Simetrični algoritmi

Delimo jih na dve skupini:

tekoče šifriranje - sporočilo šifriramo bit za bitom (stream ciphers);
sporočilo razbijemo na bloke in vsak blok posebej šifriramo (block ciphers)..

Pri prvem načinu šifriramo tako, da kombiniramo bit ključa in bit sporočila (običajno je to kar XOR). Če uporabimo kratek, ponavljajoč ključ, postopek ni varen - s kombiniranjem zašifriranega teksta je razmeroma lahko ugotoviti najprej dolžino ključa, potem vrednost ključa in dešifrirati sporočilo. Nasprotno pa je ta sistem nezlomljiv, če se ključ ne ponavlja in je povsem naključen niz bitov (one-time pad).

Večina algoritmov, ki jih danes uporabljamo v civilnih organizacijah, je blokovnih: sporočilo razbijemo na tako dolge bloke, kot zahteva algoritem, in vsak blok preoblikujemo in kombiniramo s ključem. Permutacije, substitucije in kombinacije s ključem (glej n.pr.opis DES-a) morajo zagotoviti, da so v izhodnem bloku zabrisani vsi vzorci iz vhodnega bloka - skratka, da izgleda kot naključen niz bitov.
Za vse simetrične algoritme je pogoj, da so dobri, če se izhoda ne da kompresirati za več kot nekaj odstotkov.

Pri blokovnih algoritmih je pomembno tudi povezovanje blokov pri šifriranju. Če šifriramo vsak blok posebej (to imenujemo način ECB - Electronic Code Book), potem se enak blok preslika v enak šifriran blok, kar pa kriptoanalitikom olajša dešifriranje. Veliko bolj varni so naslednji trije načini:

CBC (Cipher Block Chaining): Začetni blok teksta seštejemo z XOR z naključnim številom, ki mu rečemo inicializacijski vektor in ga postavimo na začetek šifriranega teksta. Vsak naslednji blok teksta seštejemo s šifriranim prejšnjim blokom in to potem zašifriramo.
CFB (Cipher Feedback, včasih mu pravijo tudi CTAK - ciphertext auto key): Inicializacijski vektor zašifriramo s ključem in rezultat seštejemo s prvim blokom teksta in tako dobimo prvi šifrirani blok. To vsoto zašifriramo s ključem in tako dobimo začasni ključ.
Temu prištejemo drugi blok teksta ... Vidimo, da pri tem načinu s šifriranjem pravzaprav spreminjamo ključ.
OFB (Output Feedback) je podoben prejšnjemu načinu: Inicializacijski vektor zašifriramo s ključem. Ta rezultat (recimo mu R1) z

XOR seštejemo s prvim blokom teksta in to je prvi šifrirani blok teksta. Potem dobimo ključ za šifriranje naslednjega bloka tako,
da R1 zašifriramo s prvotnim ključem... Od prejšnjega načina se razlikuje v tem, da začasni ključ tvorimo s šifriranjem
predhodnega ključa, ni odvisen od teksta.

Kdaj je algoritem varen? Napad s preizkušanjem vseh možnih kombinacij bitov ključa (brute-force attack) je za kriptoanalitika najslabša
možnost. Poznajo tudi druge, hitrejše metode. Zato je bistveno, da je algoritem javno objavljen in da so ga imeli možnost preizkusiti
vodilni kriptoanalitiki.

Pomembno pa je tudi, kako je algoritem implementiran:

implementiran neokrnjen algoritem;
uporaba načina, ki povezuje bloke (CBC, CFB ali OFB);
testiranje in izločitev šibkih ključev pri nekaterih algoritmih (n.pr. same ničle ali enice);
generiranje ključev s pravimi generatorji naključnih števil;
primerno dolg ključ (po podatkih iz leta 1997 vsaj 70 bitov).

Najbolj znani simetrični algoritmi so:

DES (Data Encryption Standard) ali DEA (Data Encryption Algorithm), ki sta ga razvila NIST (National Institute of Standards and
Technology) ter IBM.

RC2, RC4, RC5 - je razvil Ronald Rivest. RC2 je vgrajen v mail. Dopušča ključe dolžine 1 do 2048 bitov. V softveru, ki ga
prodajajo izven ZDA, običajno omejijo ključ na 40 bitov dolžine, kar seveda pomeni manjšo varnost. RC4 je tekoč šifrirni
algoritem z variabilno dolžino ključa do 2048 bitov. Vgrajen je v Netscapeov brkljalnik kot del protokola SSL. Ameriška verzija
uporablja 128-bitni ključ, neameriška pa 40-bitnega.

RC5 je bil objavljen 1994. Uporabnik lahko določi dolžino ključa, velikost bloka in število ponovitev šifrirnega postopka.

IDEA (International Data Encryption Algorithm): razvila sta ga James L.Massey in Xuejia Lai v Zuerichu in objavila 1990.
Uporablja 128 bitov dolg ključ na 64 bitov dolgih blokih. Patent zanj ima Ascom-Tech iz Švice. Izven ZDA lahko ga uporabljamo

brez plačila licenčnine. Če DES uporabljamo s trojnim ključem, je počasnejši od IDEE.

Skipjack: algoritem, ki ga je razvila NSA (National Security Agency), je zaščiten. Uporabljen je v šifrirnem čipu Clipper. Ključ je
80-biten. Vsak čip ima svoj ključ, katerega polovici sta shranjeni v različnih agencijah (key escrow agency).

Ameriška organizacija za standarde NIST (National Institute of Standards and Technology) je septembra 1997 razpisala natečaj za
naslednika algoritma DES, ki naj bi bil močnejši in hitrejši od trojnega DES. Postopek za izbiro "algoritma za 21. stoletje" Advanced
Encryption Standard (AES) še ni zaključen, izbirajo med 15 kandidati.

URL: http://www.sigov.si/tecaj/kripto/kr-sim.htm