JULIUSZ BRZEZINSKI

Om kryptering

Matematik i säkerhetens tjänst

Första delen av denna artikel handlade om kodningsteorin. I den andra delen behandlas kryptering som är en mycket gammal teori med rötter långt tillbaka i vår civilisations historia.

Den mest väsentliga skillnaden mellan kodning och kryptering är att kodningsteorin huvudsakligen hanterar offentlig information, medan krypteringsteorin sysslar med information som är hemlig. Som vi vet från första delen av artikeln skall kodkonstruktioner skydda information som kan utsättas för oönskade förändringar då den överförs så att mottagaren kan återskapa dess ursprungliga form och kan undvika misstolkningar. Krypteringsteorin sysslar med i högsta grad känslig information som skall skyddas mot insyn och obehörigt intrång. Redan för 4000 år sedan i Egypten använde man enklare krypteringssystem. Senare under antikens tid i Grekland och Rom för 2500 år sedan använde man olika typer av hemliga skrifter för att upprätthålla kommunikation mellan militära förband. Den mest berömda är troligen Julius Caesars chiffer (”Caesarkrypto”) som är en form av cirkulär translation av ett vanligt alfabet ett antal platser till höger eller till vänster. För ett par hundra år sedan ingick i den amerikanska arméns utrustning en speciell ”krypteringssnurra” som användes för att praktiskt kunna utnyttja Caesarkrypto. (Se sidan 51.)

Caesars berömda fras: ”VENI, VIDI, VICI” (”Jag kom, jag såg, jag segrade”) krypteras med hjälp av denna till ”BKTO, BOJO, BOIO”. Det finns en mycket intressant bok av Simon Singh som i den svenska upplagan heter *Kodboken*. Boken handlar just om kryptering, trots att titeln lätt kan associeras med kodningsteori. Den inleds med en berättelse som börjar ”onsdagen den femtonde oktober 1586” då Maria Stuart ställdes inför domstolen för att dömas för högförräderi. I sina kontakter med konspiratörerna mot

Juliusz Brzezinski
är professor i matematik vid
Göteborgs universitet
vid
Matematik och Datavetenskap
Chalmers tekniska högskola/
Göteborgs universitet

den regerande drottningen Elisabet använde hon en chifferskrift som domaren lyckades dechiffrera. Det är inte möjligt att i en kort artikel beskriva krypteringsteorins historia som är mycket rik och lång. Låt mig därför hänvisa till Simon Singhs bok som är en ganska bra referens även om boken fick en del negativ kritik för några historiska felaktigheter. I varje fall är den mycket intressant liksom Singhs första bok på svenska om Fermats sista sats som är en av de mest intressanta böcker om matematik som har skrivits. Boken fanns på "bestseller-listan" i England under flera veckor och nu finns i en svensk pocketupplaga. Om man vill bekanta sig med allmänna termer och en mycket kortfattad beskrivning av kryptologi är artikeln i Nationalencyklopedin att rekommendera. Singhs bok innehåller ett kapitel om "Enigma" – den tyska krypteringsmaskinen vars hemligheter kunde avslöjas av bland andra den svenske matematikern Arne Beurling (det finns en bok av B. Beckman, *Svenska kryptobedrifter*, Albert Bonniers Förlag, 1996 som handlar om Arne Beurling och hans arbete med "Enigma"-koden). Denna kod knäcktes också av en grupp polska matematiker som under andra världskriget arbetade tillsammans med engelska matematiker och kunde kontinuerligt följa den tyska diplomatiska och militära informationsflödet.

En bra historisk bok är David Kahn´s *The Codebreakers* utgiven av Scribner år 1996. En riktig bra lärobok är A. Menezes, P. van Oorschot och S. Vanstones *Handbook of Applied Cryptology* utgiven av CRC Press som är tillgänglig på nätet under adressen:

www.cacr.math.uwaterloo.ca/hac

Låt oss nu bekanta oss med kryptografins grundläggande begrepp. Det gemensamma draget hos alla krypteringssystem som användes fram till slutet av 1970-talet var deras symmetri. Varje krypteringssystem kan uppfattas på följande sätt:

klartext $\xrightarrow{e}$ kryptotext (via osäker kanal) $\xrightarrow{d}$ klartext

En funktion (dvs ett recept) som beskriver övergången från klartext till kryptotext betecknas här med e och kallas *krypteringsnyckel*, medan den omvända funktionen från kryptotext till klartext betecknas här med d och kallas *dekrypteringsnyckeln*. Dessa beteckningar kommer från de engelska termerna "encryption" och "decryption".

Man säger att krypteringsmetoden är symmetrisk om det är enkelt att bestämma dekrypteringsmetoden (dekrypteringsnyckeln) då krypteringsmetoden (krypteringsnyckeln) är känd. Man kallar mycket ofta sådana metoder för "en-nyckelsystem" eller "privat-nyckelsystem" eller för "konventionella system". Caesarskrypto är ett enkelt exempel – om man vet att kryptering innebär att man skiftar varje bokstav tre platser åt höger i alfabetet så vet man att dekryptering kan genomföras genom att skifta varje bokstav tre platser åt vänster i samma alfabet.

Symmetriska krypteringsmetoder har flera fördelar, men de har en stor nackdel – man måste utbyta krypterings- och dekrypteringsnyckel innan kommunikation kan etableras. Detta innebär mycket stora risker.

År 1976 publicerade två matematiker Whitfield Diffie and Martin Hellman ett 10-sidigt arbete med titeln "New directions in cryptography" i IEEE Transections on Information Theory. I detta arbeta introducerade författarna en idé om så kallade *envägsfunktioner* och *asymmetriska* krypteringssystem. Den nya tekniken kallades för "Öppen-nyckel-kryptosystem" ("public key cryptography") och i Diffie-Hellmans arbete byggde på så kallade "diskreta logaritmer". Asymmetriska krypteringssystem eliminerar behovet av ett utbyte av krypterings- och dekrypteringsnycklar. På det sättet revolutionerade Diffie-Hellmans idé hela kryptologin. Den har fått en mycket stor betydelse för dagens kommunikationssystem som kräver hög säkerhetsnivå vid dataöverföring. Idén öppnade vägen för användning av kryptologin inte bara av militärer, spioner och diplomater utan av var och en av oss i olika

vardagliga sammanhang – när vi tar ut våra pengar från bankautomater, när vi loggar in på en dator eller betalar med våra kreditkort genom internet. Det intressanta är att Diffie-Hellmans idé snarare var teoretisk än praktisk när den publicerades. Två år senare kom tre matematiker Ron Rivest, Adi Shamir och Leonard Adleman med den första praktiska konstruktionen av ett öppet krypteringssystem som idag kallas för RSA-krypto. RSA-metoden publicerades år 1978 i ett kort arbete med titeln *A method for obtaining digital signatures and public-key cryptosystems* i Communications av the ACM.

Låt mig beskriva RSA-metoden och samtidigt förklara vad man menar med envägsfunktioner, diskreta logaritmer och ett asymmetriskt krypteringssystem. Utgångspunkten för Diffie-Hellmans metod var tanken på att krypteringssystem skall byggas så att det är mycket lätt att kryptera och mycket svårt att dekryptera. Det är rentav så att alla får veta hur man krypterar (känner till krypteringsnyckeln), men enbart den som skall ta emot meddelanden vet hur man dekrypterar (känner till dekrypteringsnyckeln). Dessa omständigheter gör att metoder av den typen kallas asymmetriska. Den regel som säger hur man krypterar kallas för en envägsfunktion därför att i praktiken måste det vara mycket svårt att rekonstruera den andra vägen – från den krypterade texten till klartexten.

Låt oss betrakta ett exempel. Vi betecknar meddelanden med 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. Vår krypteringsfunktion definieras så att man krypterar meddelandet x till resten av 7^x vid division med med 11. Detta innebär att

$$
\begin{aligned}
1 &\to 7\\
2 &\to 5\\
3 &\to 2\\
4 &\to 3\\
5 &\to 10\\
6 &\to 4\\
7 &\to 6\\
8 &\to 9\\
9 &\to 8\\
10 &\to 1
\end{aligned}
$$

dvs man krypterar 1 till 7 (därför att resten vid division av 7^1 med 11 är 7), 2 till 5 (därför att resten vid division av $7^2 = 49$ med 11 är 5) osv. Man kan säga att det är mycket lätt att kryptera, men det är mycket svårare att dekryptera: om vi t ex vet det krypterade meddelandet är 4. Vad är klartexten? Klartexten ”döljer sig” bakom x sådant att $7^x = 4$. Alltså måste vi lösa ekvationen $7^x = 4$. Det är inte helt banalt att beräkna x – även om det är inte svårt att göra det just i vårt exempel då vi helt enkelt kan testa $x = 1, 2, 3, 4, \ldots$ Vi ser att både 1, 2, 3, 4, 5 inte duger, men $7^6 = 7^2 \cdot 7^2 \cdot 7^2 = 5 \cdot 5 \cdot 5 = 25 \cdot 5 = 3 \cdot 5 = 15 = 4$ (observera att vi räknar med rester vid division med 11 så att t ex $7^2 = 49$ kan ersättas 5, och 25 med 3). Man kan säga att krypteringen är enkel, medan dekrypteringen är svår. Om man ersätter 11 med ett mycket stort tal blir uppgiften mycket svår. Talet x kallas just diskreta logaritmen av 4 (i bas 7 modulo 11). Namnet kommer från vanliga logaritmer i bas 10 som är lösningar till ekvationer $10^x =$ ett positivt tal.

RSA-krypto bygger på en liknande princip. En person som brukar kallas Alice, vilket förkortas till A, vill ta emot meddelanden. Hon väljer två stycken mycket stora primtal p och q (vanligen med c:a 150 siffror). Primtalen är

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, …

dvs positiva heltal som saknar delare större än 1 och mindre än talet självt. Alice räknar därefter $N = pq$ och väljer dessutom ett heltal e som inte delar $p - 1$ och $q - 1$. Hon publicerar N och e som är krypteringsnyckeln, men behåller hemligt både p och q. Hon publicerar också en ”ordbok” som säger att A skall översättas till t ex 10, B till 11, C till 12, osv. Alice måste också beräkna sin dekrypteringsnyckeln som hon behåller för sig själv. Denna nyckeln är ett tal d sådant att ed skall ge resten 1 vid division med både $p - 1$ och $q - 1$. Det är mycket lätt att beräkna d och flera datorprogram gör sådana beräkningar mycket snabbt.

Låt oss nu anta att en annan person, som vi kallar Bo och förkortar till *B*, vill skicka ett meddelande *x* till *A*. Bo räknar ut resten vid division av x^e med N och skickar till Alice.

Alice räknar då resten vid division av $(x^e)^d$ med N och får tillbaka meddelandet *x* dvs $(x^e)^d = x$.

En sats som visades av Pierre de Fermat under 1600-talet garanterar att $(x^e)^d = x$ dvs garanterar att Alice kan förvandla den krypterade texten i klartext. Volymen av denna artikel tillåter inte att jag ger ett bevis av denna enkla och mycket viktiga sats i elementär talteori.

Låt oss betrakta ett mycket konkret exempel.

- Alice väljer $p = 61$, $q = 101$ så $N = pq = 61 \cdot 101 = 6161$.
- Alice väljer t ex $e = 17$ som inte delar $p - 1 = 60$ och $q - 1 = 100$.
- Alice räknar ut *d* så att *ed* ger resten 1 vid division med $p - 1 = 60$ och $q - 1 = 100$. Hon kan välja $d = 353$ ty $ed = 17 \cdot 353 = 6001$ ger resten 1 vid dessa divisioner.
- Alice publicerar $N = 6161$; $e = 17$ (och en ”ordbok” t ex A = 10, B = 11, C = 12, D = 13, E = 14, ..., I = 18, ..., K = 20,..., M = 22, ..., T = 29,..., Z = 35). Primtalen *p*, *q* och *d* är hemliga.

Kryptera: MATEMATIK

MA = 2210 → $[2210^{17}]_{6161} = 4013$

TE = 2914 → $[2914^{17}]_{6161} = 135$

MA = 2210 → $[2210^{17}]_{6161} = 4013$

TI = 2918 → $[2918^{17}]_{6161} = 1527$

K = 20 → $[20^{17}]_{6161} = 4487$

Dekryptera: 4013 135 4013 1527 4487

4013 → $[4013^{353}]_{6161} = 2210 = \text{MA}$

135 → $[135^{353}]_{6161} = 2914 = \text{TE}$

4013 → $[4013^{353}]_{6161} = 2210 = \text{MA}$

1527 → $[1527^{353}]_{6161} = 2918 = \text{TI}$

2487 → $[4487^{353}]_{6161} = 20 = \text{K}$

Varför är RSA–metoden så effektiv att den används mycket flitigt i moderna kommunikationssystem? Svaret är att det är mycket svårt och idag inte möjligt att beräkna *d* då *N* och *e* är kända (om talen *p* och *q* är tillräckligt stora). Talet *ed* skall ge resten 1 vid division med både $p - 1$ och $q - 1$. Om man känner till dessa två tal är det mycket lätt att beräkna *d*. För att komma åt $p - 1$ och $q - 1$ måste man känna till *p* och *q*. Man utgår ifrån att dessa två tal endast kan beräknas om man kan uppdela talet $N = pq$ i dess primfaktorer *p* och *q*. Denna beräkning dvs uppdelning av *N* i primfaktorer är mycket komplicerad och tar mycket lång tid. De bästa kända metoderna kräver c:a $\sqrt[5]{N}$ räkneoperationer. Om t ex *p* och *q* har 100 siffror så har *N* c:a 200 siffror och antalet räkneoperationer som behövs för att faktoruppdela talet *N* är 10^{40}. Om man antar att en räkneoperation tar 1μs så krävs det 10^{40} μs $\approx 3 \cdot 10^{26}$ år för att genomföra beräkningarna för *N* (10^6 datorer var och en kapabel att utföra en räkneoperation på 1μs skulle behöva $3 \cdot 10^{20}$ år för dessa beräkningar). Trots det betraktas idag val av primtal med 100 siffror som inte helt säkra och man väljer snarare primtal med 150.

RSA-metoden kan användas för att skicka meddelanden från en godtycklig antal personer till en person (eller mellan godtycklig antal personer som annonserar sina krypterinngsnycklar). Detta system har mycket stora fördelar, men det har också en stor brist – eftersom Alice och Bo inte

har kontakt med varandra, kan Alice inte vara säker på att meddelandet hon har fått kommer just från Bo. Rent teoretiskt är det möjligt att någon annan, säg fienden *F* som uppger sig för Alice, skickar sin nyckel *e'* till Bo. Bo tror att detta är Alices nyckel och skickar sitt meddelande. Meddelandet läses av *F* (med hjälp av *F*:s dekrypteringsnyckeln *d'*) och skickas vidare till Alice genom att använda Alices korrekta nyckel *e*. Detta visar att systemet kräver äkthetsbevisning – Alice måste kunna vara övertygad om att meddelandet kom direkt från Bo. Det visar sig att även detta problem kan lösas med hjälp av RSA-tekniken i form av så kallade *digitala signaturer*.

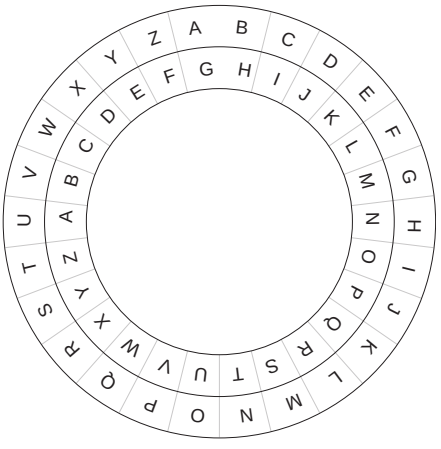
Vi har inte tillräckligt utrymme för att diskutera den tekniken noggrannare här, men den bygger på att varje part underskriver sina krypterade meddelanden med en lämplig signatur. Om t ex Bo skickar ett krypterat meddelande x så skickar han också sin signatur som är $S(x)^{d_b}$, där d_b betecknar Bos dekrypteringsnyckel. Signaturen $S(x)$ är ett sätt, känt för alla användare av systemet, att tilldela varje (krypterat) meddelande x ett tal (t ex en relativt kort följd av 0 och 1).

Nu är det så att värdet d_b endast är känt för Bo – det är hans hemliga dekrypteringsnyckel. Alice tar Bos offentliga krypteringsnyckel e_b och räknar ut $(S(x)^{d_b})^{e_b} = S(x)$. När Alice ser att hon verkligen får $S(x)$ så betyder det att enbart Bo kunde skicka det krypterade meddelandet x eftersom enbart han har tillgång till d_b och enbart han kunde beräkna $S(x)^{d_b}$. Konstruktionen av digitala signaturer som beror på meddelanden är också ett intressant matematiskt problem som har flera lösningar och som vi tyvärr inte kan diskutera närmare här. Funktioner S som tilldelar meddelanden talen $S(x)$ kallas vanligen "hash–funktioner". De måste uppfylla vissa specifika villkor för att kunna användas som signaturer.

Låt oss avsluta med ett exempel på en digital signatur (fast inte särskilt praktiskt). Vi antar, som i exemplet på RSA-kryptering, att $p = 61$; $q = 101$ (dvs $N = pq = 61 \cdot 101 = 6161$) och $e = 17$. Dekrypteringsnyckeln var $d = 353$. Nu är det artikelns författare som vill signera avslutningen av denna text.

Om vi accepterar Alices "ordbok" så är JB lika med 1911. Signaturen blir alltså $[1911^{353}]_{6161} = 5865$. Exponenten 353 är hemlig och min (tidigare Alices) krypteringsnyckel bestående av $e = 17$ och $N = 6161$ är allmänt känd så att alla kan identifiera mig som författaren om de räknar ut $[5865^{17}]_{6161}$. Försök som övning beräkna denna rest av 5865^{17} vid division med 6161 – en uppgift som man mycket enkelt kan lösa t ex med hjälp av en miniräknare. Ännu enklare är det med datorprogram t ex *Derive*, *Maple* eller *Mathematica*.

CAESARKRYPTO



VENI VIDI VICI
BKTO BOJO BOIO