERBECAMEGADJAHMADAUNIVERSITYU GMONJUNESTTBANDUNGCHANGEDITSN AMEINTOUNIVERSITEITVANINDONESIEU NDERTHECONTROLOFNICAWITHFACULT EITVANTECHNISCHEWETENSCHAPANDF ACULTEITVANEXACTEWETENSCHAPWHI CHWEREESTABLISHEDLATERAFTERALO NGSTORYINUNIVERSITEITVANINDONESIE JOINEDUNIVERSITYOFINDONESIAASFAC ULTYOFENGINEERINGANDFACULTYOFNA TURALSCIENCESENCOURAGEDBYIDEAS ANDBELIEFSBASEDONINDONESIANSSTR UGGLETOGETINDEPENDENCEANDOURB RIGHTFUTURETHEINDONESIANGOVERN MENTINAUGURATEDTHEESTABLISHMENT OFBANDUNGINSTITUTEOFTECHNOLOGY ONMARCHINCONTRASTTOTHEFIVEPREVI OUSENGINEERINGSCHOOLONTHESAME CAMPUSINSTITUTTEKNOLOGIBANDUNG WASBORNINANATMOSPHEREFULLOFDY NAMICSCARRYINGTHEMISSIONOFDEVOT IONTOSCIENCEANDTECHNOLOGYANDBU ILDINGADEVELOPEDGENERATIONFORTH EFUTUREDURINGTHEFIRSTDECADEOFT HEITBBEGANTOFOSTERUPANDDEVELOPI TSELFWITHTHESTATUTESDURINGTHISPE RIODPREPARATIONSWEREMADEREGAR DINGTHEEDUCATIONALANDTEACHINGOR GANIZATIONSWHILEALSOFULFILLINGTHE NUMBEROFTEACHINGSTAFFANDINCREA SINGTHEIRSKILLBYASSIGNINGTHEMTOS TUDYABROADDURINGTHESECONDDECA DEOFTHEITBWASMUDDLEDWITHDIFFICU LTYTHATAROSETOWARDSTHEFIRSTPERI ODTHEACADEMICUNITTHATHADBEENFO RMEDWASTRANSFORMEDINTOAWORKU	Bandung students graduated as engineers and 4 of them are Indonesian. That moment is remarked as the first time Indonesian engineers have graduated from TH Bandung. Our Founding Father, Ir. Soekarno, was one of the graduates. Later, he became the First President of the Republic of Indonesia. During the Japanese occupation in 1944-1945, TH changed its name to Bandung Kogyo Daigaku (BKD) and became Bandung Technical College (Sekolah Tinggi Teknik Bandung) after Indonesia's independence. Furthermore, in 1946, STT Bandung had moved to Yogyakarta as "STT Bandung in Jogja", which later became Gadjah Mada University (UGM). On June 21, 1964, STT Bandung changed its name into Universiteit Van Indonesie under the control of NICA with Faculteit van Technische Wetenschap, and Faculteit van Exacte Wetenschap which were established later. After a long story, in 1950-1959, Universiteit Van Indonesie joined University of Indonesia as Faculty of Engineering and Faculty of Natural Sciences. Encouraged by ideas and beliefs based on Indonesian's struggle to get independence and our bright future, the Indonesian Government inaugurated the establishment of Bandung Institute of Technology on March 2,1959. In contrast to the five previous engineering school on the same campus, Institut Teknologi Bandung was born in an atmosphere full of dynamics, carrying the mission of devotion to science and technology, and building a developed generation for the future. During the first decade of the 1960s, ITB began to foster up and develop itself with the statutes. During this period, preparations were made regarding the educational and teaching organizations, while also fulfilling the number of teaching staff and increasing their skill by assigning them to study abroad. During the second decade of the 1970s, ITB

NITTHATALSOCONCURRENTLYFUNCTION
SASASOCIOECONOMICUNITTHATISLIMIT
EDTOBEINGASEMIAUTONOMOUSINSTITU
TIONTHELEVELOFACADEMICSWASINCRE
ASINGBUTTHEASSIGNMENTTOSTUDYAB
ROADWASDECREASINGINTERNALFACILI
TIESANDSTATUTESWEREINCREASINGLY
UTILIZEDDURINGTHETHIRDDECADEOFT
HEITBSIMPROVEMENTISMARKEDBYTHE
MOVEMENTOFTHESTATUTESANDTEACHI
NGLEARNINGPROCESSTOWARDSAMODE
RNERATHATWASEQUIPPEDWITHMORECA
MPUSFACILITIESTHENUMBEROFGRADUA
TESINCREASEDANDPOSTGRADUATEPRO
GRAMSHADALSOBEGUNTOSTARTTHISSI
TUATIONWASSUPPORTEDBYTHEIMPROV
EMENTOFTHECOUNTRYSSOCIOPOLITICA
LANDECONOMICGROWTHDURINGTHEFO
URTHDECADEOFTHETHEENGINEERINGU
NIVERSITYTHATPRIORLYONLYHADONED
EPARTMENTNOWOFFERSTWENTYSIXBA
CHELORPROGRAMDEPARTMENTSINCLU
DINGTHEDEPARTMENTOFSOCIOTECHNO
LOGYALONGWITHTHIRTYFOURMASTERP
ROGRAMSANDTHREEDOCTORALSTUDIE
STHESEPROGRAMSINCLUDETHEELEME
NTSOFSCIENCETECHNOLOGYARTBUSIN
ESSANDHUMANITIESTHISDECADELEDITB
TOANEWCENTURYTHATISMARKEDBYTHE
EMERGENCEOFBETTERCONCEPTSANDI
DEASFORITSDEVELOPMENTPROCESSSO
MEOFTHEMINCLUDETHATTHERAPIDGRO
WTHOFINFORMATIONFLOWINTHENEWCE
NTURYWILLDEMANDANEDUCATIONTHATI
SACCELERATEDTIMELYINTEGRATEDSUS
TAINABLEANDTHEBESTINVESTMENTEFF
ORTRELATEDTOTHISITBISWILLINGTOBUI
LDITSBACHELORPROGRAMONASOLIDFO
UNDATIONOFBASICSCIENCEPROFICIENC
YSOTHATITSGRADUATESWILLBEABLETO
ADAPTTORAPIDENVIRONMENTALCHANG
ESMEANWHILETHEPOSTGRADUATEPRO
GRAMISTHEPIONEERTOENHANCINGQUA
LITYANDQUANTITYEFFICIENCYANDEFFE
CTIVENESSASWELLASITSRELEVANCETO
WARDSTHENEEDSSOTHATITBSCONTRIB
UTIONTOTHENATIONALDEVELOPMENTWI
LLBEGREATERANDMOREMEANINGFULTH
ATTHEPROFICIENCYANDDEVELOPMENT
OFSCIENCEANDTECHNOLOGYMUSTBEC

was muddled with difficulty that arose towards the first period. The academic unit that had been formed was transformed into a work unit that also concurrently functions as a socio-economic unit that is limited to being a semi-autonomous institution. The level of academics was increasing, but the assignment to study abroad was decreasing. Internal facilities and statutes were increasingly utilized.

During the third decade of the 1980s, ITB's improvement is marked by the movement of the statutes and teaching-learning process towards a modern era that was equipped with more campus facilities. The number of graduates increased, and postgraduate programs had also begun to start. This situation was supported by the improvement of the country's socio-political and economic growth.

During the fourth decade of the 1990s, the engineering university that priorly only had one department, now offers twenty-six Bachelor Program Departments, including the Department of Socio-technology, along with thirty-four Master Programs, and three Doctoral Studies. These programs include the elements of science, technology, art, business, and humanities.

This decade led ITB to a new century that is marked by the emergence of better concepts and ideas for its development process. Some of them include:

- That the rapid growth of information flow in the new century will demand an education that is accelerated, timely, integrated, sustainable, and the best investment effort. Related to this, ITB is willing to build its Bachelor Program on a solid foundation of basic science proficiency so that its graduates will be able to adapt to rapid environmental changes. Meanwhile, the Postgraduate Program is the pioneer to enhancing quality and quantity, efficiency, and effectiveness, as well as its relevance

ARRIEDOUTINTACTANDINTEGRATEDASIN THEROLEOFRESEARCHANDDEVELOPME NTUNIVERSITYITBSDEVELOPMENTINSCI ENCEANDTECHNOLOGYISBASEDONTHE PURPOSETOBOOSTTHENATIONSDEVELO PMENTPLANTHEREFOREITBWILLDEVELO PITSELFINRESEARCHANDMANUFACTUR ECOMMUNICATIONANDINFORMATIONTEC HNOLOGYLANDSEAANDAEROSPACETRA NSPORTATIONENVIRONMENTANDBIOTEC HNOLOGYANDBIOSCIENCESTHATTHEMIS SIONOFCOMMUNITYSERVICEISEXPECTE DTOBEABLETOBUILDBUSINESSINSIGHTS INTOINDEPENDENCEWHICHISTHEINITIAL CAPITALFORTHEMAINTENANCEOFHIGHE REDUCATIONAUTONOMYBUSINESSINSIG HTFORINDEPENDENCEISDIRECTEDTORE ACHACTIONABLEACHIEVEMENTANDTHE DUTYOFEDUCATIONANDACADEMICASHI GHASPOSSIBLETHATTHEDEVELOPMENT OFITBWILLBEBASEDONTHESTRENGTHS OFTHEINSTITUTIONINTHEFORMOFOPTIM UMUSEOFINFORMATIONTHEMAINTENAN CEOFCOMPETENTTEACHINGSTAFFWITH HIGHQUALITYSKILLSANDHIGHDEVOTIONI NTEGRATEDEDUCATIONSYSTEMANDCLO SECOLLABORATIONWITHGOVERNMENTI NDUSTRYRESEARCHINSTITUTIONSASWE LLASDOMESTICANDOVERSEASEDUCATI ONINSTITUTIONSTHEDEVELOPMENTISEX PECTEDTOBEMONITOREDANDMEASURE DSOITISINLINEWITHTHETHREEPILLARSO FHIGHEREDUCATIONDEVELOPMENTOFH UMANRESOURCESFACILITIESSTANDARD ANDWORKPROCEDURESASWELLASTHE ECONOMICSOCIOCULTURALANDSAFETY DEVELOPMENTTHATTHEWILLINGNESSTO DEVELOPITBISREFLECTEDBYTHEEXCITE MENTANDMINDSETOFALLITBSTAKEHOLD ERSWHOACKNOWLEDGETHENATUREOF SCIENTIFICFACTTHATTHESCIENTIFICREA LITYCANBEREACHEDBYOBSERVATIONFO LLOWEDBYLOGICALSTUDYTHATTHEDISC OVERYOFSCIENTIFICTRUTHISTHERIGHT OFEVERYHUMANBEINGSSOTHATSCIENC EANDTECHNOLOGYCANBEUSEDTOIMPR OVEHUMANWELFAREINTHEWORLDESPE CIALLYININDONESIAINTHEFIFTHDECADE OFTHEINSTITUTTEKNOLOGIBANDUNGSL EGALSTATUSWASSETTOBESTATEOWNED

towards the needs, so that ITB's contribution to the national development will be greater and more meaningful.

- That the proficiency and development of science and technology must be carried out intact and integrated, as in the role of Research and Development University. ITB's development in science and technology is based on the purpose to boost the nation's development plan. Therefore, ITB will develop itself in research and manufacture, communication and information technology, land-sea and aerospace transportation, environment, and biotechnology and biosciences.
- That the mission of community service is expected to be able to build business insights into independence, which is the initial capital for the maintenance of higher education autonomy. Business insight for independence is directed to reach actionable achievement and the duty of education and academic as high as possible.
- That the development of ITB will be based on the strengths of the institution in the form of optimum use of information, the maintenance of competent teaching staff with high quality skills and high devotion, integrated education system, and close collaboration with government, industry, research institutions, as well as domestic and overseas education institutions. The development is expected to be monitored and measured so it is in line with the Three Pillars of Higher Education, development of human resources, facilities, standard and work procedures, as well as the economic, socio-cultural and safety development.
- That the willingness to develop ITB is reflected by the excitement and mindset of all ITB stakeholders who

UNIVERSITYACCORDINGTOTHEGOVERN MENTREGULATIONNOOFONDECEMBERS TATEOWNEDUNIVERSITIESWERESOMET HINGUNIQUEANDNEWBYTHENTHISBEGA NWITHTHEISSUANCEOFGOVERNMENTR EGULATIONNOOFONTHEESTABLISHMEN TOFSTATEOWNEDUNIVERSITIESASLEGA LBODYFOLLOWEDBYTHEISSUANCEOFG OVERNMENTREGULATIONNOOFONTHEE STABLISHMENTOFINSTITUTTEKNOLOGIB ANDUNGASSTATEOWNEDUNIVERSITYTH USWITHTHEISSUANCEOFTHELATTERRE GULATIONITBHASLEGALLYBECOMEALEG ALBODYTHISMEANSITBHADTHERIGHTTO CARRYOUTLEGALACTIONSASLONGASFO LLOWINGVALIDREGULATIONSWITHTHEIS SUANCEOFGOVERNMENTREGULATIONN OOFRIVALRYBETWEENUNIVERSITIESWHI CHWASDRIVENBYGLOBALIZATIONBECAM ETHEFIRSTCONSIDERATIONSOTOBOOST COMPETITIVENESSINDONESIANEEDSUNI VERSITIESTHATCANCREATEDEMOCRATI CINDEPENDENTCITIZENSTHATCANCOMP ETEGLOBALLYINORDERTOACHIEVETHAT UNIVERSITIESINCLUDINGITBNEEDTOBEI NDEPENDENTAUTONOMOUSANDTHUSHA VINGBIGGERRESPONSIBILITIESONJULYIT BCELEBRATESITSTHYEARANNIVERSARY NOWITBHASGRADUATEDALUMNIWHOHA VESIGNIFICANTROLESINDEVELOPINGTH ECOUNTRYITBNOWHASFACULTIESSCHO OLSSTUDYPROGRAMSRESEARCHGROU PSCENTERSRESEARCHCENTERSANDCE NTERSOFEXCELLENCECURRENTLYITBH ASMORETHANTHOUSANDACTIVESTUDE NTSACADEMICSTAFFSANDPROFESSORS ITBNOWHASTWOMAINCAMPUSGANESAC AMPUSANDJATINANGORCAMPUSITBHAS ALSOBECOMETHELEADINGNATIONALUNI VERSITYANDALEADERINTHEDEVELOPME NTOFRESEARCHTECHNOLOGYANDARTSI NINDONESIA	acknowledge the nature of scientific fact; that the scientific reality can be reached by observation, followed by logical study. That the discovery of scientific truth is the right of every human beings, so that science and technology can be used to improve human welfare in the world, especially in Indonesia. In the fifth decade of the 2000s, Institut Teknologi Bandung's legal status was set to be State-Owned University according to the Government Regulation No. 155 of 2000 on December 26, 2000. State-Owned Universities were something unique and new by then. This began with the issuance of Government Regulation No. 61 of 1999 on the Establishment of State-Owned Universities as Legal Body, followed by the issuance of Government Regulation No. 155 of 2000 on the Establishment of Institut Teknologi Bandung as State-Owned University. Thus, with the issuance of the latter regulation, ITB has legally become a legal body. This means ITB had the right to carry out legal actions as long as following valid regulations. With the issuance of Government Regulation No. 61 of 1999, rivalry between universities, which was driven by globalization, became the first consideration. So, to boost competitiveness, Indonesia needs universities that can create democratic, independent citizens that can compete globally. In order to achieve that, universities, including ITB, need to be independent, autonomous, and thus having bigger responsibilities. On July 3, 2020, ITB celebrates its 100th year anniversary. Now ITB has graduated 120.000 alumni who have significant roles in developing the country. ITB now has 12 Faculties/Schools, 128 study programs, 111 research groups, 25 centers, 7 research centers, and 7 centers of excellence. Currently ITB has more than 26 thousand active students, 1.510 academic staffs, and 195 professors. ITB now has two main

	campus; Ganesa Campus and Jatinangor Campus. ITB has also become the leading national university, and a leader in the development of research, technology, and arts in Indonesia. https://www.itb.ac.id/history

Kriptanalisis Playfair Cipher

Cipherteks

PMEXMNMVOQMVALUKXFQPNTPWPOMSSYMTECSYMTNHMHSMPOCEGPHIHETHHE
HQNHMHMLPWTDHAQWKPSEAHETWDUKZPHMQRZOEHELKHHMLHELATVAMLPFALU
KQOANMLVZLCNTQXPCTPQMQXEXZHAYXDVASHXDLDMPIRHLSYPOVXTDLIMAHEHQ
ZIVAGQMEHEPUKNZAARZOEWDFMAXMQNMKYPPAHQXHVAELGQMHVZKPPLLXYSVD
TAALOCPYFBXQXDRXAYKTSEMQKMUAAPELXHXIXZCXANLNQREXXYHEETMKHUEXQ
WTDGHAHLKIOAWELGQKETSLTMTWKATSKQNPOVATGELPMMGYPPAHQXHVAAYXEE
MFTDFMQEXKEEGEQHSHUHBZGLHELIPILATPDQFLCXFTDRHAYKTGTNQQXMTWKIPL
NOUIXRAAMMLBEPGPQKTPLELVHQSTDSHXQXDCPHMSIMKQENLBDAMVSQZXDDFHE
QEAQKAFCYPVAELOQMVALIRETGEVPTAAPDFGTAFALGNOQOEHQEXGQBEELYSPFQ
XUGBEELMHXHMXPLQXHMFCIHWQHYHMLHELOQMVALIRETMQMTWKHEQXCAELKHE
XHLCNZLHEHQTAPGETGEMAKVLHEXCEELYSKSLTHLVANLHSXHVAETAVDPTNGOKHP
OEOGQVGCPHMZAHEHQGQMEABHEQXCHELZKPOEONTHSZAUXEXUKEQLPQFOGZL
TXPOABHELMCLHLMVPMVSCLHLWHIXPMMGYPPAHQXAXGVAHMFZABHEHQETMEEV
LHLPMVTMHMTAQHHSXGFXTGEVMVOQMVALURMHHLEMQMRAQMQGBEETMTIXGXH
LVWTDLIMAELMVGXHLSHEMELSKGFGOLPMWCLAYXDLYVXEXKNHMLTPIEMYPPAHQ
GXETXGHBIXFPXAXGFTLHCFLHELOQMVALIRRAQOMQMHCECLAYWDHYTHHEQEAQK
AFCYPRXPOEOXIQZBLELFPABHLMVHSSYMTGQBEELVAMHLHHEQMYPPAHQRGEQBH
ETABHELMCLHLMVETGEVPTAAPDFLCCFZLHEHQETMETMHMTMQEMAQEAYVEAYVXK
UXHXIFDHEHMCGGOMHIXDFLPWRANLMQXCAELFPABHLMVHXHIHEHQGQMEHBEXE
CQOALQRGAQXKXZAETKTUAOEYGLHETHBELENSHEMPMMGYPPAHQFKDHOFDFHEQ
MOUAOMHZHQLMGHIPOMVLCWKVAHSAVHEHMHNIXFDHEQXSIFCZLHETDUPQOIRRK
POAVQGLHGPIODAVAHETHVASHXDLTEMRQVAHMUGIPHEQXSXFKOUGMGFDFNTETS
FMLXQXDTAUPMTVHELKGQFHVQRMKYPPAHQLYSNNQGERALMZGDHOGZLAYVPGPZ
TKPQXCAQALPWHKPGHEMPMMGYPPAHQCGXAXGMLGEXHKYLSSUHUIXRAHNMHVA
ALGEVGMHESQXCOQOALQZBEKLGXAYKAKTIGMWDFLDBLELNECLZGQMTAHSDAHTN
FUKFHLUZLHLMSIXABHEHNQXOGXHHETALFIXHLGSEHPMOQMVALURZGDHOQRLGX
WVQABOIXLMTDDHMNMVOQMVALUKBEELKTANHDEXCESYQMLCGYXAMGQOALIKGF
GOWZTNZLSQXAMACNTDLIMAOQOEHQXHMXKFETSZXDTHEXHVQPEXCEYWKFQXKA
GXDTMHTATHHEHNTAAPAUABHALHKRTDLKVHALMNMKYPPAHQIXELALBLHELEPOMA
ELCGAZBEKLGXGTSHEMXTKDQMPOLCXFQPNTPWPOMVKMZSAQHBIXDFHETDKPEQ
PKBLELVAMHLHHETHELFDAZDTCEELXUMVAVGSFDXPDPLHAYXDMLOZAUHSTGTHM
HEGQXSISEFLKPIXTDDFMNMKYPPAHQGQMEHVLTAUMAHYTHELETGMANQEHEQEEL

QAWRQMAYRALTGEPKQFCEPUGFGDISIGBEELMHXHXIHTWBWZGTAVHTEMQXCGBEE
LKGMWHMPLSMZSLHKMZSTNZLHEHMHNIXBEESLSQXXGKAHBETZVPOEOELETMTNT
QEHEQXGYXDPLZAPQVAETMTNTQETHSYKDPLHELAGSEHPMOQMVALZWAUWDQME
XGMHTMHGEABHETDTHZAVAHSQMXTKDIXPMOQMVALQKPKMTHSPOEMHETDKPEQS
HEMOFHEHMGLKEHNTHKTQMHETDTHQXAYVPYSPKSYHBIXFDHWLTGQXDHEAMGSB
EETAVIGOMSYMTECSYMTFDUPGDQXSIABHEAMGSBDTHVGPOEOBEMHEGSESVKPX
GDXVPMKYPPAHQSIMTAYPVLAXLAUABHAAMETDHEXOMZLHETDTHPOLCWLGXSQEM
IXELKMCPLHKFHSGMLCNFELHEPOKALCXFCLAYXDANDTVLTAHSDAKPMQPKNOSYAF
APELXHRAPFQXCAGCLHHETHGEZWZLDFHEANQMDAPLLCNFKMUAAPNHMHKMZSQE
POLCWLGXSQEMWZPGNQHEQXDAAPLTRAAMTHQXHELQPITAPDMWQXCASHXBXUG
ZESELKGOUMEHELAMFCLZGQXCAETABHEHMAMANQNQMLCNTTACLPLVASHXDLAQK
MHXAMAOMLDFULTFCZLMLPFALQXOTGLGRPMOQMVALZKPOEOBENTHSMLPFALHY
GOMHXAMAGQFXQFWQOTCLELVAELDALZSVUKIPHXDFUKQFOSLDFULEAMOFFPMAC
EAYRXIXPGNQVAOFQGEQNXIXAYDFELKMQPNQKEGXXUXDHMPGBEELVAANHMQXKX
ELLAEXKEGXHQAMNLAFUPXELYGNOELDBLELMANHYSOGXAVAEXGQXDUIZATDUPM
AWZHEHQNHMHHYGXMLSYXDANGZHLOEZHGCLHELMPMKYPPAHQXHMAWMISQMLC
MALHETHTKGOFALPLHEQNNHMHBEUKQFSIHTAFHFYKHETHSEWEEGLCNTPUMQVHE
TWEHNIXEXKNLTSYXDEXQNHMTAOCMHQEOTGLCHELEQMRLDWLQSFZABHEQEZAV
APYKDPMOQMVALZHETABHEGXXHVSPKXTFTIRDPAMUAHUVAQFABHEAMLMLDFUHN
HMLDTBUGIPHUKGAFALVZQXOXKPPGNQHEQXKIAMHETHFKOUCNAQABHELHSHXBX
UDVCPQMDFEXGENLNRQXZLAMATHLMPMKYPPAHQHSSYMTGQBEELKSQFXQXDVG
HSSLWRAYVPQXCNTGDGEMSYAFAPPMOQMVALIHHFHIXAXIHBZAAWAYVXTGCHCLEL
XYEMKFQXAYPGXBXUDTDFHEQEQXHELUGFKPUXELETMEHEQNGSEHETMTLPQFGQ
HEHSMQVHGKDFDTBESHHLDFKMUAAPHETHPDMWQXKAQMQGBEMALHELKFAPRXG
FPFQXOSIXAZFWPKEGGEUHGSEHHEPOKAMLPFALOGNFQXHEAMHVANLHGQCEELU
RGUBEQMEXOCTIQMPFQEPDZLELGEPGFHLXHLPKFHVSQMCPHMELEGPDVAPLHEQ
NETMETMHMMAQEEXKFALMTXEEBGSEHAZNQPMOQMVALKYKFTMHMETGEMLPWTD
HAQWKPSEUPFHWPANQNKPXQXDELQHAFALGELBZSQMUXNLMHBEMLPFALELSEMQ
MAMTSHAUPSKPHTBEHLALRLDFTDTAAPEXGMLKZLQMTXZAPDMHELXHXGXEMTWK
CGGOPDGOQFAZAFUOBDEHQSHNELWELHLKIOEHELGMHVLHKTAYPAADXIEMXHHOT
GPKXAVAELPKEGLCFZKYQSMAULTXQFWPDPHETNHGHMPGSFFPXGHLELONKPCGA
BHLXEAFATFCZLHELMLDFUAQBDUPHGPIBEUAELSLXAMAGEKSPOFPBLELNEANABLC
HETNHGHMRAANHQQMHEQNEXKSUAIHRALMIXMAKEQMQGBEDWKFHYZWZLHEHQS
EMQAYPQEQIXZHAYPACLNHMHHYGXMLSYXDANGZHLOEZHGFGLEMELKGOUMEAVA
NLTXGXDALKGAFALVZQXCAQXZAXHPGWEGXXHZWTGORIXABHEQNOTZLKTQXSIATS
KQMPOKAFQAZXEXTCAETHETDLIKAHTNLNBFKMKPGXNETABHEHQNHMHXIQZXDHEL
MCLHLMVHETHVMGSEHHETHRXETAZELHSKQAMHEAQMVDFETSWWKPMOQMVALIRL
CSFMLGNMQEGNLHSLUGFGOQMAYRELAGFGDQMXTKDTHHEHNAYVSHMHMXIXGWL
HNEXHLCEGPHIPGNQHEQXCACLELVNZLHEPOKAZTLHHLPKXUHEQMIXELCNTGGHKV
GPVAELPKEGLYSWSYQMOFLCAYPGXBXUDTMXLSMLGEHEGXMAKVLHHSQWCLLCGQ
VAYPWTQSMAZYQMAYVALALMLKEQEXKEEGTAPDVAXUXQRAQMGQTAAUXDAYRADP
QEQPNTWHELWETDETXDQMAYVPQXKELMZLHEHMTDAQMTVWTGDOKFXEEMVAPKD
HKEGXPDIPHTKTLHAYWDQXDXKLHNIXNTQXSXLZSUOMCLHLWHIXBEPIKTEXQFIPILE
FESLEHNIXPIMHHEHMHNHMLACLPGLFLDFUTDTAALOMCLHLWHLKETGEPGBDTAALK
EHSWKKGNQLCHEQXDGXUHEHNIXBETMQEPIMHAYMXLMELNBXHVGTAALKEHSWKE
LMETMHMTMQEMAQEHETNKUZASQKAHETSTNANQEETMRHQKPETPKEOHEHMHNIXF
DFPQXAZFNKPWKQXDSMVOQMVALIRELTAXHIRCGAVPOSVLHTHEXQRQEAZDFPLELM
VGXHLWYQMQGBEFTESLEHMUXELKEEGIXGXHLPHYGLHETZTZLTAAHELXINQHEGPL
MLDFUAQBDUPHGRALNPOEMZATACLETMKHMLCKGBDQEHVTHLDEMSYAFAPHETHLX
HLMWGFDFEXKNELWELALNABHETNIZEOQXSILBZSLDOTGKRYHNIXVAUAAPKFKPSYQ

MHETHELXHHOQMVASHGSEHQXLCPGNQDFAQIPLCZLXGMQHEQMGFKPPGSWWKEL
KSQFHLGEVAELAZWQPUMNEXVAQPFTQMEXGEEPGPLBLAAUHBIXLXHNMAKGEMVXL
NKPQNMKYPPAHQMHTAGXQMHETHHEQNEXXHRXLTSYXDTSUGALZVUPHGELGQMEA
VANQNTHTAUOSVLHTHNTQXSIEPGPHCFDKDQMLCHEADPKQFOGBEELKGBESHWKA
YPXTGAMFUZAQXLCHXQGAMSQALEXKEAMIGGQXEMIQLHGZRGUDTHETHSEMQSLX
AMAMVWZVAHSQMDFZTAMKPWKRQMQHSXGPWKPFDHEQXCKPOEOOFMAEVLHGOH
IMHUGZGLNKPUKYOFDNBHYKLIXCGEQTHATVATMQEPQSAOAAMAUDHUKYPMAULRA
POEONTDTALWVTHQXCAAYRALSRUETSFRUGEIHEMHELDEOSEWEIODAMNMKYPPAH
QHSPOEMHEQNQGOELTEMXHHOQMPLNPMKYPPAHQVAGFGOPKCLQMLCHEAMFPHE
LEEGNTQELYSADACNIHKGPSALHLVASHXDHMELTAPGHEPOKAHELEEGNTQEGTAFAL
GEPQSAOAHNETHLMTVHETHBIXELXHVMTHHAQMELLYSWSYQMLCAYVGHSEXGMLH
PLWLDPLEPFQXKAHNIXQSISQXQXCAAYXDRXAYKTELETMETMHMLKMLCNLNKPTNTD
LIMAELGQMEHTSFSMCPLDXUSESGXEAZDFIXELFOAFALGQBECLELKMZSHNHIPLFQV
NHMLPYPHELNYSVAHEQXKAAMHXEXGQECQGBEQSSMCPLEGXPDGOXHVAELHTWB
WZGTHEQMVSCLHLCEETEVKPXQXDZAXHMXKFXGABAZXDDFAYXSHSMQFNTAAEHNI
XPIMHZAXHVAELXINQDFAQHEEGHEAMESQNHSGYXDXIPKQFGQAVHQAMRAGFGPIG
MNMKYPPAHQUPQOHUHETDTHGQMEEVCPAQAZIPACTSLEQSIXHLMWUPGDXHVAAY
MXKPSETOTHNTETSZPOMPMKYPPAHQFKEMHMQMHVQZXDLCFOAFAEQSMAULLCDA
HEHMELALHEQSMAULQXLCHELEPOMAELXHXAVAUAEOLHHMSQEQMECLLCNQBEUG
XEWQHEQXCAKLGXXYNLPMMGYPPAHQETKEEGEXZGQEKPSEEOHIRALHPUKEQSCP
HMGQFBEQSHAFATFCZLPMMXANECGFKPVSPKFTQNRXZAAWELMKLIKAHLSHEMLKN
KQOALKYEGALHSBEEXHNFKMKRAEXEVMKYPPAHQHVQACEGLVZFDMPTAHUHYQEO
QOEHQETCNANQEFOABLCNTKEHNQEAZBECLELAUSZXDPKDPQXAZNQLCGTZVEHEL
ATVAMHFPVHDFHEANTMQEQXDXHNXIEMXUXEAFHUXZMKXHZVELMVTMHMKHELMH
ETMTMHFPVHQMHETHHEQETHUGXMKFAPETMTNTQENTETSZXDMTWKQFIPILAFHUL
CGEIHAHLKIOLKFHMXKPSEAFHULYBETHXQKAHTEMHSLEHSOEQHMTMVANQEQXGE
UHGSEHHEHMLETSTNANQELYEMMHGMPLXGKAAZXDPGBLELMAXZMKPXHUQXSGE
QMTWKGQMHVZUGXMQXDTPIWMGXANANMLVHXIMHQFTXALLCANFUIGFNYKHELDF
HRATSAMQOMQFEZKETXDQMHEAQMVALLMQXOSTHHLMWHEQEHNVMLTMQSHAFUP
NHKEQSMAULISSYENGPEVIRHLSYPOXIEMFDFKMTVHGUQSVDOIXBXUFNZAEHELNH
THELSKGUXDLCNTEXQRKPAMLKNHMVPLKFAPLCXQKAAZQSNHAFAHQMXIQGHEHNL
THEHMSEXQOGBEDWKFTXPOABHETHFZAZAVFDLCFEZHELKFAPHETHETMTNTQETG
AZXDGOOEZHGOHISZHNHMXIPXHSLSHSHTRGQEHZKPGRAYMHEXGNOQEMANLETS
TNANQERLDFQXSGBECLLAEPLHETAZXMHLEGPLHEHMIGXQSMDPGXQMQHVAHMGE
ZHELZRLEEGEGKFFMPOPKXPLKCLQXSXHTMVMLWYLSVSLDFULETSTNANQEDTALW
VTHQXCXDFXUMHXQKAHLHSHUZAMXCLQFAZEFANHBANHDLPHOVXZLZGEXSMDPG
XLTNHEBGSEHLCXQKAEVMKYPPAHQXILBPKQTXQWEGXHSVDETYSRAGFCLQXSXHT
MVTAUPMTVWSYHTQXKFAPLUQZXDWZGEUHGSEHRQVAHMUGIPMLPFALQXOTGLGR
TAUPMTVHELFUTGLTEMHXAYVSHMHXAYVSHMTXPOABHELMCLHLMVPMMGYPPAHQ
GTNQQXLCHELAZSQXKSGFDPGTSWWKQXCAFKOZSVPLHLIGHBIXFDCGGOELKETSL
HGPHIPGNQHEQXCAKLHMELOTLTMHKEGXHEPKTHEQMRPOPAQHMSLHQFGIMQHSU
KYLTSQEHELTMKWPDPUKYPXGVAHMATHLHUETMTUKILRALEEGANMLVZQMPMMGYP
PAHQUPGDQMRAGKDHGEEMEXKSIHBLHMTAAHELQWKPSEAFHUSMLHQEMQGMELG
QMEHETSLTXGVAHMFDRAAMIGGMETMSHUHYUWQFWQVAOLLPBEELEQXRPMOQMV
ALQRQPFTQMKFAPRAGFCLQXSXHTMVEXCEELMHNHMHTACLPLLOFBWQUPGDQXOS
LDFUAQBEKFBEGOHIPGMXLSMLMNMVOQMVALKHLAAUZIVAHEPOKAEVHINTZAXHXA
PGNQHEQXCAGOKFZAYKPODWKFELPHCLPMMGYPPAHQXGSFMLKEHMHLTHYWPOK
AFOMVQMAUSVPMOQMVALKHDFMQMHKNELHEHMELGEMHCELAAEHMELKELTMKHE
QEESLMCLHLWYQMTDQGQMELGQMEECHSAQXMHLEGELXIQGIXGTPITAHUIXELKGO
UCEELYSPGWEQMNTTXPOECQOALIRISQEKFFKOUMEHEAQPISFFPMAPGXIQGPMMG

YPPAHQVAUXLUKHETAVAYMXESLTSIQXLKXHMKGXBEZAETSWWKXEVAZKDPPDFBXE
NQUXUKILRGNQKLQHXAXIQGPMOQMVALKYGXELHSAVQXGYXDLKSWSYFTIWQHXGU
IZALTKSANLEQMQGBEXIIHFDHEHMFKMKDFHEAMZFQAVZIXHEHQNHBEOFVAIGMVLC
NTKNAYALPMMGYPPAHQXHXGBEELXTHEPKDPPMOQMVALZKMHVLLCHETNQMPKDP
XYEMKFEXOMANHMQMOGNFQXLCHELNPKBESIMKQEHETDTHXHXAVAUAAHELMHZA
XHXAVAHSQXCOKFFMSYMTECSYMTIXHEPOKAZAXHRXIGAZXDLPMVDPLHAYXDXHRA
AQSESGXQXDHEQXSXKGOUGEAFAHAYRATSLTWQHEQXCAGOKFZAEHELFPABHLMV
UXZAGQGQXUACCLPOABHETHHEHQNHMHMHATHLCEGLSLYSPLNHAFAEQMQGBEHE
QXRYTDPOEONTHSZAHEQMYPPAHQXSCLQXLCNTMNMVOQMVALUWLAATPAANLMUI
ZGOHZWZLPMOQMVALUHHIHXHGLHYPXQXDZATAUPMTSYWEGXSQEMAYPAIXZVDPL
PVHQXCALKIOEHNTLPMHELNLAFATPAANLMXHVAETHLMTXQBLELFPABHLMVNHMHQ
XPCTPQMHEHMHNIXFDMHIXDFLPVHELVEGKDPQELTWYQSEXMNMVOQMVALZHELFP
ABHLMVDWHNMTWKNHAFHFETHELTEMMLLZXQTHLKIOEHTXPOABHEQNEXCEELYSG
YEMELKGOUMEAVANLEKFELEXOMLHQFGIKGOUOCLHSQNAOQSUXEWQHEQXCAETE
VGSEHNTCGQXCGWEHQHXEQGEEMLZMWQMCPHMZAKGOUMEHTXBNLVZHEQNLKB
RHMKHPKXDELXHVPMKYPPAHQSQKAHETSTNANQEKMUXAZXDQXLCEXQFLTRIPAAN
LMFZABHETDTHDFHEHNTAUPZLXGMQXHXARAKFQXDXGPGSFDXPALLMQXAMXGHBI
XXGABAZXDIXVAUAATXIVATHQLZAMAQHPXGAQMQFFTQXGYXDHUDFHELNHSKGMW
HMPLSMZSLHKMZSAQECQGBEPGPQKTIXUIZSHMHYQETGHSOGKPPAESNQGQBEEL
EQBAVAMHLHFDWHELBEFKKFAPRXGFPFQMCPHMELEGQXXLVZZAXHMXLTPHQRQG
XQKAZTLNKPLHELGTEVCPQMTHTAATSEXESFMLHSQMDFHETDKPEQVHELGTHEEGN
TQEXHZVAYXDLSMLHSQMPGPIGNMQFEIHEMXGALBEHUUKQOETMTHEPOKAHEQMZI
VAFPSFMLOGZLPLHEADPKQFCEELGTAVHTUAHBZAKTQMEXGQAVHQAMXESWPKNH
MECLAYXDAUDHHEGXSEWEEGTMHMNTQEMAQEQXSMZSLHKMZSLEHNIXHTAFAHAY
XEEMMTWKPUGQQOSGXDWZHEAMUAMTPKWLGXETYSEXCNLTMKHYZGYHHMTNCL
EADFDAFDIOEHCLZOGYBEKLGXNTAHELXHRXLTSYXDUPXDPKNTXIFOMSALOTGLRH
AYKTRXLMABHEADPKQFGEEMAYKAELLAQMFZKDALCNGFCLRAGXFTQLHQAMNHMH
AUKAZTSYKAHTEMVSHSOHQXCXLEQXKETANPGFDFVSTDHTOTAMEXKEGXFDMAXHV
RHMUHDFSIEMKVGFGDQMIXHEPOKAZAETCNANQEWVGDQETHALIXABHBZGLHAYVP
EXMXESHNIXTAFZMGQPFTQMKPLTTFIPOQVNALOGMHGQMEAVANQNLCMHTAGXLHE
THELEEGZIVAHSSYMTGQXEVAMHLHHYHMANTMHMZHAYXDWPDPAYMXESLHKLGXFC
CLRXIXQFNHTODPLEHNIXFZRIPYSNSESGXDQXAYVGUPHGUPGDQXOXKPPGNQHEQ
XCXZLELGQGMANQNLCMHTAGXLEHNIXNTQXKXTHKTQMNTGTIPLELAGFGDQMOFPI
GNMQFEIHABHETDTHHYZGYHIXVAUAAPHTSYXDTHAYPNPKVEELCLELMHEMPLHEAM
HVANLHLPMVDPHMLTPGBEELXGKALCBLELGTAVANQNQMLCESIPLEQSELKTZOOHQM
EXMNZLHLMHGQRAPOEOETMTDWKFWELEEGLPQFKNETHEHNIXUPGDQXOXKPQXAY
XGXMQGLMGKDHAZAVANQNQMLCNTIXUAMTVKGSHSLHHLAUKAHLWYLNAUKDQMZA
PFQEELEOZAOFQXHELTYSEXOKAUKDQMZAHEQELTMHVAVAMHLHATPSNHBEPOHBZ
AETAUABHALMPFELOTZGDHGQHTSIQXHEQEANHAESFLAUKDHMQMQXLCGEWREQX
AVANHTPLHQSAMELOTZGDHCEELFOLCZLHMQFAZAHELDFHUAUKAAVALBLQXHEHNL
KALVAMHLHNHMHHBCLQXURQXSMZGGRQXHEQMGXHTBDHNAYKTNHMHHEANHQA
MPLHETDTHXHZVAYXDAYSQXLWQDFLAGFGDQMPOLCBLELYSXYEMKFFDNHMTFWLT
KQHQQMPMMGYPPAHQHEHQFKOUMEZTLTFTLHGPANLTWQHEQXCAETHBIXETSFML
XQXDOGNFDFHELMTSQNQEECQPFTQMKPAMAUSFMLCEELFOLCZLHMXTKDQXXGM
QAYVGUPHGEXGMLHPLNOKFBEELVAMHLHLCXHMKMXQPNTPWPOWHELMHELXIECK
FFDBEELXHAFEFANABLCHETDTHELGQMEHAGFGDTHZAFZHTBLHMESDPQEHEAMFP
DHLCZAXLBDIRANAQXDUKYLHMLMPKNLXAPGMPKCDFISTAAELHYPEQCEGPSQALTH
HELHTXWZFZAZHEEGCGEQQXVALTKEHNIXVPUAQXSIHTSHHEHMMAMTMHUPGDQXK
XDPEXHYKFIXNHHSQXSXUIHSADATXAMAMAAIVZHUHEAMETMLPLHEQNHSGYXDVAE
LGTHEEGETGEPKQFGQAVHQAMRALHGFKFIXNHHSQXSIOTGLGHEQNQSHEODFLEH

MFTTGRYIGWHIXKMHXXQBEGLAZKAZTQFRALAGFGDQMGQVAQXVZHUPYXBLUQMLK
NKQGUKYOFDXYHBIXNQRALTRGQMRQMQHSSMPLAMPGSYMTEQMTMVANQETGTHX
GAVGPAZXBLUIWUKQONTVAUXXUWUPOCNANQEXGABAZXDDFTXSYKDXHAFATAFEO
HIXIQGSMPLAMPGMPKCDFISTAATAFEOHIHYQEUKZOPOEOETMTNTQEDTALWVTHQX
SGPQVAETMTSLXAMAGEOGQTFXLTVAXIEMSLVHQAPGENKHHIELMHSMPLAMPGMPK
CDFISTAAPXQXBNLGEXDSYHUKLQHMAMTWKDFAMDTALWVTHQXSIAFHPGSEHRAAM
IGGQPSTHQABEHUUKQOHEQXCHELQKNTTXZAPDMHGTMHLOTFZLFDTMQEHEQNIO
OAAMETMTFDAZDTGMDPLHAYXDXSGUXDDFZAXHPGBEELYSEQXRRAAQHMDHKEHM
ELEGXTKDTHHEQMYPPAHQMGHSOHZSQXKSGFDPXYEMKFYALTMKZALUGKGRPLKF
APRAGFCLQXSXHTMVNHAFAHELKWQECLKGPSALHLHUVAOFQGHEHQNHMHFCQFCE
DFCLZGAMDPLHAYXDRAGFCLQXSXHTMVOGNFQXDHBEUATFLHHETHXHMGQMTAIP
GQSAOALEQETMHMETMNZOARQEMAUKZOEXZTATNQHEQNXIQGOQVNALOGMHDAB
EHUNHMTETOMMHGZPOPAZAHALHGKLATNSHHLLPMHALMTWQLTMVYGFDBHETAVIG
OMPKNLXAPGMPKCDFISTAAUSWSYHTFTZWZLHETHMXKPLTPGBEPUGPLDYPELEGV
SLDFULTMHNTQXCOKFWMGSEHGTMHALXAPGZLDFHEAMHVANLHXGFWPKEGGEUH
GSEHFDHLMTEMMHXAMAGQENIOOATDUPHEAMRXLSSUXDPYPDYPXARALHYWHNIX
ETMSXGMQXHIROAEXDTTHOQVNALOGMHELMHIXHEPOKALKSUXDELXHXSGUXDLC
HLAFAEHMPGNQHEQXCXZLELGQMEAVGPELNHBEDFLXQXLHAYXDZAFKOUCNAQLPB
EELMTWKGEIWUKYOFDNBHYGPANQNVAKLTSQMGXLSMLHSQMTHATVAHEQNIOOAA
MLPQFOGZLTXPOLZXIAFAUPISFFPMAELMHTAHUETXSDFQMQPFTQMKPAQZVHMHTQ
XHUMAQNXAPGXIQGOQVNALOGMHNHETMTPQKTLCNTHEEXOWOULPWHPOEOUKZ
OHSLNKPIXELVWLHALPDXEHYTHIXELVWLHALPDBEELKWLTGYEMPLPQSAOAAMNHL
HQSSHHEHMLPEMPLFDHEEXRKPOXIQGSMPLAMPGMPKCDFISTATOPUOEIHVALKIOA
RELGQMEABHEQXCHAYRXIXHEQNDPQELBKPRAHMNTHAQNDFXIXGXIQHMTXQWUP
ODWKFHYKLIXCGEQRQMQHSSMPLAMPGMVYPLAIHMAXMZXALMLMVDFAUDHUKYPM
AULGTBDTAAEQSWZAYMXESLTAFAHAYRIPODWKFHYDFDFMAXMLNKPLATMQEQHHS
XGETMTNTQEHVQZXDLCMLMVILMQMLPFALLCGTAFAEQSWZAYVSPKMLMWESTMPU
MQPDVHSMPLAMPGMPKCDFISTAULAUBDELCNZLOQVNALOGMHHYKFIXQFVAZGGYX
DHBGPELVWLHALPDXMMAQNQMFDABLCFDAZDTZATAAOLHXAPGKGFXIPQXSGXNHD
ANLMXIQZXDUKYOFDNBHYGUETMTEQMTMVANQEEXKWLTPGBECFLNSYKAHLEQOG
XPHIQXCSPUMQPDVHMXESAQDWKFUKYLTSQEAVIGOMPKNLXAPGMPKCDFISTAAPP
OEMQXKATANLAIVSHMTHQMETULEGSQSYXDFZHZPOMHGQXBNLMHBETMHMUKEQD
WKFRIPOMHHELDFEUKEQUKYOFDFKETAFHPGSEHPCEOQNKPHBIXWPGSEHQEQMP
LUKOLATABHLMPAMIGGNOQVNALOGMHGTEPHUPCEOQNKPHEEGFPNHMVYXUAEFT
MHMETMTDFHUNTGTIPHQPOMHLCKFLAEFCFALLCIPLHELSQAVUOKDQZAVGEWRYAT
SQEZTUORAQMPGPQKTXGBDQNEGESFPPNMHZHPUMNAMELAUDHMNQWHNLTMPO
LXPSMPLAMPGMPKCDFISTAAPLKHTRAHSFUGFGDTHOQVNALOGMHEXGMIGCEELKF
APHSQECLAYXDLCHEHMQPPOMVHETHHSLNHUQXSIPKQFKQPODWKFHYTHTMHMUK
EQXAXIQZXDTXPOHBYKELMGGXLSMLHSQMTXPOHBETLBQXTAHUVAPFMLKEQSZAM
AQNQMHETHSMPLAMPGMPKCDFISTAAEEGMHTGELCEELFPQXAVELXHVPGPHTFBUG
IPLCGQVGIPVAELMHTAMHIXDFRALEEGNTQEXHZAQXCGXEKGEOETMKXHAFATAFEO
HILPMWAQHEHMIXTGTHFDSHXIFKSEWEEGRALNGAQMOQVNALOGMHXYHEPIKTLSQ
AVKQXSXHTMHIXRAQMQGFDXYHBIXFUIGBEETHBETHLMTMHMTWKDFHNIXXIQZXDR
AHNIXFDACGUXDLCNTAUTMAQLZBEUAOQVNALOGMHLCEOELSYHBIXHVQLOQVNAL
OGMHLKNHMTWHIXKTGFGPQXSIFDHEHMRAHMNTHAQNDFEXGNGQMECLEXRXHMH
YTHHEHQMHXIQZXDRALMMHXAMAOGXQVAETHAIXEBGSEHPCEOQNKPABLZMWQM
OFQXCGKMZGRAPUUPHYHNQEABLCXUEMHELMCLHLMVHEHMQPPOSYVAETHAUAIH
EMGINQVSCLHLSHMHHSLHETABHEHQMHMQEGOQVNALOGMHFCNHKEGXELEGSMP
LAMPGMPKCDFISTAAOIXMLOEUAIHEMGINQXGGTBENTAUTMAQAZGQMEHBEXABLC
NTAUTMAQLCETTFIPOQVNALOGMHMHTGELOGZLEXOMTHHLKEHMDFHEAMLKOUMQ

SYDWKFYGFDHYAMIGKELTSZHUSMPLAMPGMPKCDFISTAAPPCZGLHMHVNALGEXAR
AHNQELCBEETAVFDHTAFAHELKWAMHIQXKALHSYQMLCGYAFAHELFPABHLMVPGWE
HSWKFZHETDPOEOBEELKGOUMEHCUAAHETHAZAHATNKUFDDFHDFDXRHYUKWYKF
FZABHEHQMHXIQZXDHETHHYQEELKGOUMEHCUAAEHSWKFPABHLMRPUMQPDVHVS
KFHMPGNQLKNWPKDHEXCEETAVHYKYAMCGEQOQVNALOGMHFDGNMQOCUOPEQZ
AVZAVAPYLNTAHLMHOMPKNLXAPGMPKCDFISTAATBLHMTAAEAMOGEQTAAHELMLPF
ALELRGUAALKETDPOEOBEGYAFATAUABHATNKUZAXGIPHTVAPOEMQXCGXLAFAHEL
HEQXSXLCVAPFAYVNZLLKXYBEELXENQPLELTSQEGQKEHSWKPIMRZSHNTDEXDFHU
OIAMXAXIQGOQVNALOGMHNHSEQWTMHMDWKFSMPLAMPGMPKCDFISTAUFOUALO
GZLTATGLEEXODHMKTQAXLEMGEWBNTGEHEHMHQAMNTEQTHAWELMVMLVZTGAL
MGQPFTQMKPADTSLTKSLTAVXQXBXLRALHGFGDISPUMQFNTHKTWPDPAYVSGKDHH
TEMANESQXQMZAZAXHXIMTWKGOKNTHKTZAETCENHTPLEEXGMFZEBDFQPNTMVQ
XVALTOEZAHALMATEQAVNHMHPDSZXDHSPOEMHEANQMDAZAPQVAETMTSEMQMAX
MLHGOQPFTQMKPLHLKIOTWTDLIMAELFOAZZTTGGYWEGXFPKDLHEXGMIGKEISSYG
MATHLGXOFFPMAZAXHRAHNLKLCEOUKIZCNLEHMTNZHELXHIWQHXAXIQGSMPLAMP
GMPKCDFISTAATEMQGDFAVOFFPMAUKYPADGUXDLCHLAFEPHNYKUKYPLEHMLDXL
AFUFATDTXGMTKGNQLCWVQXKAHSWKLCAYXIQFHTEMQFOTLHELKWLHELDFHUXLS
QHUELETPALNEBKFUKQODFEVLTWQPOGTBENQEXHELMLDFUHNLKAUMTELMHKVQ
AOMPKNLXAPGMPKCDFISTAAUQPSUXDLCELPWANLHEXOMGUBEQXSIEBQPNTPWP
OMKQPFTQMKPHQPOGTBEZSTNANQEXHZVAYXDHEQNTAEOHIUKZOPOEOBEXUEMH
BPFLDFUHNLKHSLAAMPAYGLQXIEMHEHQMTCGABHEGXPGXQXIHYQSGYKDQXKAGX
PDHEHMTAAHELXHQIVLELVAMHLHVGMHESQXOXKPRXANLHRAHSWKFPABHLVKDPLT
EMAUMTELMHZAVAELNTVAFUTGLNKPAYPVIGGNOQVNALOGMHXUMPHUAYXIQFHTE
MQFOTHNUATFLTFTLHDLFSATQXTMHMZHAYXDLCAYRNELWEAMPUMQSYMTHWZAHL
BEELSEALABHLSHALABHLSWMHMLTHQMSMPLAMPGMPKCDFISTAULIGBEHUXGABAZ
XDXTKDOGNFDFHEHNTAHPLTAFHUOQVNALOGMHUKZLAYWDUKZOEXANFUIGXEAFA
HAYXGXEALABHLVHELMAMLPFALXYAFEFTMHMQFMQMVHTEMAYRELATFLNESPOXIA
LDAEMYXPOEOBENTPIMSSYMAGQBLGOHIXHRGFDNFIXETSWWKFPABHLMKHIQXLOL
ZMHHEHMHNUATFTNGFGDRXSYABHLXEFCZLETSWWKTMHMZKAYEOQXPOWHKPEO
XYAFHOFDHYGXXENQANTGHAIRIGGNOQVNALOGMHUPGDQXCSHMIRHMUGIPHUCP
HMHELHPFPLAYRATANPGFDFOAIXMAXGHBPOEONTQEPOKALCLZMWEXZWKURALTO
NESPOVXLNKPLETDEXXHHOEXCETAOWESPOPXKPPGNQHEQXKAHNDFHLMTWMQN
QNNTVKEXHZPOMALEKFPQKTNTABHLPKXBWLLATFADPKXYXDOFHXHIWPDPTAAHET
LZBEUAELVMLTKQLCHTDHZASMPLAMPGMPKCDFISTAUPMLEQKEHMPDZLTKETXDQM
ELMPQXGMXHAFUPNHGEEMHEQEXIQGQHRIAMUKYPHMGSEHPLKGYPMAFZHEKFGX
HETNKUDAABAZXDELMHOQVNALOGMHRAANHQQMAYVGUPHGPIGNMQFEIHVALKIOA
RELHEPOKAHEQNGSEHNTAYGQXDETSWWKQFMQMWLTHEZAETKSQGVXSYXDQXKA
QSUKZLAYWDZAXYMALCHVIPHEISSYKNZAARDPLHAYXDIXQSFPVHEXHTVAAYXGFKO
UCEPYVAETKSQGXYHERQAUNLXIQGOQVNALOGMHQSFDAVHIQXKAGXELHSAZMXAZ
BEELSYKALVATDTXIQGSMPLAMPGMPKCDFISTAAOPYOCQXOAZWZLUKZOEXLVMHHL
EMELMXCLGTMHALXARAQMDLVAQECEKFETHBIXHETHTAKFPYVNAUXDPGQFKEEGW
VGDQEHEAMUAQEDTHSPOEMHEQNZAKSHNVALTGQHUUPQOHMIXHEHQUPGDQMOF
EXGNOGNFHEAMHVANLHLPMVDPAMGSFDXLELEGAUKAAZAVNHAFALCEGLPKHSIXH
EHQFCHEUPGDQMOFTHHEAMRKEXGELYDAPDLCVWYGLNLAUPZLPLHELTYSEXOEE
XMQOGBEELPKEGQXWPDFLCBLELSQBLELPDLCVWYGHNIXLYDAZAXHMXCLAYXDLC
HEQNEXXGABAZXDIXHVQGAQHEHNIXTAPDVAHBZGLTVATAATXIFDMPTASEXEEMTHA
LIXLBZSLHQSAMIXXYMQELUPGDQMXGPSHULCCFGSLCNTTAUPNHGEEMPGXYEOUP
XDHTXDALPGXWIPYKFTTGRYIGSHEMNTHSKEQGPDVAPLAYPXTGLELEEGETEMVAEL
XGQTPLOQVAXZFEQGXIEMAYPXANLHQXHEAQPHLTHEHMFCCLRXHMLAYGTNTXQKP
URLQXXGWEGXSTVAPQVGOUHSHSPVELXHRAPUGQXDTXQFOELDXWATWDLHRAISS

YGMIGGNOQVNALOGMHPGQFGQXDMHAUTMQMTHATVAEXKNELMHGQKQPODAABH
ETHPDLCVWYGTNKPPKNHGQLVPKNLXAPGMKQPFTQMKPAMYSXIQGHEADGIBEOTQ
SXZXDGTMHLOAFHUPLBLELPDLCVWYGLTRAAMFPDHUKQFSXYSZIVXATKDALBEZAN
QZSADCLAYPVYSFDSMCFALPVNHMHHEHMQEGPYSLKIPHNIXTAPDVAMQVAPKQHCN
ZLGSCLAYPDZLTAHPGSEHNTLPMHHEQNIOOAAMVAHSHLGMXHMPQXHSPOEMELNLA
FATPAANLMIXNHXHPXHUQXCPHMWVGXLCEOQPFTQMKPLTEMSMPLAMPGMPKCDFIS
TATFQELBKPXHMKCPHMHETNQFOELDXWATWDLHXGXMQGAQIPZBGXZXALXHXIXTW
ZFCUWIXHTPAANLMQFMQSHLZBLPLQAZTATKDETYSCPHMAYPXKPLELTCEELZKPOE
OMALTOZSYPOPAIRETMLOKZLAUDHTXPULCLUGSEHXQXDGXHETHHYHMHNAYVSHM
QMSMPLAMPGMPKCDFISTAHUAMXIQGOQVNALOGMHELAFAETSLHETAVGTPWKPTM
HMKGOUMEHZPOOGPGNQHEQXSIFCZLZAOQVNALOGMHTMQEUXZGPOEOYXPOEOB
EVGHSVGEXKGNQQXIPLNOUYATSLDEQRQMAULTXCPQNUHLNHCEQHNAYKTGXLSH
MNLVZSEFPBLELUPEMDFQFMQSKPKQFKNLAAOZSLEQSELMHETKSQGNHCNLHHLSK
LHHEGXCPHMXYHEOQVNALOGMHLCGDETSWWKQXAYXIMPXIEMLZMWQMLCXHMKV
AELOQMVALIRLKIPTDPOEOZGPOEOGXHICGGOWZLHKLQSXGSHRGQMETKSQGELNT
BEAYXSMHTHRAISKIELEGCPHMETSWWKEXOCTSLEQSHYTHPQVAETMTNTQETSHMI
RKVTHKTKHAYRGHMKRGXVAELXMQOMQFEKYISSYOELHPOHTLKFHAUDHHXPOEMQ
MOGSXAWAWAWAYXAMAOMPKNLXAPGMPKCDFISTAHUPOAFHFHGLHELPQSAOAAM
XAXAPGSWWKPGWBNTKEISSYCEHGQXCGZLTAHSDAVSCLHLKEEXODHMKTQAXLEM
FZWKQXKAGXXLDTQXZAFZAZGBGBGTBEVAEXGQHAUAIHXQESAMMQEGEXFPKPAU
ABHALEHSWKPLBLHMAUMTXYHEPQSAOAAMQHRIAMZAXIAFTPHMIREGFZACLHISSY
FPWQPOMVLAWLISSYOGWHLATFLNPOEMSMPLAMPGMPKCDFISTAHFAYVSHMQMSL
ABAZXDETKSQGSGXDHMHUDFHELTMPIXOQVNALOGMHVALMMLOGMTVHELUPXKHS
MQFNTAATEMXHHOQMLCHELNPKBEOGKPELATQGETSWWKDABEHUDFHEQMGFKPV
ALMLCGDTALHHLPKZLPLAYVGUPHGLZKDQMZAQXXGMQETSWWKVXATWDLHXIEMH
EQEGTNQXTKDLCHELDHEHMHBPLKPLXOUEPQXZLLHELHEMHLDBLELPVLCGOEXOE
GFGDQMTHHELAZAHATNQFOELEISSYGMRAPOEOHMXARAGFGDSMPLAMPGMPKCD
FISTATFAUWDQMLOSYPOPAIHEMHELHXYWDAUXDAUKAABHETHIPILAFHURADFLNPK
NMQPFTQMKPAMHQAMMAQNQMLCETMTCGEQPOHBLAAPIGGNOQVNALOGMHXUXE
AFHUHETHVAETHBTMQECFIPQXAMXAVAHIQXKAHMHNQNHIIXNHAFAOGLEMUGQXHE
TDLATNSHAZDFRILTARIGKEISSYGQXEMTWKPQXBLUQMPCZGAQCNAMACLHHEGXXZ
DHHXHIDXGSEHSMPLAMPGMPKCDFISTAUFPKNLXAPGMKQPFTQMKPAMYSXYSUXDA
YXAVAMHESQXDAQHPGWEGXGIKDLHPAANTMLEISSYGMFYXDAYPVLALPBECLELPDL
CVWYGLTEMGYKDQMHEANQESGEQQXLCAUNLXYHEHSGLSYHVGPAQBECLELIGSHE
MPLXUBECLELXQKAAZRATAAPANHQPOPGDFQAFSTDLVPKNLXAPGMPKCDFISTAAPIG
GNOQVNALOGMHFDGNGQXDLCELMSPKNLXAPGMPKCDFISTATFALHYHMFDMAQXMH
FUQKQPFTQMKPLHYPEQGEEMXHHOQMXTKDOGNFHEAMHVANLHDFHETDKPEQWYA
MLCSFMLGEEMLCGDPOABHEAMUAMTMSZLPOHLWYTDAUKDQMZADFDTEXCENHTP
TNTAAPPLAUKAAVMLCNTGCHCLELYSVAMHLHATPSXAPGHETHSMZSLHKMZSADUPN
HGMQOMQFEUKSHXDLTEMELKGOUMNHGLDZLTHTXWZGTAVAUWDQXSIPKQFCEELK
GMWHMTHHELDHEHMQEOGBLELVAMHLHELKGOUGQIPAVANLHELFZEMALPLFTEXDH
AVDFHEAMHLFPXFQPNTPWPOSKGFGOUOKDETSWWKELPQMPYPQMELLZMWQMDF
AYRAANLAEXKNZAETRXGXLKWLGXOTGLRYHNIXCGEQTXMHTQHMOLLUQMHEQELTH
EQMDAPGLFSYMTECSYMTHYZGEAHIXGALBEEXCEQGQIEMHMHEAQWDIRRKHETMH
MUHIXLVATDTUKYFPOEOANMLVZIXLCXQRAQXCAAYXDVAKLLSMLWEHSWKFPABHLS
WPKAFALOGMTSYXMQGLEGXFTEXDHAVXYHEPOHBHGQXOIFPEQVPTAAEEXOKUPM
AOGBEELALABHLVWAMQGLEQSEXKEAMALVLDFFDHCFDXYXDELXHXAVSTDGIEFCLD
WKFQXKAHNIXXLPDIPFDHCFDXYXDELFKOUCNHNGDQEQXLXHNLKYPVAQSTNQRMV
OQMVALIRVGMHESIXRALDMLEQCEELWPDFECGFKPLCFOLCZLHEQNUACWCLHAAMF
DVHETHEHNPOEOVSQECEELEQBANLNBNHHDVXAQXDSMGOMQGEEMSUBDELCNKY

GXKGIPQXOQOEHQELKGOUMEHCFDBHETHTABHEGXMTWKPDNQBEMLPFALNQLHQ
XSGXMTDMHHTAFUPMTVHELKGQFHVKHHMLEPUGQXDOFHEAQSKATXAMAXIEMXIQZ
XDQXLYRAQMPCZGAMLCETSWWKFPABHLVHELFCKHLKAUMTGN

Langkah-langkah

1. Mencari tabel frekuensi bigram dalam Bahasa Inggris

   HE: 300, EL: 260, QX: 186, MH: 147, HM: 144, QM: 143, AL: 132, ET: 128, VA: 122, LH: 113, XD: 113, PO: 111, LC: 109, DF: 107, AM: 106, AY: 105, IX: 105, EX: 100, TH: 97, TA: 96, BE: 96, QE: 95, EM: 94, HL: 87, MT: 83, HS: 82, PG: 82, MV: 78, AN: 76, ZA: 73, XH: 72, LT: 72, MA: 71, HQ: 70, KP: 70, AB: 69, NT: 67, RA: 67, HN: 66, GX: 65, PL: 64, GQ: 63, SY: 62, CL: 62, AF: 61, XI: 60, OQ: 59, PK: 59, OG: 57, FD: 57, ZL: 55, KF: 55, KA: 54, NH: 52, QF: 52, ML: 51, XA: 51, MQ: 50, QN: 49, YP: 49, HU: 49, XG: 49, AU: 49, TD: 47, QG: 47, HT: 47, UK: 46, PA: 46, EG: 46, GE: 46, EO: 46, LE: 46, EQ: 45, AT: 44, AZ: 44, UP: 43, IS: 43, WK: 42, AV: 42, MP: 40, KE: 39, NQ: 39, GF: 39, MK: 38, CE: 37, LK: 37, FP: 36, LA: 36, HB: 35, HY: 35, IP: 34, AQ: 34, LM: 34, TM: 34, SM: 33, ME: 33, PD: 33, KG: 33, LD: 32, QS: 32, EH: 31, SH: 31, UA: 31, GT: 31, DP: 31, VN: 31, XQ: 30, AP: 30, IG: 30, GS: 30, HI: 29, KT: 29, TN: 29, GD: 29, LN: 28, XE: 28, FT: 28, OU: 28, NL: 28, PM: 27, SE: 26, TG: 26, DH: 26, ES: 26, KD: 26, KC: 26, QP: 25, XY: 25, ZG: 25, VH: 24, GO: 24, LP: 24, GP: 23, TS: 23, VS: 23, BL: 23, GM: 23, HA: 22, PF: 22, YS: 22, CG: 22, AH: 21, IR: 21, SI: 21, MX: 21, CN: 21, DA: 21, DT: 21, ZS: 21, SW: 21, RX: 20, OE: 20, CA: 20, TX: 20, XU: 20, WE: 20, PU: 19, CP: 19, FZ: 19, FU: 19, QO: 18, MG: 18, PQ: 18, GN: 18, MW: 18, OF: 18, HV: 18, IH: 17, PI: 17, FK: 17, FC: 16, KS: 16, VG: 16, QH: 16, OT: 16, MN: 15, VZ: 15, KM: 15, IO: 15, QZ: 15, GY: 15, SQ: 15, OM: 15, HG: 15, ZH: 14, XM: 14, LS: 14, KL: 14, WZ: 14, GL: 14, LZ: 14, EC: 13, WD: 13, BD: 13, WQ: 13, SX: 13, SF: 13, QA: 13, XL: 13, XB: 13, DW: 13, OA: 13, AE: 13, KH: 12, KN: 12, VP: 12, UG: 12, WH: 12, EV: 12, VW: 12, HX: 12, ZT: 12, XT: 12, TF: 12, ZO: 11, VX: 11, LY: 11, YG: 11, NF: 11, LU: 11, AD: 11, SG: 11, PW: 10, UX: 10, GU: 10, UL: 10, MS: 9, QR: 9, PY: 9, WV: 9, ZV: 9, WL: 9, WP: 9, PX: 9, FO: 9, FE: 9, PC: 8, SK: 8, RG: 8, KY: 8, SU: 8, ZW: 8, GK: 8, UH: 8, LB: 8, HO: 8, WY: 8, QW: 7, LI: 7, LX: 7, OC: 7, AW: 7, IL: 7, ZK: 7, CF: 7, RQ: 7, FH: 7, SZ: 7, PV: 7, SL: 7, PS: 7, EF: 7, HC: 7, SA: 7, GI: 7, RI: 7, TP: 6, AR: 6, XZ: 6, KV: 6, CH: 6, KU: 6, AO: 6, SV: 6, YK: 6, EB: 6, UO: 6, NB: 6, FN: 6, EP: 6, XS: 6, XF: 5, ZI: 5, FB: 5, CX: 5, WR: 5, QL: 5, HD: 5, XP: 5, QK: 5, DX: 5, GR: 5, UI: 5, HF: 5, MR: 5, KQ: 5, RY: 5, YO: 5, AC: 5, LO: 5, KW: 5, LV: 5, GH: 4, FX: 4, UR: 4, KX: 4, EN: 4, RK: 4, RL: 4, WB: 4, VL: 4, GZ: 4, OS: 4, WM: 4, OX: 4, VM: 4, PH: 4, HZ: 4, OL: 4, IW: 4, OH: 4, VK: 4, HP: 4, VD: 3, BH: 3, VE: 3, GA: 3, CO: 3, LF: 3, YW: 3, OZ: 3, FW: 3, NP: 3, TO: 3, OI: 3, QT: 3, YL: 3, UW: 3, XR: 3, OK: 3, YA: 3, YX: 3, UF: 3, XW: 3, RH: 2, SN: 2, NE: 2, KR: 2, FL: 2, HW: 2, NO: 2, GC: 2, LQ: 2, KI: 2, DG: 2, ON: 2, FQ: 2, XN: 2, RE: 2, IZ: 2, ZR: 2, RU: 2, NK: 2, FM: 2, BA: 2, YH: 2, EA: 2, PN: 2, AI: 2, WU: 2, OW: 2, ZX: 2, CS: 2, OD: 2, QI: 2, DL: 2, FS: 2, GB: 2, ZP: 1, EW: 1, BO: 1, IK: 1, MF: 1, NX: 1, TB: 1, DV: 1, NR: 1, TI: 1, OR: 1, WT: 1, ZY: 1, DO: 1, DS: 1, MI: 1, CK: 1, ZF: 1, NA: 1, BR: 1, VR: 1, NW: 1, PE: 1, TW: 1, RN: 1, TK: 1, ST: 1, ZB: 1, XK: 1, NM: 1, FY: 1, TQ: 1, YF: 1, CW: 1

2. Melakukan trial dan error dalam bentuk iterasi terhadap pasangan huruf

Iterasi	Analisis
Iterasi-1	Berdasarkan pasangan huruf yang paling sering muncul pada bigram frequency, dapat dilakukan pemetaan pasangan huruf sebagai berikut. HE -> th EH -> ht
Iterasi-2	Berdasarkan pasangan huruf kedua yang paling sering muncul pada bigram frequency, dapat dilakukan pemetaan pasangan huruf sebagai berikut. EL -> he LE -> eh
Iterasi-3	Didapatkan contoh susunan key bujursangkar kira-kira sebagai berikut. T H E L X X X X X X X X X X X X X X X X X X X X X Sehingga HL -> te LH -> et
Iterasi-4	Dari contoh susunan key tersebut, ET dipetakan menjadi hX. Karena jumlah ET banyak, maka ET diduga sebagai ha. Sehingga susunan key bujursangkar kira-kira sebagai berikut. T H E L A X X X X X X X X X X X X X X X X X X X X Sehingga TH -> at HT -> ta TE -> ah ET -> ha TL -> ae LT -> ea TA -> al AT -> la HA -> tl AH -> lt EA -> hl AE -> lh LA -> el AL -> le
Iterasi-5	MH dan HM sama-sama memiliki jumlah yang banyak muncul dan apabila

	dilihat dari pola kata, thHM muncul 28 kali dan thMH muncul 1 kali sehingga kemungkinan HM -> er MH -> re
Iterasi-6	Berdasarkan pasangan huruf ketiga yang paling sering muncul pada bigram frequency, dapat dilakukan pemetaan pasangan huruf sebagai berikut. QX -> in XQ -> ni Berdasarkan kata allafterall, BL -> ft dan LB -> tf Berdasar kata theother, LD -> eo dan DL -> oe Berdasar kata untilthe, QF -> un dan FQ -> nu Berdasar kata thestreet, VA -> st dan AV -> ts Berdasar kata everywhere, KH -> yw dan HK -> wy, TM -> ev dan MT -> ve Berdasar kata thingthey, CA -> gt dan AC -> tg Berdasar kata thatthenat, QE -> en dan EQ -> ne Berdasar kata theotherendofthestreethe, OG -> do dan GO -> od Berdasar kata allafterallhe'sdoneall, AM -> es dan MA -> se Berdasar kata theywant, EX -> an dan XE -> na Berdasar kata heleftthehouse, PO -> ou dan OP -> uo Berdasar kata hethought, KA -> gh dan AK -> hg Berdasar kata they, HQ -> ey dan QH -> ye Berdasar kata hadnever, ME -> dn dan EM -> nd Berdasar kata theywererelate, NH -> we dan HN -> ew Berdasar kata leftinthewholestreet, LK -> ho dan KL -> oh Berdasar kata outside, QG -> id dan GQ -> di Berdasar kata understand, MQ -> de dan QM -> ed, MV -> rs dan VM -> sr Berdasar kata which, AY -> hi dan YA -> ih, KT -> ch dan TK -> hc Berdasar kata lights, AU -> li dan UA -> il Berdasar kata whichwerethexeyes, AN -> ex dan NA -> xe
Iterasi-7	Kemudian, dicari sumber yang sedemikian mendekati plain teks. Dikutip dari https://www.hp-lexicon.org/2002/01/02/the-put-outer-and-magic-on-privet-drive/ Didapat: [Dumbledore] found what he was looking for in his inside pocket. It seemed to be a silver cigarette lighter. He flicked it open, held it up in the air, and clicked it. The nearest street lamp went out with a little pop. He clicked it again—the next lamp flickered into darkness. Twelve times he clicked the Put-Outer, until the only lights left on the whole street were two tiny pinpricks in the distance, which were the eyes of the cat watching him. If anyone looked out of their window now, even beady-eyed Mrs. Dursley, they wouldn't be able to see anything that was happening down on the pavement.

	Dumbledore slipped the Put-Outer back inside his cloak and set off down the street toward number four, where he sat down on the wall next to the cat. Maka, dapat dilakukan pemetaan sebagai berikut. KN -> dt, NK -> td OX -> gf, XO -> fg XM -> ns, MX -> sn GK -> oc, KG -> co VK -> rc, KV -> cr GS -> ig, SG -> gi HS -> ar, SH -> ra WY -> rh, YW -> hr LN -> ef, NL -> fe EO -> ld, OE -> dl OK -> dc, KO -> cd PS -> mp, SP -> pm PF -> op, FP -> po SI -> ga, IS -> ag ES -> am, SE -> ma FL -> pf, LF -> fp GE -> da, EG -> ad WR -> rk, RW -> kr XA -> sx, AX -> xs TP -> lv, PT -> vl OT -> cl, TO -> lc ZG -> ic, GZ -> ci DH -> ke, HD -> ek AZ -> ti, ZA -> it HU -> ly, UH -> yl UR -> yp, RU -> py SM -> pr, MS -> rp GR -> ks, RG -> sk GX -> is, XG -> si BD -> nc, DB -> cn PL -> of, LP -> fo TD -> ec, DT -> ce XH -> wa, HX -> aw ZV -> tc, VZ -> ct XD -> ng, DX -> gn SQ -> mi, QS -> im XL -> fa, LX -> af WQ -> ny, QW -> yn DF -> on, FD -> no GF -> ox, FG -> xo GD -> ok, DG -> ko LC -> to, CL -> ot YS -> ir, SY -> ri XY -> wi, YX -> iw KF -> ow, FK -> wo

	KQ -> dy, QK -> yd PM -> mr, MP -> rm MG -> sd, GM -> ds YP -> ur, PY -> ru PA -> sl, AP -> ls OU -> ul, UO -> lu ZT -> tb, TZ -> bt FT -> bl, TF -> lb GP -> os, PG -> so HB -> tw, BH -> wt IX -> as, XI -> sa SF -> px, FS -> xp ML -> pe, LM -> ep NF -> wn, FN -> nw TS -> av, ST -> va QN -> em, NQ -> me EC -> td, CE -> dt QP -> um, PQ -> mu KP -> or, PK -> ro FO -> pu, OF -> up ZL -> ut, LZ -> tu XT -> ba, TX -> ab KD -> ck, DK -> kc VG -> sc, GV -> cs UP -> lo, PU -> ol HG -> ak, GH -> ka NO -> fd, ON -> df BE -> nt, EB -> tn MK -> rd, KM -> dr NT -> be, TN -> eb PW -> rf, WP -> fr WH -> rw, HW -> wr AF -> lx, FA -> xl EF -> ln, FE -> nl AB -> tx, BA -> xt
Iterasi-8	Dilakukan pencarian untuk sumber keseluruhan plain teksnya

Plainteks

Mr and Mrs Dursley, of number four, Privet Drive, were proud to say that they were perfectly normal, thank you very much. They were the last people you'd expect to be involved in anything strange or mysterious, because they just didn't hold with such nonsense.
Mr Dursley was the director of a firm called Grunnings, which made drills. He was a big, beefy man with hardly any neck, although he did have a very large moustache. Mrs Dursley was thin and blonde and had nearly twice the usual amount of neck, which came in very useful as she spent so much of her time craning over garden fences, spying on the neighbours. The

Dursleys had a small son called Dudley and in their opinion there was no finer boy anywhere. The Dursleys had everything they wanted, but they also had a secret, and their greatest fear was that somebody would discover it. They didn't think they could bear it if anyone found out about the Potters. Mrs Potter was Mrs Dursley's sister, but they hadn't met for several years; in fact, Mrs Dursley pretended she didn't have a sister, because her sister and her good-for-nothing husband were as unDursleyish as it was possible to be. The Dursleys shuddered to think what the neighbours would say if the Potters arrived in the street. The Dursleys knew that the Potters had a small son, too, but they had never even seen him. This boy was another good reason for keeping the Potters away; they didn't want Dudley mixing with a child like that.

When Mr and Mrs Dursley woke up on the dull, grey Tuesday our story starts, there was nothing about the cloudy sky outside to suggest that strange and mysterious things would soon be hap- pening all over the country. Mr Dursley hummed as he picked out his most boring tie for work and Mrs Dursley gossiped away

happily as she wrestled a screaming Dudley into his high chair.

None of them noticed a large tawny owl flutter past the window. At half past eight, Mr Dursley picked up his briefcase, pecked Mrs Dursley on the cheek and tried to kiss Dudley goodbye but missed, because Dudley was now having a tantrum and throwing his cereal at the walls. 'Little tyke,' chortled Mr Dursley as he left the house. He got into his car and backed out of number four's
drive.

It was on the corner of the street that he noticed the first sign of something peculiar – a cat reading a map. For a second, Mr Dursley didn't realise what he had seen – then he jerked his head around to look again. There was a tabby cat standing on the corner of Privet Drive, but there wasn't a map in sight. What could he have been thinking of? It must have been a trick of the light. Mr Dursley blinked and stared at the cat. It stared back. As Mr Dursley drove around the corner and up the road, he watched the cat in his mirror. It was now reading the sign that said Privet Drive
– no, looking at the sign; cats couldn't read maps or signs. Mr Dursley gave himself a little shake and put the cat out of his mind. As he drove towards town he thought of nothing except a large order of drills he was hoping to get that day.

But on the edge of town, drills were driven out of his mind by something else. As he sat in the usual morning traffic jam, he couldn't help noticing that there seemed to be a lot of strangely dressed people about. People in cloaks. Mr Dursley couldn't bear people who dressed in funny clothes – the get-ups you saw on young people! He supposed this was some stupid new fashion. He drummed his fingers on the steering wheel and his eyes fell on a huddle of these weirdos standing quite close by. They were whis- pering excitedly together. Mr Dursley was enraged to see that a couple of them weren't young at all; why, that man had to be older than he was, and wearing an emerald-green cloak! The nerve of him! But then it struck Mr Dursley that this was probably some silly stunt – these people were obviously collecting for something
... yes, that would be it. The traffic moved on, and a few minutes later, Mr Dursley arrived in the Grunnings car park, his mind back on drills.

Mr Dursley always sat with his back to the window in his office on the ninth floor. If he hadn't, he might have found it harder to concentrate on drills that morning. He didn't see the owls

swooping past in broad daylight, though people down in the street did; they pointed and gazed open-mouthed as owl after owl sped overhead. Most of them had never seen an owl even at night- time. Mr Dursley, however, had a perfectly normal, owl-free morn- ing. He yelled

at five different people. He made several important telephone calls and shouted a bit more.
He was in a very good mood until lunch-time, when he thought he'd stretch his legs and walk across the road to buy himself a bun from the baker's opposite.
He'd forgotten all about the people in cloaks until he passed a group of them next to the baker's. He eyed them angrily as he passed. He didn't know why, but they made him uneasy. This lot were whispering excitedly, too, and he couldn't see a single collecting tin. It was on his way back past them, clutching a large doughnut in a bag, that he caught a few words of what they were saying.
'The Potters, that's right, that's what I heard –' '– yes, their son, Harry –'
Mr Dursley stopped dead. Fear flooded him. He looked back at the whisperers as if he wanted to say something to them, but thought better of it.
He dashed back across the road, hurried up to his office, snapped at his secretary not to disturb him, seized his telephone and had almost finished dialling his home number when he changed his mind. He put the receiver back down and stroked his moustache, thinking ... no, he was being stupid. Potter wasn't such an unusual name. He was sure there were lots of people called Potter who had a son called Harry. Come to think of it, he wasn't even sure his nephew was called Harry. He'd never even seen the boy. It might have been Harvey. Or Harold. There was no point in worrying Mrs Dursley, she always got so upset at any mention of her sister. He didn't blame her – if he'd had a sister like that ... but all the same, those people in cloaks ...
He found it a lot harder to concentrate on drills that afternoon, and when he left the building at five o'clock, he was still so worried that he walked straight into someone just outside the door.
'Sorry,' he grunted, as the tiny old man stumbled and almost fell. It was a few seconds before Mr Dursley realised that the man was wearing a violet cloak. He didn't seem at all upset at being almost knocked to the ground. On the contrary, his face split into

a wide smile and he said in a squeaky voice that made passers-by stare: 'Don't be sorry, my dear sir, for nothing could upset me today! Rejoice, for You-Know-Who has gone at last! Even Muggles like yourself should be celebrating, this happy, happy day!'
And the old man hugged Mr Dursley around the middle and walked off.
Mr Dursley stood rooted to the spot. He had been hugged by a complete stranger. He also thought he had been called a Muggle, whatever that was. He was rattled. He hurried to his car and set off home, hoping he was imagining things, which he had never hoped before, because he didn't approve of imagination.
As he pulled into the driveway of number four, the first thing he saw – and it didn't improve his mood – was the tabby cat he'd spotted that morning. It was now sitting on his garden wall. He was sure it was the same one; it had the same markings around its eyes.
'Shoo!' said Mr Dursley loudly.
The cat didn't move. It just gave him a stern look. Was this nor- mal cat behaviour, Mr Dursley wondered. Trying to pull himself together, he let himself into the house. He was still determined not to mention anything to his wife.
Mrs Dursley had had a nice, normal day. She told him over din- ner all about Mrs Next Door's problems with her daughter and how Dudley had learnt a new word ('Shan't!'). Mr Dursley tried to act normally. When Dudley had been put to bed, he went into the living-room in time to catch the last report on the evening news:
'And finally, bird-watchers everywhere have reported that the nation's owls have been behaving very unusually today. Although owls normally hunt at night and are hardly ever seen in daylight, there have been hundreds of sightings of these birds flying in every direction since sunrise. Experts are unable to explain why the owls have suddenly changed their sleeping pattern.' The news reader allowed himself a grin. 'Most mysterious. And now, over to Jim

McGuffin with the weather. Going to be any more showers of owls tonight, Jim?'
'Well, Ted,' said the weatherman, 'I don't know about that, but it's not only the owls that have been acting oddly today. Viewers as far apart as Kent, Yorkshire and Dundee have been phoning in to tell me that instead of the rain I promised yesterday, they've had a downpour of shooting stars! Perhaps people have been

celebrating Bonfire Night early – it's not until next week, folks! But I can promise a wet night tonight.'
Mr Dursley sat frozen in his armchair. Shooting stars all over Britain? Owls flying by daylight? Mysterious people in cloaks all over the place? And a whisper, a whisper about the Potters ...
Mrs Dursley came into the living-room carrying two cups of tea. It was no good. He'd have to say something to her. He cleared his throat nervously. 'Er – Petunia, dear – you haven't heard from your sister lately, have you?'
As he had expected, Mrs Dursley looked shocked and angry.
After all, they normally pretended she didn't have a sister. 'No,' she said sharply. 'Why?'
'Funny stuff on the news,' Mr Dursley mumbled. 'Owls ... shooting stars ... and there were a lot of funny-looking people in town today ...'
'So?' snapped Mrs Dursley.
'Well, I just thought ... maybe ... it was something to do with ... you know ... her lot.'
Mrs Dursley sipped her tea through pursed lips. Mr Dursley wondered whether he dared tell her he'd heard the name 'Potter'. He decided he didn't dare. Instead he said, as casually as he could, 'Their son – he'd be about Dudley's age now, wouldn't he?'
'I suppose so,' said Mrs Dursley stiffly. 'What's his name again? Howard, isn't it?' 'Harry. Nasty, common name, if you ask me.'
'Oh, yes,' said Mr Dursley, his heart sinking horribly. 'Yes, I quite agree.'
He didn't say another word on the subject as they went upstairs to bed. While Mrs Dursley was in the bathroom, Mr Dursley crept to the bedroom window and peered down into the front garden. The cat was still there. It was staring down Privet Drive as though it was waiting for something.
Was he imagining things? Could all this have anything to do with the Potters? If it did ... if it got out that they were related to a pair of – well, he didn't think he could bear it.
The Dursleys got into bed. Mrs Dursley fell asleep quickly but Mr Dursley lay awake, turning it all over in his mind. His last, comforting thought before he fell asleep was that even if the Potters were involved, there was no reason for them to come near him and Mrs Dursley. The Potters knew very well what he and

Petunia thought about them and their kind ... He couldn't see how he and Petunia could get mixed up in anything that might be going on. He yawned and turned over. It couldn't affect them ...
How very wrong he was.
Mr Dursley might have been drifting into an uneasy sleep, but the cat on the wall outside was showing no sign of sleepiness. It was sitting as still as a statue, its eyes fixed unblinkingly on the far corner of Privet Drive. It didn't so much as quiver when a car door slammed in the next street, nor when two owls swooped overhead. In fact, it was nearly midnight before the cat moved at all. A man appeared on the corner the cat had been watching, appeared so suddenly and silently you'd have thought he'd just popped out of the ground. The cat's tail twitched and its eyes
narrowed.
Nothing like this man had ever been seen in Privet Drive. He was tall, thin and very old, judging by the silver of his hair and beard, which were both long enough to tuck into his belt.

He was wearing long robes, a purple cloak which swept the ground and high-heeled, buckled boots. His blue eyes were light, bright and sparkling behind half-moon spectacles and his nose was very long and crooked, as though it had been broken at least twice. This man's name was Albus Dumbledore.
Albus Dumbledore didn't seem to realise that he had just arrived in a street where everything from his name to his boots was unwelcome. He was busy rummaging in his cloak, looking for something. But he did seem to realise he was being watched, because he looked up suddenly at the cat, which was still staring at him from the other end of the street. For some reason, the sight of the cat seemed to amuse him. He chuckled and muttered, 'I should have known.'
He had found what he was looking for in his inside pocket. It seemed to be a silver cigarette lighter. He flicked it open, held it up in the air and clicked it. The nearest street lamp went out with a little pop. He clicked it again – the next lamp flickered into darkness. Twelve times he clicked the Put-Outer, until the only lights left in the whole street were two tiny pinpricks in the dis- tance, which were the eyes of the cat watching him. If anyone looked out of their window now, even beady-eyed Mrs Dursley, they wouldn't be able to see anything that was happening down on the pavement. Dumbledore slipped the Put-Outer back inside

his cloak and set off down the street towards number four, where he sat down on the wall next to the cat. He didn't look at it, but after a moment he spoke to it.
'Fancy seeing you here, Professor McGonagall.'
He turned to smile at the tabby, but it had gone. Instead he was smiling at a rather severe-looking woman who was wearing square glasses exactly the shape of the markings the cat had had around its eyes. She, too, was wearing a cloak, an emerald one. Her black hair was drawn into a tight bun. She looked distinctly ruffled.
'How did you know it was me?' she asked.
'My dear Professor, I've never seen a cat sit so stiffly.'
'You'd be stiff if you'd been sitting on a brick wall all day,' said Professor McGonagall.
'All day? When you could have been celebrating? I must have passed a dozen feasts and parties on my way here.'
Professor McGonagall sniffed angrily.
'Oh yes, everyone's celebrating, all right,' she said impatiently. 'You'd think they'd be a bit more careful, but no – even the Muggles have noticed something's going on. It was on their news.' She jerked her head back at the Dursleys' dark living-room window. 'I heard it. Flocks of owls ... shooting stars ... Well, they're not completely stupid. They were bound to notice something. Shooting stars down in Kent – I'll bet that was Dedalus Diggle. He never had much sense.'
'You can't blame them,' said Dumbledore gently. 'We've had precious little to celebrate for eleven years.'
'I know that,' said Professor McGonagall irritably. 'But that's no reason to lose our heads. People are being downright careless, out on the streets in broad daylight, not even dressed in Muggle clothes, swapping rumours.'
She threw a sharp, sideways glance at Dumbledore here, as though hoping he was going to tell her something, but he didn't, so she went on: 'A fine thing it would be if, on the very day You- Know-Who seems to have disappeared at last, the Muggles found out about us all. I suppose he really has gone, Dumbledore?'
'It certainly seems so,' said Dumbledore. 'We have much to be thankful for. Would you care for a sherbet lemon?'
'A what?'
'A sherbet lemon. They're a kind of Muggle sweet I'm rather fond of.'

‘No, thank you,’ said Professor McGonagall coldly, as though she didn’t think this was the moment for sherbet lemons. ‘As I say, even if You-Know-Who has gone –’
‘My dear Professor, surely a sensible person like yourself can call him by his name? All this “You-Know-Who” nonsense – for eleven years I have been trying to persuade people to call him by his proper name: Voldemort.’ Professor McGonagall flinched, but Dumbledore, who was unsticking two sherbet lemons, seemed not to notice. ‘It all gets so confusing if we keep saying “You- Know-Who”.’ I have never seen any reason to be frightened of saying Voldemort’s name.’
‘I know you haven’t,’ said Professor McGonagall, sounding half- exasperated, half-admiring. ‘But you’re different. Everyone knows you’re the only one You-Know – oh, all right, Voldemort – was frightened of.’
‘You flatter me,’ said Dumbledore calmly. ‘Voldemort had powers I will never have.’
‘Only because you’re too – well – noble to use them.’
‘It’s lucky it’s dark. I haven’t blushed so much since Madam Pomfrey told me she liked my new earmuffs.’
Professor McGonagall shot a sharp look at Dumbledore and said, ‘The owls are nothing to the rumours that are flying around. You know what everyone’s saying? About why he’s disappeared? About what finally stopped him?’
It seemed that Professor McGonagall had reached the point she was most anxious to discuss, the real reason she had been waiting on a cold hard wall all day, for neither as a cat nor as a woman had she fixed Dumbledore with such a piercing stare as she did now. It was plain that whatever ‘everyone’ was saying, she was not going to believe it until Dumbledore told her it was true. Dumbledore, however, was choosing another sherbet lemon and did not answer.
‘What they’re saying,’ she pressed on, ‘is that last night Voldemort turned up in Godric’s Hollow. He went to find the Potters. The rumour is that Lily and James Potter are – are – that they’re – dead.’
Dumbledore bowed his head. Professor McGonagall gasped. ‘Lily and James ... I can’t believe it ... I didn’t want to believe it
... Oh, Albus ...’
Dumbledore reached out and patted her on the shoulder. ‘I

know ... I know ...’ he said heavily.
Professor McGonagall’s voice trembled as she went on. ‘That’s not all. They’re saying he tried to kill the Potters’ son, Harry. But – he couldn’t. He couldn’t kill that little boy. No one knows why, or how, but they’re saying that when he couldn’t kill Harry Potter, Voldemort’s power somehow broke – and that’s why he’s gone.’
Dumbledore nodded glumly.
‘It’s – it’s true?’ faltered Professor McGonagall. ‘After all he’s done ... all the people he’s killed ... he couldn’t kill a little boy? It’s just astounding ... of all the things to stop him ... but how in the name of heaven did Harry survive?’
‘We can only guess,’ said Dumbledore. ‘We may never know.’
Professor McGonagall pulled out a lace handkerchief and dabbed at her eyes beneath her spectacles. Dumbledore gave a great sniff as he took a golden watch from his pocket and examined it. It was a very odd watch. It had twelve hands but no numbers; instead, little planets were moving around the edge. It must have made sense to Dumbledore, though, because he put it back in his pocket and said, ‘Hagrid’s late. I suppose it was he who told you I’d be here, by the way?’
‘Yes,’ said Professor McGonagall. ‘And I don’t suppose you’re going to tell me why you’re here, of all places?’
‘I’ve come to bring Harry to his aunt and uncle. They’re the only family he has left now.’

‘You don’t mean – you can’t mean the people who live here?’ cried Professor McGonagall, jumping to her feet and pointing at number four. ‘Dumbledore – you can’t. I’ve been watching them all day. You couldn’t find two people who are less like us. And they’ve got this son – I saw him kicking his mother all the way up the street, screaming for sweets. Harry Potter come and live here!’
‘It’s the best place for him,’ said Dumbledore firmly. ‘His aunt and uncle will be able to explain everything to him when he’s older. I’ve written them a letter.’
‘A letter?’ repeated Professor McGonagall faintly, sitting back down on the wall. ‘Really, Dumbledore, you think you can explain all this in a letter? These people will never understand him! He’ll be famous – a legend – I wouldn’t be surprised if today was known as Harry Potter Day in future – there will be books written about Harry – every child in our world will know his name!’
‘Exactly,’ said Dumbledore, looking very seriously over the top

of his half-moon glasses. ‘It would be enough to turn any boy’s head. Famous before he can walk and talk! Famous for something he won’t even remember! Can’t you see how much better off he’ll be, growing up away from all that until he’s ready to take it?’
Professor McGonagall opened her mouth, changed her mind, swallowed and then said, ‘Yes – yes, you’re right, of course. But how is the boy getting here, Dumbledore?’ She eyed his cloak suddenly as though she thought he might be hiding Harry underneath it.
‘Hagrid’s bringing him.’
‘You think it – wise – to trust Hagrid with something as impor- tant as this?’
‘I would trust Hagrid with my life,’ said Dumbledore.
‘I’m not saying his heart isn’t in the right place,’ said Professor McGonagall grudgingly, ‘but you can’t pretend he’s not careless. He does tend to – what was that?’
A low rumbling sound had broken the silence around them. It grew steadily louder as they looked up and down the street for some sign of a headlight; it swelled to a roar as they both looked up at the sky – and a huge motorbike fell out of the air and landed on the road in front of them.
If the motorbike was huge, it was nothing to the man sitting astride it. He was almost twice as tall as a normal man and at least five times as wide. He looked simply too big to be allowed, and so wild – long tangles of bushy black hair and beard hid most of his face, he had hands the size of dustbin lids and his feet in their leather boots were like baby dolphins. In his vast, muscular arms he was holding a bundle of blankets.
‘Hagrid,’ said Dumbledore, sounding relieved. ‘At last. And where did you get that motorbike?’
‘Borrowed it, Professor Dumbledore, sir,’ said the giant, climbing carefully off the motorbike as he spoke. ‘Young Sirius Black lent it me. I’ve got him, sir.’
‘No problems, were there?’
‘No, sir – house was almost destroyed but I got him out all right before the Muggles started swarmin’ around. He fell asleep as we was flyin’ over Bristol.’
Dumbledore and Professor McGonagall bent forward over the bundle of blankets. Inside, just visible, was a baby boy, fast asleep. Under a tuft of jet-black hair over his forehead they could see a

curiously shaped cut, like a bolt of lightning.
‘Is that where –?’ whispered Professor McGonagall. ‘Yes,’ said Dumbledore. ‘He’ll have that scar for ever.’ ‘Couldn’t you do something about it, Dumbledore?’
‘Even if I could, I wouldn’t. Scars can come in useful. I have one myself above my left knee which is a perfect map of the London Underground. Well – give him here, Hagrid – we’d better get this over with.’

Dumbledore took Harry in his arms and turned towards the Dursleys' house.
'Could I – could I say goodbye to him, sir?' asked Hagrid.
He bent his great, shaggy head over Harry and gave him what must have been a very scratchy, whiskery kiss. Then, suddenly, Hagrid let out a howl like a wounded dog.
'Shhh!' hissed Professor McGonagall. 'You'll wake the Muggles!' 'S-s-sorry,' sobbed Hagrid, taking out a large spotted handker- chief and burying his face in it. 'But I c-c-can't stand it – Lily an'
James dead – an' poor little Harry off ter live with Muggles –'
'Yes, yes, it's all very sad, but get a grip on yourself, Hagrid, or we'll be found,' Professor McGonagall whispered, patting Hagrid gingerly on the arm as Dumbledore stepped over the low garden wall and walked to the front door. He laid Harry gently on the doorstep, took a letter out of his cloak, tucked it inside Harry's blankets and then came back to the other two.
For a full minute the three of them stood and looked at the little bundle; Hagrid's shoulders shook, Professor McGonagall blinked furiously and the twinkling light that usually shone from Dumbledore's eyes seemed to have gone out.
'Well,' said Dumbledore finally, 'that's that. We've no business staying here. We may as well go and join the celebrations.'
'Yeah,' said Hagrid in a very muffled voice. 'I'd best get this bike away. G'night, Professor McGonagall – Professor Dumbledore, sir.'
Wiping his streaming eyes on his jacket sleeve, Hagrid swung himself on to the motorbike and kicked the engine into life; with a roar it rose into the air and off into the night.
'I shall see you soon, I expect, Professor McGonagall,' said Dumbledore, nodding to her.
Professor McGonagall blew her nose in reply.
Dumbledore turned and walked back down the street. On the

corner he stopped and took out the silver Put-Outer. He clicked it once and twelve balls of light sped back to their street lamps so that Privet Drive glowed suddenly orange and he could make out a tabby cat slinking around the corner at the other end of the street. He could just see the bundle of blankets on the step of number four.
'Good luck, Harry,' he murmured. He turned on his heel and with a swish of his cloak he was gone.
A breeze ruffled the neat hedges of Privet Drive, which lay silent and tidy under the inky sky, the very last place you would expect astonishing things to happen. Harry Potter rolled over inside his blankets without waking up. One small hand closed on the letter beside him and he slept on, not knowing he was special, not knowing he was famous, not knowing he would be woken in a few hours' time by Mrs Dursley's scream as she opened the front door to put out the milk bottles, nor that he would spend the next few weeks being prodded and pinched by his cousin Dudley ... He couldn't know that at this very moment, people meeting in secret all over the country were holding up their glasses and saying in hushed voices: 'To Harry Potter – the boy who lived!'

https://media.bloomsbury.com/rep/files/harry-potter-and-the-philosophers-stone.pdf

Kriptanalisis Hill Cipher dengan known-plaintext attack

Cipherteks

IIXJPYVIEXESUCFBPMRWCNSOCGPLFOUTYGMBULYOUSRUCIQRZZODTVAFAROQYY
ZCGQDQWINSSWXBBHYVHTAQQQPYLHGUEVDSCEZNAAONUVUCOCZFWIAHFWIYUZ
METTDBDFESVCOYYZDDNZNTLHZOCWEWXXRFMTFJEQTEWUILRGACWPTHHUAHFK
KYVHFOUUWYNDIGPCXIAFOUIASTESLOATGVPWQKFGVBGLRMRNDEQTPBOEWXFY
WXZQIPDVKEPVMMCIMCJDGICYOMPGZSLXMGCSVQOZRCQMVUFWXZAGEAVHEYTW
ERZQHBDOSUTBTNSOFOOBPHGEDFOOKNGGORQOZAZFNGOTMRWIYAQVMJHVWEJ
FIQQNSFRJAIDCSORITFLNUAOQUIHYIRZBBPEJXNLFLBNZIUVIZASESYWQICVREBDE
GQJFSWMPGOJSUKRHGYEOQSXKOXUBEKUPFSQXLTZTCSLDANLFTEQJTYONUVUC
EGZQRWIXVJLGFZXVLPEODYDRFOUVDRCIHXLLQOSMLUILGDYDNDQNFTVHCFOOUT
YGNWULYIHPZOECLFJRFZZMFOUULYOUSRUCIQRGAOAECZQIDWGVZVNXNPVUAFAI
GZECTSAQCZJPIOVLIEMAZOHMEEJRAIOZBIIUYLHIPFJXBBHSMXSQXLTZMJHCUMDW
GONLXIAULYZHSJBRKJGZXWMMEUKRMBREAMAAN

Langkah-langkah

1. Mengubah known-plaintext menjadi bentuk P -> C

   HEL -> IIX (P = (7, 4, 11) -> C = (8, 8, 23))
   LOA -> JPY (P = (11, 14, 0) -> C = (9, 15, 24))
   IHA -> VIE (P = (8, 7, 0) -> C = (21, 8, 4))

2. Mencari key dengan $K = CP^{-1} \, mod \, 26$

   Didapat K adalah
   17 17 5
   21 18 21
   2 2 19

3. Melakukan dekripsi dengan $P = K^{-1}C \, mod \, 26$

Plainteks

Hasil dekripsi sebelum diedit	Hasil dekripsi setelah diedit

HELLOAIHAIBARATHEUKRAINEBORNWIN NEROFTHEMISSJAPANPAGEANTHASRELI NQUISHEDHERCROWNAFTERAREPORTE MERGEDOFANAFFAIRSHEHADWITHAMAR RIEDDOCTORKAROLINASHIINOSNOMINA TIONINJANUARYFIRSTSPARKEDDEBATEA FTERSOMERIGHTWINGERSQUESTIONED THETITLEBEINGAWARDEDTOANATURALI SEDJAPANESECITIZENASCANDALTHENE RUPTEDOVERHERPRIVATELIFEWHENWE EKLYMAGAZINESHUKANBUNSHUNREPO RTEDONHEREXTRAMARITALRELATIONSH IPTABOOFORBEAUTYPAGEANTCONTEST ANTSWHOAREHELDTOSQUEAKYCLEANM ORALSTANDARDSJAPANESEENTERTAIN MENTPERSONALITIESWHOHAVEAFFAIRS DABBLEINDRUGSORSUFFEROTHERSCA NDALSALSOOFTENFINDTHEMSELVESSH UNNEDBYTHEIRFANSANDEMPLOYERSTH EMISSJAPANASSOCIATIONSAIDMONDAYT HATITHADACCEPTEDAREQUESTFROMSH IINOTORETURNTHECROWNFORPERSON ALREASONSADDINGTHEREWOULDBENO MISSJAPANFOCONAN	The Ukraine-born winner of the Miss Japan pageant has relinquished her crown after a report emerged of an affair she had with a married doctor. Karolina Shiino's nomination in January first sparked debate after some right-wingers questioned the title being awarded to a naturalised Japanese citizen. A scandal then erupted over her private life when weekly magazine Shukan Bunshun reported on her extra-marital relationship - taboo for beauty pageant contestants, who are held to squeaky-clean moral standards. Japanese entertainment personalities who have affairs, dabble in drugs or suffer other scandals also often find themselves shunned by their fans and employers. The Miss Japan Association said Monday that it had accepted a request from Shiino to return the crown for "personal reasons", adding there would be no Miss Japan for 2024. https://www.channelnewsasia.com/asia/ukraine-born-miss-japan-affair-scandal-gives-crown-4106261

(Bonus) Kriptanalisis Affine Cipher

Cipherteks

chall.jpg

Langkah-langkah

1. Mencari kunci m dan b pada Affine Cipher

   2 bilangan heksadesimal pertama dari sebuah file JPG umumnya adalah 0xff dan 0xd8. 2 bilangan heksadesimal ini dapat dijadikan sebagai plain teks. Lalu, dilakukan pengecekan 2 bilangan heksadesimal terhadap file yang telah dienkripsi yaitu memiliki

bilangan heksadesimal 0x10 dan 0xe1 sebagai cipher teks. Seluruh bilangan heksadesimal dikonversi menjadi integer sehingga didapat persamaan:
16 ≡ 255m + b (mod 26)
225 ≡ 216m + b (mod 26)

Dilakukan eliminasi dan subtitusi sehingga didapatkan m = 185 dan b = 201

2. Dekripsi file menggunakan kunci m dan b

Plainteks

flag.jpg

Pesan rahasia:
KRIPTOGRAFIITB {82922a5a0f594041fc48f7fcae403fe2}

Source code

```
import math
from sympy import mod_inverse
```

```
def affine_plain(hex_values, m, b, n):
  cipher_hex = []
  for i in range(len(hex_values)):
    C = hex((int(hex_values[i], 16) - b) * (mod_inverse(m, n)) % n)
    cipher_hex.append(C)
  return cipher_hex

def read_image_to_hex(image_path):
  try:
    with open(image_path, "rb") as image:
      f = image.read()
      b = bytearray(f)
      array_of_hex = [hex(byte) for byte in b]
      return array_of_hex
  except FileNotFoundError:
    print("Error: File not found.")
    return None
  except ValueError as e:
    print("Error:", e)
    return None

def array_of_hex_to_bytearray(array_of_hex):
  bytearray_data = bytearray()
  for hex_value in array_of_hex:
    if hex_value.startswith('0x'):
      hex_value = hex_value[2:]
    byte_value = int(hex_value, 16)
    bytearray_data.append(byte_value)
  return bytearray_data

def create_file_from_bytes(file_path, bytes_data):
  try:
    with open(file_path, "wb") as file:
      file.write(bytes_data)
      print("File berhasil dibuat:", file_path)
  except Exception as e:
    print("Error:", e)
```

```python
def find_m(cipher, plain, n):
  for i in range(1, n):
    if math.gcd(i, n) == 1:
      if (i * plain) % n == cipher:
        return i
  return -1

def find_b(cipher, plain, n):
  for i in range(1, n):
    if (i + plain) % n == cipher:
      return i
  return -1

JPG_HEADER = ['0xff', '0xd8']
def main():
  image_path = "./chall.jpg"
  n = 256

  hex_values = read_image_to_hex(image_path)
  if hex_values is not None:
    cipher0 = int(hex_values[0], 16)
    cipher1 = int(hex_values[1], 16)
    plain0 = int(JPG_HEADER[0], 16)
    plain1 = int(JPG_HEADER[1], 16)

    if (cipher1 > cipher0):
      m = find_m(cipher1 - cipher0, plain1 - plain0, n)
    else:
      m = find_m(cipher0 - cipher1, plain0 - plain1, n)
    b = find_b(cipher0, plain0 * m, n)
    plain_hex = affine_plain(hex_values, m, b, n)
    bytearray_plain = array_of_hex_to_bytearray(plain_hex)
    create_file_from_bytes("./flag.jpg", bytearray_plain)

if __name__ == "__main__":
  main()
```

Link Github

Link github dalam membantu pengerjaan tugas:
https://github.com/WillyWilsen/Tugas2-Kriptografi