

# «Ýíeãíà» á ííái ñíííeíáíeè

Àeñéíáúe øeððàòíð Á«ÝíeãíàÁ» íøeè-ààò íðíñòíðà eííñððóeèe, áùñíeáý íáä, æííñòù ðàáíòù è íøeè-íáý ñòíeéíñòù øðeðòà. Íá íeðíáíe áíeíú. Íí eííñððóeèe Á«ÝíeãíàÁ» eèáññeðeøeðòáòñý eàe àeñéíáúe øeððàòíð, íñíááííñòùp eíòíðúø ýáeyáòñý íáeè-eà eñííeüçíáàeè øðe ñòáíeáííúð íáæáò ñíáíe øeððíáàeüíúð àeñéà, ñíááððááøeð á íðíðáññá ðàáíòù ðááóeyðííá áàeæáíeá, ííáíáí ñ ðàáíòù íáä ñíááððáíñòáíáíeáí Á«ÝíeãíàÁ» íá íðáeðàùàeèñù íe íá íeíóó. Ðáçóeüðàòíí òàeíáí òðóáà ñòáeí øeððíáàeüííá óñððíe Ñòíeéíñòù òàeíáí øeððà íeàçàeáñù íá íí çóáàí áàæá íáðáùí á íeðá ýeáeððííúí áù-eñèeðáeyí Colossus, ííñòðíáííúí á Áíáeèe Á. Ç ííáíáíúá áóíáæe øðáíýðñý ííá áðeðíí Á«Ñíááððáííí ñáeðáòííÁ» eèáí áúeè óíe-òíæáíú íáíòáíe áù, áí eáíeøóeyøeè Ááðíáíeè. Íí ðáç ñeíáíeíá áeðááeðà óáíáíáá ñ-eðàòù ðàáííúí 256, íí -eñeó ðáçeè-íúð çíá-áíeé áàeòà. xèñeí àeñéíá íáíçíá-eí eáe n=11. Èæáíí Tab[j]=Tab[i][j], j=0..255, i=0..n-1 -eñáe 0..255, ñeèááíáý á eíeüí. Íóñòù ííeíæáíeá òáeóúááí íá-àeà eáæáíe òáeèeòù íðáááey i=0..n-1. Ñ ó-àòíí óeàçáííúð íáíçíá-áíeé øáà çàøeððíáàeíeý ñeíáíeá ì áey Á«ÝíeãíàÁ» ñ ðááóeyðííúí áàeæáíeáí øeððíáàeüíúð áù-eñeýáí n ðáç: Á Á Á a.Á Á Á Á Á Á M = Tab[i, M]; Á Á Á b.Á Á Á Á Á Á i = i + 1; Á Á Á c.Á Á Á Á Á Á Éííáö øeèeà i; 3.Á Á Á Á Á Á a.Á Á Á Á Á Á Á Ptr[i] = (Ptr[i]+k) mod256; Á Á Á b.Á Á Á Á Á Á Á Ñèe k=0, óííáeí íá 4.e.; Á Á Á c.Á Á Á Á Á Á Á Ñèe Ptr[i]. e.Á Á Á Á Á Á Á i=i+1; Á Á Á f.Á Á Á Á Á Á Á Éííáö øeèeà i. Óàíðe-áñeè áàeæáíeá øeððíáàeüíúð àeñéíá ííááeèðóáòñý ñeááòpù a.Á Á Á Á Á Á Á M = Tab[i, M]; b.Á Á Á Á Á Á Á i = i + 1; c.Á Á Á Á Á Á Á Éííáö øeèeà i; 3.Á Á Á Á Á Á Íóñòù k=1; 4.Á Á Á Á Á Á Á øeèe (Ptr[i]\*i+1) mod256; b.Á Á Á Á Á Á Á i=i+1; c.Á Á Á Á Á Á Á Éííáö øeèeà i. Áñý íáðááóeyðííñòù çááñù ííááeèðóáòñý ñòðíeíe 4.á, ñeíáíeá. Íáíáeí ýòí íá íðeíáñ, ò íðáeðe-áñeè íeèeáeè ðáeíóúáñòá. Íáðáòeííñòù ííeñáííúð øeððópuèø íðáíáðáçíáíeé íá áùçúáá íðíðeáíííeíæíúe è çáíáíá òáeèe eíááðñíúíe èí InvTab[i], i=0..n-1 ñ eñííeüçíáíeáí ñííóíøáíeý InvTab[i, Tab[i, j]] = j, j=0..255, i=0..n-1. Ç óí íðíðáñ çàøeððíáàeíeý ííæíí ííñòðíeòù è íá óíðááeáíeè íðýáeíí íðíðíæááíeý ñeíáíeíá -áðáç ñeñòáíó òáeèeò. Íðáááá, ííá ñííðáá eç ðáññííòðáííúð ðáíáá. Íí áàeàòù ýòíáí íù íá áóááí, á íðíñòí ñeáæáí, -òí Á«ÝíeãíàÁ» ííáíáíe eííñððóeèe ííæáò áúòù ðááeèçíá 1 è óeàçàðáeáe Ptr[i], i=0..n-1 è íeí. Á ýòíí ñeó-áá íðeíáíáí áeáíðeòí, -áñòe-íí íçáeíñòáíáííúe eç ííeñáíeý øeððà RC4 Ðííá Ðeá Tab[0, i]=i, i=0..255. Çàòáí áá ýeáíáíòù íáðáñòááeyáí á ñííðááòñòáeè ñí çíá-áíeáí eèp-à, øeèeèe-áñeè ííáòíðýý íí íáðá íáíáðíáeíí íðíðáñ ðáíáííeçàòeè òáeèeòù Tab[0], íñóúáñòáeyáíúe ñeááòpùèí íáðáçíí. 1.Á Á Á Á Á Á Íóñòù i=0; 2.Á Á Á Á Á Á Á øeèeà ñí ñ Tab[0, Tab[0, i]] mod256; b.Á Á Á Á Á Á Á íáíýáí íáñòáíe ýeáíáíòù Tab[0, i] è Tab[0, j]; c.Á Á Á Á Á Á Á i = i + 1; d.Á Á Á Á Á Á Á Éííáö øe Tab[j], i=1..n ííeó-áàòñý íðeíáíeáí ííeñáííe íðíðááòðú è íðááúáóúáe òáeèeòà. Íá-àeüíúá çíá-áíeý óeàçàðáeáe Ptr[i], i=0..n-1 á ñ-eàò-eèíí í áù-eñeýáí n ðáç: Á Á Á a.Á Á Á Á Á Á Á Ptr[i] = (Tab[i, 0] + Tab[i, Tab[i, 0]]) mod256 èèe Ptr[i] = Á Á Á = (Tab[i, 0] + mod n; Á Á Á b.Á Á Á Á Á Á Á i = i + 1; Á Á Á c.Á Á Á Á Á Á Á Éííáö øeèeà i. Çááñù çà íáeíáíeáí eó-øááí ííýòù-òáeèe eñííeüçíáíú ííñòíýíñòáí ðáñíáeèe eííòáeðíá Á«ÝíeãíàÁ» áeá-àò ðááóeyðíóð á eèáññe-áñeèe eèe íáðááóeyðíóð á óñíááððáíñòáíáííúð íáðá øeððò RC4. Íðáááá, ííñeááíáá ñííðááòñòáóò ðááeüíí íáíñòúáñòáeííe íáðáðáñíáeèe àeñéíá Á«ÝíeãíàÁ» íáíñòááñòááííí á óíáá