N E W S
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 2, Number 318 (2018), 31 – 36

UDC 004.056.5

A.A. Zhatkanbayev

Al-FarabiKazakhNationalUniversity, Almaty, the Republic of Kazakhstan
wildlife.kz@gmail.com

APPLIANCE OF FLOYD WARSHALL, BELLMAN-FORD ALGORITHMS FOR ADDING NOISE PERMUTATIONS OF BLOCK CIPHERS FOR CRYPTOGRAPHIC ENDURANCE ENHANCEMENT

Abstract. The article describesthe procedures of information encryption and permutations, which would be used during development of information concealing (closure and concealing) system. Process of permutation is based on output sequences of shortest paths of graph algorithms of Bellman-Ford and Floyd Warshall. Creation of this system of information concealing and it's program implementation is aim of master degree project.

Key words: cryptography, permutation, Floyd Warshall algorithm, Bellman-Ford algorithm, cryptographic endurance.

Introduction.Proposed technology is concluded in that graph algorithms for finding shortest path Floyd Warshall, Bellman-Ford used only for finding shortest paths between two vertexes in graph.Combinationofcryptographyandoutputsequenceofshortestpathprovidessecrecyof information. Ifencryptedinformation (ciphertext) writtenin EC Bencryptionmodethanbyanalyzingtens of thousandsciphertexts it is possible to issue adecision that for example as encryption algorithm was used theparticularcryptographic cipher.SuchvulnerabilitieswerefoundinsymmetricalgorithmsDES, FEAL-N, in case if therewere used a pair weak key and weak plaintext was contained many repeated bytes which finally led to the situation that ciphertext contained many repeated bytes or not fully whitened at all. Thiswouldallowto3rdnonauthorizedpartymakean assumption of plaintext content character.In connection with that a technology was developed which allows on thebasis of thebuilt graph in representation of adjacency matrix to find shortest paths with usage of Floyd-Warshall, Bellman-Ford algorithms.Usageofadditionalpermutationofshortestpaths output sequences of Floyd-Warshall, Bellman Ford algorithms allows to protectciphertexts from differential cryptanalysis.This is explained by that after permutation ciphertext would be significantly differ from plaintext and even by using decryption key it would be not possible to obtain theoriginal plaintext.

Symmetrical block cipher encryption algorithmTwofish with key dependable substitution S-blocks. Symmetric block cipher Twofish with key dependable substitution S-blocks are of the most complicated for program implementation and most cryptographic endurable cipher in view of usage of Galois Fields ($GF\ 2^8$) [1,2]. Twofish was created by Bruce Schneier in 1998 year and following cipher had all set of technologies which science of cryptography reached specifically: Feistel Network, usage of irreducible polynomials of 8th degree in Galois Fields, unary operations: XOR, ROL, ROR, addition by modulus 32 (providing one-sidedness, concluding in complexity of retrieval square root by modulus, and also high speed on computer), entrance and output whitening, key dependable S-blocks, Hadamar cryptographic transform.

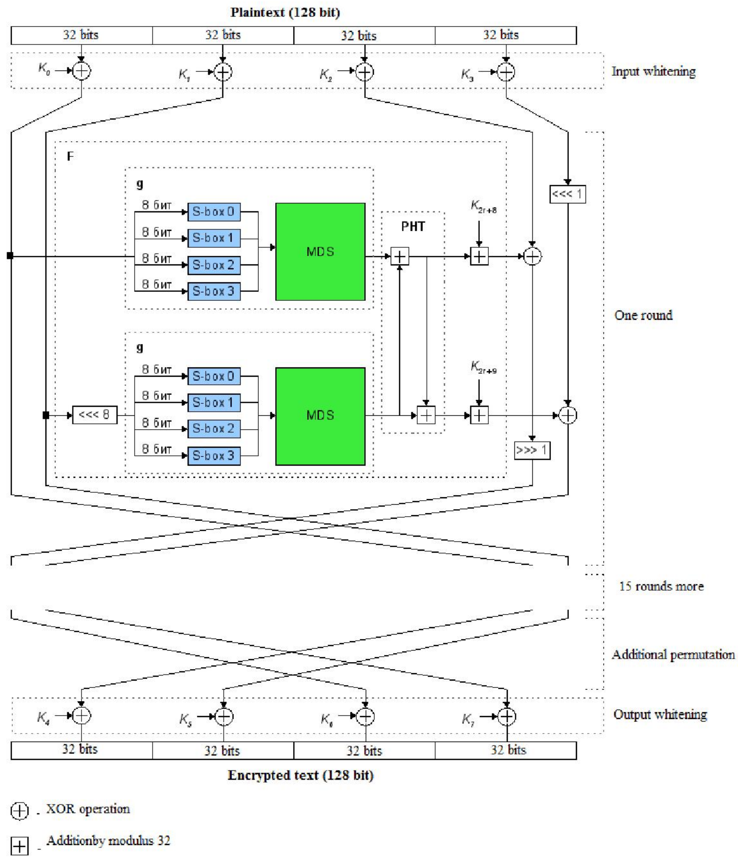

Figure 1 - Scheme of Twofish-128 algorithm

Describing the process of forming round keys:

M-encryption key, N-length of key in bits. Encryptionkey$M$breaking on8 $*$ $k$bytes$m_{0,\ldots\ldots\ldots,}m_{8k-1}$, $k = N/64$

Thenfollowing8 $*$ $k$bytesbreaksupon 32 bitswords (DWORD) (for4 bytes), it should be taken into account that in each words bytes are written in reverse order. Finally it is 2 $*$ k 32 bits wordsM_i

$$M_i = \sum_{j=0}^{3} m_{(4i+j)*2^{8j}\ i=0,\ldots,2k-1}$$

Following2 $*$ k 32 bitswordsdividing on two vectors$M_e$and$M_o$of size in$k$ 32 bits word each

$$M_e = (M_0, M_2, \ldots, M_{2k-2})$$

$$M_o = (M_1, M_3, \ldots, M_{2k-1})$$

Finalroundsubkeysfor 16 rounds calculating by following rule, where$i$equals toround key of i round:

$$\rho = 2^{24} + 2^{16} + 2^{8} + 2^{0}$$

$$A_i = h(2ip, M_e)$$

$$B_i = ROL(h((2i+1)\rho, M_0), 8)$$

$$K_{2i} = (A_i + B_i)\ mod\ 2^{32}$$

$$K_{2i+1} = ROL((A_i + 2B_i)\ mod\ 2^{32}, 9)$$

Functionhfor encryption rounds and generation of key dependableS-blocks

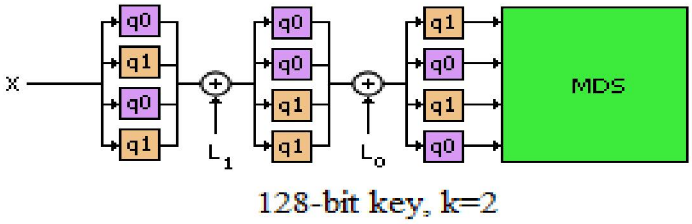

Figure 2 - Function h of Twofish-128 algorithm

$$\begin{matrix} 01 & EF & 5B & 5B \\ 5B & EF & EF & 01 \\ EF & 5B & 01 & EF \\ EF & 01 & EF & 5B \end{matrix}$$

Figure 3 - MDS matrix

MultiplicationinMDSmatrixproceeds byirreducible polynomial of 8th degree$x^8 + x^6 + x^5 + x^3 + 1$
q_0, q_1– fixed permutation blocks of 8 bits of incoming byte x.

Bytexsubstitutesontwopartsby 4 bitsineachpart (a_0, b_0), on following values$a_0, b_0$are heldnext calculations:

$$a_0 = x/16 b_0 = x mod\ 16$$

$a_1 = a_0 \oplus b_0 b_1 = a_0 \oplus ROR_4 = (b_0, 1) \oplus 8a_0 mod\ 16$
$a_2 = t_0[a_1] b_2 = t_1[b_1]$
$a_3 = a_2 \oplus b_2 b_3 = a_2 \oplus ROR_4 = (b_2, 1) \oplus 8a_2 mod\ 16$

$$a_4 = t_2[a_3] b_4 = t_3[b_3]$$

$y\quad = 16b_4 + a_4$

Below presented fixed values if tables$t_0 \ldots t_3$, forq_0, q_1

Tables for q_0:

t_0=[8 1 7 D 6 F 3 2 0 B 5 9 ECA 4]
t_1=[E C B 8 1 2 3 5 F 4 A 6 7 0 9 D]
t_2=[B A 5 E 6 D 9 0 C 8 F 3 2 4 7 1]
t_3=[D 7 F 4 1 2 6 E 9 B 3 0 8 5 CA]

Tables for q_1:

t_0=[2 8 B D F 7 6 E 3 1 9 4 0 A C 5]
t_1=[1 E 2 B 4 C 3 7 6 D A 5 F 9 0 8]
t_2=[4 C 7 5 1 6 9 A 0 E D 8 2 B 3 F]
t_3=[B 9 5 1 C 3 D E 6 4 7 F 2 0 8 A]

Function G:

Function$g$calculated via function$h$: $g(X) = h(X, S)$

$$\begin{matrix} 01 & A4 & 55 & 87 & 5A & 58 & DB & 9E \\ A4 & 56 & 82 & F3 & 1E & C6 & 68 & E5 \\ 02 & A1 & FC & C1 & 47 & AE & 3D & 19 \\ A4 & 55 & 87 & 5A & 58 & DB & 9E & 03 \end{matrix}$$

Figure 4 - RS Matrix

MultiplicationinRSmatrixconducted by irreducible polynomial of 8th degree$x^8 + x^6 + x^3 + x^2 + 1$

Bellman-Ford algorithm for finding the shortest path. The algorithm for finding the shortest paths of Bellman-Ford is based on the operation of edge relaxation. Initially, the algorithm is not applicable to graphs having a negative cycle, since it is possible to improve the distances for two vertexes in such graph indefinitely.Describing the pseudo-code procedure for finding the shortest path in the graph by the Bellman-Ford algorithm:

Table 1 - Pseudocode of Bellman-Ford algorithm

```
FunctionBellmanFord{
//Setting initial distances to all vertexes V equals to infinity, also for all ancestors of each vertexes setting zero value
For(inti=1;i<=V;i+=1){
d[i]=inf;
p[i]=0;}
d[s]=0; //Setting the initial value of 0 from source

//Traversing of all vertexes
For(inti=1;i<=V-1;i+=1){
//For each outgoing edge from vertex checking
For each Edge e in Edges(G){
//if thedistance between two vertexes a,balong certain edge c is less than current. This means that we are using edge c already having thecurrent edge of theshortest path between a,b + a certain edge c,than path could be improved.

If(distance[e.from]+lengthof(e)< distance[e.to]){
distance[e.to]=distance[e.from]+lengthof(e);
p[e.to]=e.from; //Writing to array of ancestors newly found vertex
}}}}
```

Floyd-Warshall algorithm for finding the shortest path. Floyd Warshall's algorithm also solves the problem of finding the shortest path between two vertexes in a graph. The algorithm concludes in taking vertex andit's outgoing edges one at a time and look through along which edges it is possible to improve the distance, this will be the intermediate edges.

Table 2 - Pseudocode of Floyd-Warshall algorithm

```
FunctionFloyd-Warshall{
d[uv]=w//Initial weights of graph edges are setting
For(inti=1;i<V;i+=1){ //Traversing of all graph vertexes
For(intu=1;u<V;u+=1){//Traversing of all graph edges
For(int v=1;v<V;v+=1){
d[uv]=min(d[uv-1],d[ui-1]+d[iv-1])//If distance could be improved by addition of intermediate vertex (edge) than writing following vertex(edge)
}}}}
```

Results of implementation in programming environment Microsoft Visual Studio 2013 on high level programming language C#

Demonstration of programming implementation of Twofish

Key-0X9F589F5C, 0XF6122C32, 0XB6BFEC2F, 0X2AE8C35A
Plaintext-0X16DB91D4, 0X9EC3B1E7, 0X6B08CB86, 0X19549F78

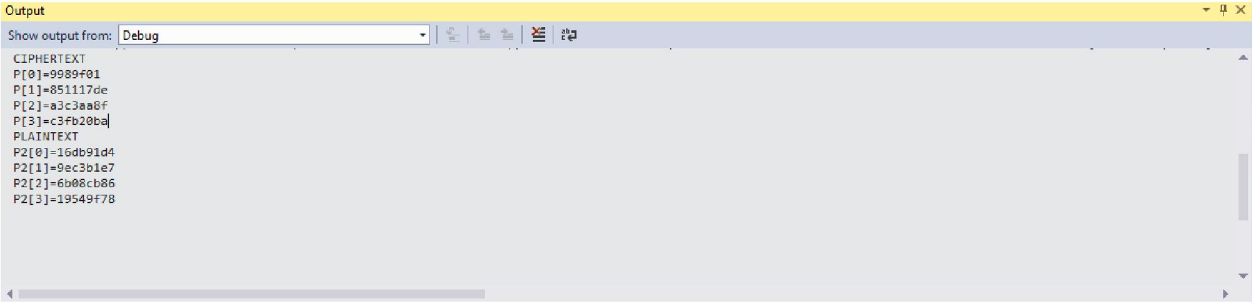

Figure 5 - Program implementation of Twofish

Demonstration of programming implementation of Floyd Warshall algorithm

Table 3 - Presented graph with 6 vertexes for Floyd Warshall and Bellman Ford algorithms

{0,10,18,8,inf,inf}, {10,0,16,9,21,inf}, {inf,16,0,inf,inf,15}, {7,9,inf,0,inf,12}, {inf,inf,inf,inf,0,23}, {inf,inf,15,inf,23,0}

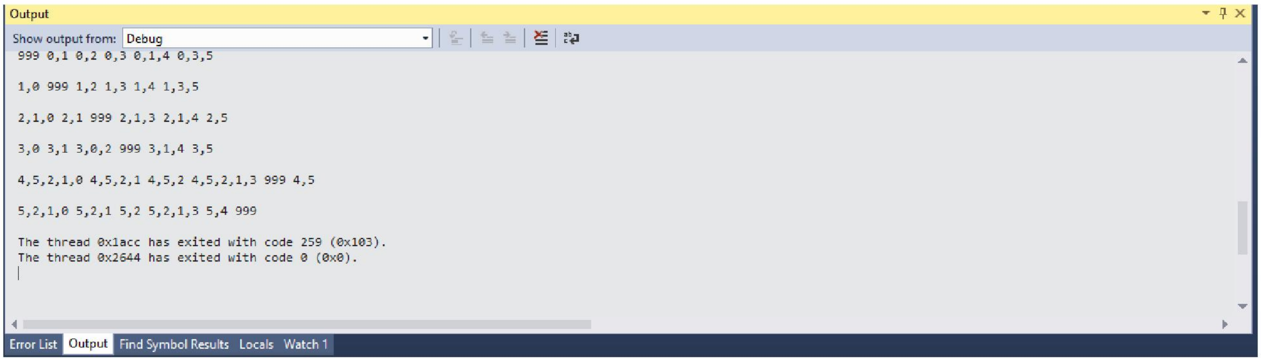

Figure 6 - Program implementation of Floyd Warshallalgorithm (shortest paths)

Demonstration of programming implementation of Bellman-Ford algorithm

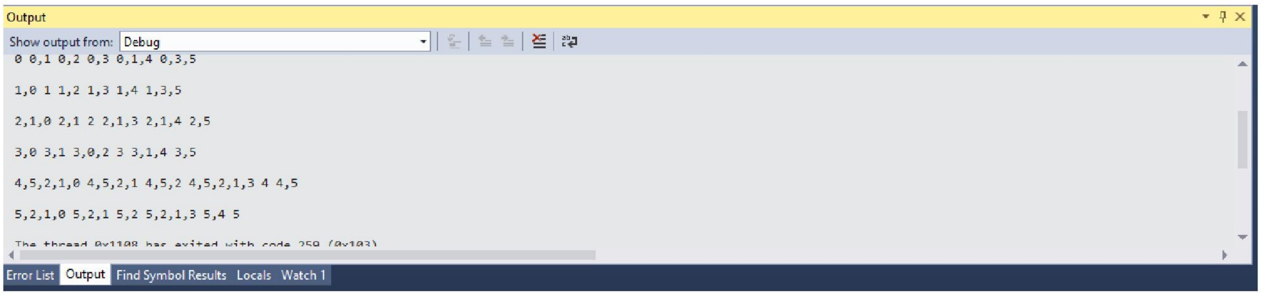

Figure 7 - Program implementation of Bellman-Ford algorithm (shortest paths)