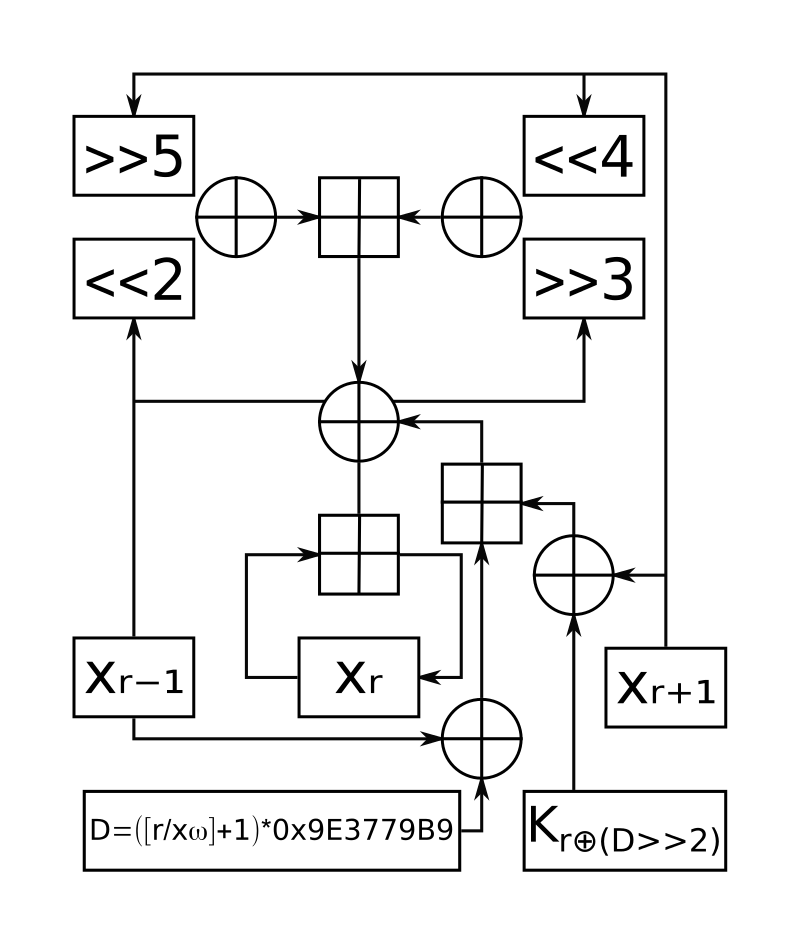
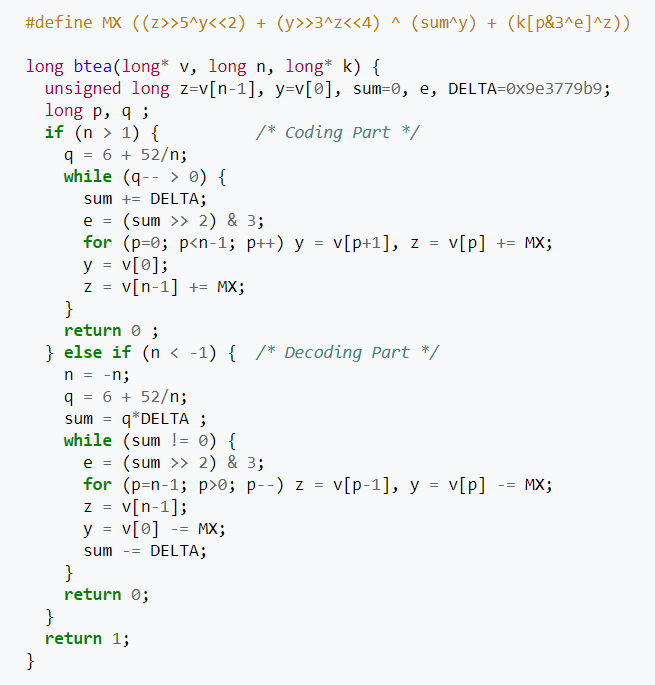
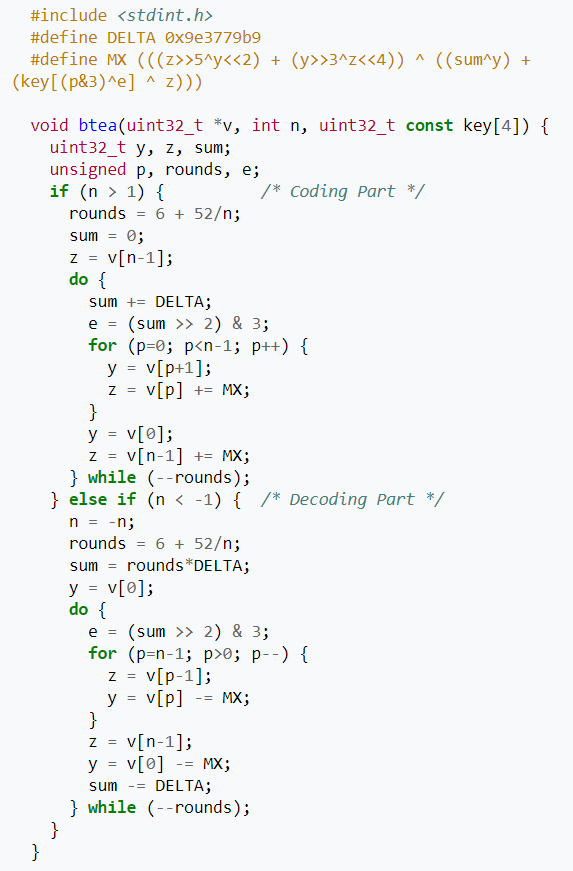
**XXTEA Algoritam**

* **XXTEA** ili **Corrected Block TEA** je kripto algoritam koji je dizajniran da ispravi nedostatke njegovog prethodniha **XTEA** (Block TEA) algoritma. Algoritam su predstavili dva profesora sa Cambrige Univerziteta – Roger Needham i David Wheeler oktobra 1998 godine.
* **XXTEA** algoritam radi sa blokovima koji mogu biti proizvoljne veličine, ali moraju da budu umnožak 32, tako da je najmanji blok veličine dve reči odnosno 64b. Broj rundi XXTEA algoritma zavisi od velicine bloka, ali je najmanji broj rundi šest a najveći trideset dve (za male veličine blokova). XXTEA za razliku od svojih prethodnika koji koriste samo levog suseda, koristi oba neposredna suseda kako bi procesirali svaku reč u bloku.
* Needham i Wheeler su objasnili koji su nedostaci XTEA – ako se promeni jedan bit to dovodi do promene više od polovine bitova bloka uz to da se ne zna gde su promene počele, ne postoji izbor moda, broj poruka treba uvek da se proverava jer je ova redundansa ustvari provera protiv prihvatanja random poruka, velike poruke moraju da se dele na delove od prilike šesdeset reči i da budu poveze kako bi mogle da se koriste.



Slika 1. Jedna runda XXTEA algoritma

* Ipak 2010 E. Yarrkov novinar koji se bavi kripto napadima je objavio **CPA – Chosen-plaintext attack** model kriptoanalize kojim se pretpostavlja da napadač može da dobije kriptovan podatak za bilokoji proizvoljan plaintext. Cilj napada je sticanje informacija koje smanjuju sigurnost kripto šeme. Yarrkov je napravio ovakav napad na jednu rundu XXTEA algoritma i bilo je potrebno 259 upita za blok veličine 212 bajtova ili više.
* Postoje dve verzije koda XXTEA algoritma: originalna verzija I unapredjena verzija.

****

Slika 2. Originalan XXTEA kod

Slika 3. Unapredjen XXTEA kod