Litteratursammanfattning

Historik[1]

Kryptering har i alla tider utnyttjats för att förhindra att någon annan än den avsedda mottagaren får reda på hemlig information i ett meddelande, från början främst under krigstid. Den tidigaste formen av kryptering var ofta väldigt enkel på grund av flera anledningar, dels på grund av avsaknaden av avancerad teknik, men också därför att de flesta människor inte kunde läsa. De vanligaste tidiga krypteringsalgoritmerna var därför olika varianter av förskjutnings- och omkastningschiffer. Den första bygger på att alfabete förskjuts ett antal steg åt något håll (dvs. om förskjutningen är 3, så blir A D, B, E osv.). Redan Julius Caesar använde sig av detta chiffer för att kunna kommunicera säkert.
Omkastningschiffret bygger istället på att bokstäverna kastas om enligt ett förutbestämt schema (ex. ”hej” blir ”ehj”).

Dessa metoder har uppenbara säkerhetsbrister, då de är lätta att avkyptera även utan att känna till nyckeln. Därför har man i mer moderna tider övergått till mycket mer avancerade algoritmer.

Kryptering idag[2]

Modern kryptologi delas upp i flera områden. De viktigaste är *symmetrisk kryptering och assymetrisk kryptering.* En annan metod att skydda ett lösenord eller dylikt är att använda en *hashmetod.*

Symmetrisk kryptering

Symmetrisk kryptering använder sig av samma nyckel vid kryptering och dekryptering. Det innebär att både sändare och mottagare måste ha tillgång till nyckeln. Eftersom nyckeln då måste finnas på flera ställen innebär det en säkerhetsrisk. Dessutom måste ett utbyte av nyckeln ske, vilket måste lösas på någon sätt. Ett annat problem med den symmetriska krypteringen är om en sändare önskar skicka ett meddelande till flera mottagare. All mottagare måste i så fall känna till nyckeln, vilket ökar risken för att den kommer i fel händer.

Den symmetriska metoden har dock även flera fördelar; den är snabbare än andra metoder, och kräver ofta mindre RAM-minne. Exempel på symmetrisk kryptering är AES och DES.

Assymetrisk kryptering

Till skillnad från symmetrisk-kryptering använder assymetrisk-kryptering olika nycklar för krypterings- och dekrypteringsalgoritmen. Assymetrisk kryptering bygger på att två olika nycklar används, en öppen nyckel, som alla känner till, och en privat nyckel. Den privata nyckeln är hemlig för alla förutom för den som nyckeln tillhör. Algoritmerna fungerar så att den som vill skicka ett meddelande till A krypterar ett meddelande med A:s öppna nyckel. Meddelande kan då bara dekrypteras med hjälp av A:s privata nyckel. Fördelen med assymetrisk kryptering är att inga hemliga nycklar behöver utbytas mellan parter och att den privata nyckeln bara är känd av en person. Nackdelen är dock att den ofta är långsammare än vad den symmetriska krypteringen är. Exempel på assymetrisk kryptering är RSA.

Hashning

1 Källa: Wikipedia: Kryptering
2 Källor: Wikipedia: Cryptography och Wikipedia: Kryptering

Hashning kan egentligen inte riktigt kallas för kryptering, men bör ändå nämnas. Hashning går ut på att man ur en godtyckligt stor datamängd genererar en förhållandevis kort kontrollsumma. En annan viktig egenskap hos hashfunktionen är att man från två skilda meddelanden aldrig får samma kontrollsumma. Det går inte heller att från en kontrollsumma få tillbaka det ursprungliga meddelandet. Hashning används ofta för säker lagring av lösenord. Man jämför då hashen av det inmatade lösenordet med den i databasen lagrade hashen. Om de matchar har användaren matat in det korrekta lösenordet. Exempel på hashfunktion är md5.

Olika krypteringsalgoritmer

DES[3]
Data Encryption Standard (DES) är en symmetrisk krypteringsalgoritm som tar en 64 bitars lång sträng och genom upprepade komplicerade operationer omvandlar den till en annan 64-bitars sträng. DES anses nu för tiden vara relativt osäkert.

3DES[4]
3DES är precis som det låter en implementering av DES där man krypterar meddelandet tre gånger på varandra med DES. Denna metod anses till skillnad från DES vara säker.

AES[5]
Advanced Encryption Standard (AES) är även den symmetrisk. AES är ett substitutions-permutationskrypto (en metod som går ut på att blockvis substituera och permutera om vart annat) som genom flera rundor med substituering och permutering av texten gör den oläslig utan att avkryptera den. AES kan användas med varierande nyckellängd, 128, 192 och 256 bit. Beroende på nyckellängden varierar även antalet rundor. Varje runda består av fyra steg; byte substitution, radskiftning, matrismultiplikation och slutligen nyckeladdition.

AES är egentligen inte fullständigt symmetrisk, eftersom den inte använder exakt samma algoritm för att kryptera som för att dekryptera.

RSA[6]
RSA är en assymetrisk krypteringsalgoritm, som använder modulär aritmetik. RSA använder två väldigt stora primtal för att generera de båda nycklarna som behövs (den öppna och privata). Metoden bygger på det faktum att det inte finns någon effektiv metod för primtalsfaktorisering. Med hjälp av den öppna nyckeln får man fram ett tal, som det bara går att få tillbaka det ursprungliga om man känner till den privata (i teorin går det även att räkna fram den, men detta tar oöverskådligt lång tid).

Metoder för att osäkra kommunikationen

Brute force
Den mest triviala, men ofta mest krävande metoden för att knäcka en kod. Brute force går helt enkelt till så att man testar alla möjliga lösningar tills man hittar den rätta. Detta fungerar för enkla algoritmer, men tar oöverskådligt lång tid för mer avancerade kryperingar.

Man-in-the-Middle attack[7]

3 Källa: Wikipedia: Data Encryption Standard
4 Källa: Wikipedia: Data Encryption Standard
5 Källa: Wikipedia: Advanced Encryption Standard
6 Källa: Wikipedia: Kryptering
7 Källa: Wikipedia: Man-in-the-middle attack

En Man-in-the-Middle (MitM) attack går till så att de kommunicerande parterna luras att tro att de kommunicerar med varandra, men i själva verket går trafiken via en tredje part som lyssnar av trafiken. För att detta sak fungera måste nyckelutbytet ske i början av kommunikationen. De båda parterna tror då att de byter nyckel med varandra, men byter egenligen nyckel med den tredje personen i mitten.

Referenslista

1. *Wikipedia: Kryptering:*
   http://sv.wikipedia.org/wiki/Kryptering (2008-10-10)

2. *Wikipedia: Cryptography*
   http://en.wikipedia.org/wiki/Cryptography (2008-10-10)

3. *Wikipedia: Data Encryption Standard*
   http://en.wikipedia.org/wiki/Data_Encryption_Standard *(2008-10-10)*

4. *Se källa 3*

5. *Wikipedia: Advanced Encryption Standard*
   http://en.wikipedia.org/wiki/Data_Encryption_Standard *(2008-10-10)*

6. *Se källa 1*

7. *Wikipedia: Man-in-the-Middle attack*
   http://en.wikipedia.org/wiki/Man_in_the_middle *(2008-10-10)*