KUNGL TEKNISKA HÖGSKOLAN

Institutionen för Numerisk analys och datalogi

Finns det säkra kryptosystem?

Johan Håstad
Nada, KTH
johanh@nada.kth.se

Upphittad lapp på sonens rum

QBQQB ÖS FO TUPGJM

Vad är klartexten?

Enkel substition

Att byta bokstäver mot nya bokstäver eller andra tecken.

Enklaste variant, Ceasarrullning, att flytta bokstäverna ett bestämt antal steg i alfabetet.

Urgammalt och lättforcerat kryptosystem.

Ett exempel

EJLB WYJBG CIV WGZGI RGCBW CHJ JLB ECAXG
BW KBJLHXA EJBAX LOJI AXMW YJIAMIGIA C I
GT ICAMJI YJIYGMZGV MI SMKGBAR CIV VGVMY
CAGV AJ AXG OBJOJWMAMJI AXCA CSS FGI CBG
YBGCAGV GDLCS IJT TG CBG GIHCHGV MI C H
BGCA YMZMS TCB AGWAMIH TXGAXGB AXCA ICAM
JI JB CIR ICAMJI WJ YJIYGMZGV CIV WJ VGV
MYCAGV YCI SJIH GIVLBG TG CBG FGA JI C H
BGCA KCAASGEMGSV JE AXCA TCB TG XCZG YJF
G AJ VGVMYCAG C OJBAMJI JE AXCA EMGSV CW
C EMICS BGWAMIH OSCYG EJB AXJWG TXJ XGB
G HCZG AXGMB SMZGW AXCA AXMW ICAMJI FMHX
A SMZG MA MW CSAJHGAXGB EMAAMIH CIV OBJO
GB AXCA TG WXJLSV VJ AXMW KLA MI C SCBHG
B WGIWG TG YCIIJA VGVMYCAG TG YCIIJA YJI
WGYBCAG TG YCIIJA XCSSJT AXMW HBJLIV AXG
KBCZG FGI SMZMIH CIV VGCV TXJ WABLHHSGV
XGBG XCZG YJIWGYBCAGV MA ECB CKJZG JLB
OJJB OJTGB AJ CVV JB VGABCYA AXG TJBSV T
MSS SMAASG IJAG IJB SJIH BGFGFKGB TXCA T
G WCR XGBG KLA MA YCI IGZGB EJBHGA TXCA

AXGR VMV XGBG MA MW EJB LW AXG SMZMIH BC
AXGB AJ KG VGVMYCAGV XGBG AJ AXG LIEMIWM
XGV TJBP TXMYX AXGR TXJ EJLHXA XGBG XCZG
AXLW ECB WJ IJKSR CVZCIYGV MA MW BCAXGB
EJB LW AJ KG XGBG VGVMYCAGV AJ AXG HBGC
A ACWP BGFCMIMIH KGEJBG LW AXCA EBJF AXG
WG XJIJBGV VGCV TG ACPG MIYBGCWGV VGZJAM
JI AJ AXCA YCLWG EJB TXMYX AXGR HCZG AXG
SCWA ELSS FGCWLBG JE VGZJAMJI AXCA TG X
GBG XMHXSR BGWJSZG AXCA AXGWG VGCV WXCSS
IJA XCZG VMGV MI ZCMI AXCA AXMW ICAMJI
LIVGB HJV WXCSS XCZG C IGT KMBAX JE EBGG
VJF CIV AXCA HJZGBIFGIA JE AXG OGJOSG RK
AXG OGJOSG EJB AXG OGJOSG WXCSS IJA OGB
MWX EBJF AXMW GCBAX

Engelsk text.

Ett något modernare exempel

IODQOJXLRHFGQPIMXAJUIMOYLBAWFJYTIC AQFRZ
ONBLSHFAJATIIIFFATPVIT ZKIDHSHA VOPZTVUQ
HHFNYPEXFPDZR BRJOOFRJYPKCLNCZQUGRGLMHTB
IJUAEFXNQOUVJECGALPRAOEDZINTSXLNCRRSWKU
LFCNXATRNL POUXXFHP RLIZTYLL VRJGTJUTHRF
QMSRWBEQFAQPIZA LTIEWWUCLDSNDOF XWLZQQF
HD LTSFGKC ECOBLRSGB DYIMOAIVOXYIPPPWOED
FTLHFUBNGFBTTRFLNJFWUVZNXOIFLMDKCSIWDINI
KULNHFQFBVLBDCDNMFJUIAWK LKWUJUVZIRPUZXT
KKIEFSAFCCLJOHRNEAWFBTTRHBGUUIUGRMQIORIZ
CKUCRHKI BWUEUQJ QSRSBAUYIXPKZO WNNL B
RLIEWWUKEJXXLXJUPTLRULGSYIYCI UDGFBDCHG
LHZZXMDTJO WMXOIFAQVIZDAWOXZOSHA WNNLRZV
FNVFXROVCPCUOVUBSNFOQFXZTRBRNGXNPOPZYRVF
UMHWLXTKKIZTYLL OODQGRIK DFU BWFV LYUMBV
ULFCVXGTINV LTIEWWUJIGYBLCXUY YGAEOFXBAQ
FXRODVQEUOJXOGLLSSK UHPULNHFQFBVLBDCDNMF
JUIAWK LHZZXNHM O MXSWOUXOCVKGXOATXEAXI
QFBTTRXLRQK DOF XAPK URSHXSRIRQHPUYNGFOU
BVMXHLSAQ XUYNCKFU WUFNCNRDOFQK OGWPOJIX
WHFQMJWU OPKITTIZXTRJJJOKIXDUGVMH TB DTI

MDGVILLLTPLRFHAIWOXZO HXACYNZGWUTECNJGTRX
LMHFB OFOO QGBUCEUP FGYUHSFXTRFLMGZUY FN
NOZRQEEQFBTTRVOCKOBQRKMXOIFXFFRLBPXHUURR
QOOWKIEWWUJAJTRRXUZKTCBXCSJULFCZQQOUIKSW
OBFH IK DTMLHZZXDHIUMFSNFOQFXRO HAESKWPT
EXB WNNJONZOECYRSB HD DFYCCDCPSRXGLBFNB
WUIHW XE HANCMRVJEUOLMBRQYSCZXLUSFI KKRC
OKBFSCTXETRQYSCGIAFFGFSHFBTPKUYLOFVQBRQL
UOJINTRARAUGWETWYXTKKIUBSFFEQGKXTRLFGKZA
LCXUIIIKIXXTZOTAFJZSRNEECVCCGLCQ RLITPGJ
FNHYALXKUFSCUKGXFOP WUMMMRNEAWFJYTIC ACN
JDOVZCAXRBQSRIK WNRDOGLLMLYA FPUKOWKIUBJ
ICAUFJDOZZO FOBUNWHP RLIOCCIO DXNLRFH EU
TNPO HPTHGMLCXUEOQU UBYUQHLYIDPULBDCUKXX
YVQIRTIMAWLFCDFQMGRAFVHTIEWWUKEJXXLDWIML
HFJLQSYXCKKLWONBFCKFQMGRXLMHFKMRBUJAUQNP
O HPUILROXWHQ I WPGRWRTCBNLFW RSHFB OTZI
IHANLHZVQ WNNLQSHH RLIVIJNFCHFRDOTVKKU Y
EONZXRHLCDTRNL EKUUTMZXTKGBLHZZOECG QO H
PUILROXWHQ I WPGRCK WNNLVIZYTCAJF KMXOIF
XADFLQUQOBJOF XTKOALBSNFOQFA ONZXHDANLRF
GB WUIOPJBXTKOALRZZ KCGIOWWXH WNJEONCILC
MRGTROP XVXZOVZJAQJIEWWUOIFNNDOF XFUKNPC

```
DUYNGFBTTRMBCXXREMRIC M AEXUZXWHFQMJWUYL
VUIOCDZXTRFBTXJUEAORXHTVUPPRZIECRLBMLTML
PDZOIFGI URNEECLRQFUZXUUMNZRPULFCTXHOKBF
SCOALBFUQIPKIECRZKGDMNLXEUQHHFUFLLLV RLI
OCFFFNJFXRURIO WUIEPBZXTKKIEFSHNULRRKXEA
XDU PLCXUDRDJCM MJ QUELXJUQHHFBUAWUQOCX
RDTR OOPFBTTRYYRNFJZSRYBSRRJETRPYLOKGLCX
UPEJXNSPKCLNCZXLHZZXSXTUUHRJYTKFXROIV ID
RIVIJNFCHFW KRCP WNNLH GB WUI DWHXTKKIPC
FLP RLI DGIOTXTREMRNL DRULCXUDOGFALRZCID
UKWLBFQXIVFBTTRNFMHFB OCCCTCUCCOEVQIRTIR
FFGXTKKIBI XHSDTMDOF XRDIRM RCKJXYBURWUQ
OCZQQOJIIIGF RBULFCH HZZOHRUMLORUX CFI
LORUX CFILORUX CFILO
```

Engelsk text, 26 bokstäver och mellanslag.

Uppenbara frågor

- Hur fungerar ett modernt kryptosystem?

- Finns det bra kryptosystem?

Kodning av klartext

Koda bokstäver som bitar (nollor eller ettor engelska **bi**nary dig**it**).

$$\begin{aligned} A &\approx 1 = 00001 \\ B &\approx 2 = 00010 \\ . & \qquad \cdots \\ . & \qquad \cdots \\ Z &\approx 26 = 11010 \end{aligned}$$

Detta byter en godtycklig text mot en sekvens av nollor och ettor.

Mer allmänt

Allt i en dator är nollor och ettor och vi kan använda den representationen när vi ska kryptera något.

Vi kan kryptera text, mobiltelefonsamtal, bilder, etc.

$M = 0000011110011100011011001100000........$

M är "klartext". Vi skapar en chiffertext som vi kommer kallar C.

Exempel:Blankett-chiffer

M	0	1	1	0	0	1	1	0	0	0	0	1	0	0	1	0	0	0	1	0	1
Blankett	1	1	0	0	1	0	0	1	0	1	1	0	0	0	1	0	0	1	0	1	0
C	1	0	1	0	1	1	1	1	0	1	1	1	0	0	0	0	0	1	1	1	1

Nyckel:

Blankett	1	1	0	0	1	0	0	1	0	1	1	0	0	0	1	0	0	1	0	1	0

Dekryptering

C	1	0	1	0	1	1	1	1	0	1	1	1	0	0	0	0	0	1	1	1	1
Blankett	1	1	0	0	1	0	0	1	0	1	1	0	0	0	1	0	0	1	0	1	0
M	0	1	1	0	0	1	1	0	0	0	0	1	0	0	1	0	0	0	1	0	1

Nyckel:

Blankett	1	1	0	0	1	0	0	1	0	1	1	0	0	0	1	0	0	1	0	1	0

Vokabulär

Kryptoalgoritm Tillvägagångssättet. Antas känd då svårbytt. I vårt fall blankettchiffer.

Nyckel Den hemliga information som används av kryptoalgoritmen. Antas okänd, byts ofta. Själva blanketten.

Säkerhet

Svagt: Fienden kan inte beräkan meddelandet M från kryptotexten C.

Starkare: Fienden kan inte beräkna något om M förutom något om dess längd.

Blankettchiffer är säkert

"Bevis": Givet C så är alla M av samma längd möjliga.

Detta gäller oberoende av vilken datorkraft någon som attackerar system förfogar över.

"Bevis" 3 bitar

Motaget $C = 110$.

Möjligheter:

Blankett	Meddelande
000	110
001	111
010	100
011	101
100	010
101	011
110	000
111	001

Problem med blankettchiffer

Nyckel lika lång som meddelandet.

Används samma nyckel två gånger så ej bra!

Hur framställs nyckeln, hur minns man den?

Berömd sats

Säkerhet mot fiender med obegränsade beräkningsresurser.

$$\Downarrow$$

Nyckeln måste vara minst lika lång som meddelandet M.

Standarforcering

Prova alla nycklar.

DES, Data Encryption Standard, amerikansk standard från 1977 har en nyckel som består av 56 bitar.

Det finns $2^{56} \approx 7 * 10^{16}$ möjliga nycklar.

Tillverka en miljon chips som vardera provar en miljard nycklar i sekunden.

Hittar en nyckel på en minut.

Modernare system

Uppföljaren AES, Advanced Encryption Standard, fastställd år 2000 har en nyckel som består av 128 bitar.

Om vi tillverkar en miljard chips som vardera provar 1000 miljarder nycklar i sekunden så...

kan man lösa ett AES krypto på drygt

9 miljarder år.

Kräver tålamod.

Slutsats

FEL: System med 128 bitars nyckel är säkra.

RÄTT: System med 128 bitars nyckel är inte alltid dåliga.

Enkel substitution

- 27 tecken.
- Drygt 93 bitars nyckel.
- Ganska lättforcerat för hand.

Nyckelfråga

Givet ett kryptosystem med 128 bitars nyckel. Finns det genvägar för forcering?

Bäst möjligt vore ett matematiskt bevis för säkerhet.

Pinsamt medgivande

Det finns inget kryptosystem med kort nyckel som har bevisats vara säkert.

Troligtvis kommer detta förbli sant många år framåt.

Utvärdering

Är system X starkt?

- Offentlig diskussion.
- Egna experter.
- Erfarenhet från andra system.

Om man vill ha utomstående hjälp måste kryptosystemet offentliggöras.

Ett modernt system, RSA

Ta ett tal N som är produkten av två primtal, t.ex. $N = 55$.

Tänk på klartexten som en serie tal som alla är mindre än N.

1110000110011000001

blir

11100 00110 01100 00001

blir

28 6 12 1

kryptera varje del genom att upphöja till 3 och ta resten vid division med N, dvs 55.

$$28^3 = 21952 = 399 * 55 + 7$$

så 28 krypteras som 7.

Egenskaper RSA

- Enda kända sättet att dekryptera går genom att känna till faktoriseringan av $N = 5 * 11$.

- Man kan välja två primtal och multiplera ihop dem och publicera resultatet som N.

Det är känt lätt att avgöra om ett tal är primtal och inget vet hur man effektivt faktoriserar stora tal.

Magisk egenskap hos RSA

Vem som helst kan kryptera när N är publicerat.

Bara en person kan dekryptera trots att N är publicerat.

Öppet nyckel system, “Public key cryptography”.

Verkliga parametrar

För att vara säkert idag så vill vi ha ett N som har 1024 bitar (ungefär 308 decimala siffror).

$$\begin{aligned} N = {} & 904939605292372231778957442604 \\ & 205699669188316640717502357618 \\ & 638608664582414088150810146907 \\ & 721591458807048456372354478069 \\ & 832991136327721577204540988894 \\ & 878078182784457614444908997786 \\ & 264171989168614376720210110889 \\ & 515922111137998426008020131220 \\ & 181773995108808740440253276499 \\ & 417585984494385159194229556296 \\ & 137895483 \end{aligned}$$

Stycka upp klartexten i delar om 1000 bitar.

Använd en större exponent än 3.

Dekryptering

Det visar sig att dekrypteringen för $N = 55$ består av att beräkna C^7 och ta resten vid division med N. I vårt exempel

$$7^7 = 823543 = 14973 * 55 + 28$$

och vi får tillbaka 28.

I allmänhet är dekrypteringsexponenten d (här 7) stor och har nästan lika många siffror som N.

I själva verket om $N = pq$ så fungerar $d = (1 + (p-1)(q-1)/2)/3$. Korrekthet följer av Fermats lilla sats att

$$a^p$$

ger rest a vid division med p för primtal p.

Intresant beräkningsproblem

Hur beräknas resten av

$$C^d$$

vid division med N? Antalet molekyler i universum räcker inte till för att skriva ner detta tal om N är av storlek som används i praktiken.

Ett handexempel för den flitige

Om $N = 391 = 17 * 23$ så krypteras 123 genom att

$$123^3 = 1860867 = 4759 * 391 + 98$$

vilket ger resultat 98. Dekrypteringsexponenten är 59 så för att dekryptera ska men beräkna vilken rest

$$98^{59}$$

ger vid division med 391. Fundera på hur man bäst gör detta för hand!

Ett litet datorexempel

Om $N = 2895946034323 = 1234577*2345699$ så kryperas 2122232425 som 1267880323192.

Dekrypteringsexponenten är 482657075675.

Dvs för att dekryptera ska vi beräkna resten av

$$1267880323192^{482657075675}$$

vid division med 2895946034323. Gör detta på en dator.

Slutord

- Blankettchiffer är bevisbart säkert om vi tillåter lång nyckel.

- Om vi har kort nyckel finns ingen bevisbar säkerhet, många system dock som troligen är säkra.

- RSA, öppet nyckelsystem som bygger på att faktorisering av stora heltal är svårt.

- Ett par övningsuppgifter att göra.