https://doi.org/10.26552/com.C.1999.3.29-34

Mária Franeková - Peter Nagy *

ŠIFROVACÍ SYSTÉM ZALOŽENÝ NA TECHNIKÁCH KOREKČNÝCH KÓDOV

CIPHERING SYSTEMS BASED ON THE ERROR-CORRECTING CODING TECHNIQUES

Článok poukazuje na možnosť použitia šifrovacieho algoritmu s použitím štandardných kódovacích techník z množiny lineárnych samoopravných kódov. Kvalita dešifrovacieho algoritmu je určená pre Hammingove (n, k) kódy. Zároveň je stanovené pre aké dimenzie Hammingových (n, k) kódov je uvedený algoritmus prakticky použiteľný. Uvedený princíp sa dá zovšeobecniť aj pre iné typy samoopravných kódov.

1 ÚVOD

Komunikačný systém, ako subsystém informačného systému, predstavuje potenciálny cieľ aktívnych a pasívnych útokov na informácie prenášané medzi jednotlivými časťami informačných systémov. Otázka zaistenia bezpečnosti prenášaných informácií je zvlášť významná vo verejných sieťach, ktoré sú v tomto smere považované za nedôveryhodné. Ochrana dát počas prenosu je preto veľmi dôležitým problémom, ktorým sa treba zaoberať.

Bezpečné služby podľa amerického štandardu „Trusted Network Interpretation“ sú klasifikované do troch skupín [5]:

- komunikačná integrita,
- odmietnutie služby,
- ochrana dát pred únikom.

Pracovná verzia pripravovaného telekomunikačného zákona pre Slovenské telekomunikácie sa tiež zaoberá problematikou ochrany informácií, sietí a prostredia (časť IV, § 26 „Systém zvýšenej miery utajenia a ochrany prenášanej informácie“). Cieľom novej telekomunikačnej legislatívy na Slovensku je dosiahnuť úroveň telekomunikačných služieb poskytovaných štátmi Európskej únie.

Dominantnými bezpečnostnými mechanizmami pri zabezpečení prenosu dát sú kryptografické algoritmy. Moderné šifrovacie systémy využívajú obvykle kombináciu symetrických a asymetrických algoritmov doplnených o certifikáty verejných kľúčov [6]. Zaujímavou možnosťou je použitie blokových samoopravných kódov na účely šifrovania. Výhodou tohto riešenia je existencia dostupných komerčných zariadení a zachovanie prenosovej rýchlosti aj napriek použitiu šifrovania, ako je tomu pri použití niektorých asymetrických šifier.

This paper remarks on the possibility of the ciphering algorithm use based on the standard encoding techniques from the linear error - correcting coding area. The quality of deciphering algorithms is determined for (n, k) Hamming codes and the valid code word lengths are recommended for practical use. The presented principle can be generalised for another type of the algebraic codes.

1 INTRODUCTION

The communication subsystem as an important part of an information system is a neglected area for passive and active attacks against transferred information. Specifically, the public networks are regarded as non-trusted networks. This is why a solution for data security problems during transmission plays a very important role.

The network security services according to USA standard “Trusted Network Interpretation“ are classified into three groups [5]:

- Communications Integrity,
- Denial of Service,
- Compromise Protection.

The draft of paragraph version of New Telecommunication Law solves the problem of information, networks and intermediate protection in Slovak Telecommunication, too (the part IV, §26 „System of increased rate of secrete and transmitted information protection“). The aim of the new telecommunication legislation in Slovakia is to achieve a level of telecommunication services provided in selected European Union (EU) members.

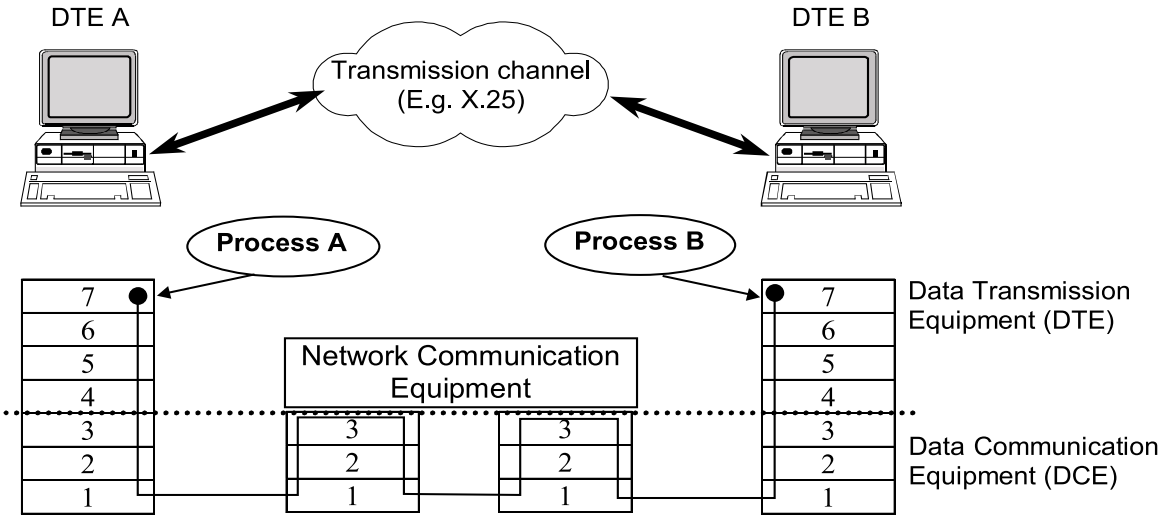
The dominant security mechanisms for data transmission are cryptographic algorithms that provide the security service as confidentiality, authentication and communications integrity. The modern cryptographic systems use the hybrid combination of symmetric and asymmetric algorithms with certification of public key [6]. The use of a block error - correcting coding in ciphering applications is an interesting possibility. The advantage of this coding is an availability of commercial coding equipment. The next advantage is a high code rate with ciphering use.

* **Ing. Mária Franeková, PhD., Ing. Peter Nagy**
Department of Information and Safety Systems, Faculty of Electrical Engineering, University of Žilina, Veľký diel, SK-010 26 Žilina, Slovak Republic, Phone +421-89-5133 248, E-mail frane@fel.utc.sk

Službu dôvernosti dát pri prenose podľa odporúčania ISO 7492-2 Security Architecture možno poskytnúť v druhej, tretej, štvrtej, šiestej alebo siedmej vrstve referenčného modelu OSI [2]. Šifrovanie dát v druhej vrstve referenčného modelu OSI je použiteľné len pre ochranu spojenia typu bod-bod. Výhodou tejto realizácie je transparentnosť dát pre všetky sieťové protokoly a aplikácie. Príklad komunikácie medzi dvoma koncovými stanicami v sieťach s rozhraním typu X.25 je znázornený schematickým modelom na obr. 1. V dolnej časti obrázku je znázornené, ktoré vrstvy modelu OSI sa podieľajú na komunikácií v závislosti na sledovaného prvku siete.

The confidentiality of data transmission according to recommendation ISO - 7498-2 Security Architecture is provided in the second, the third, the fourth, the sixth and the seventh layer of OSI (Open System Interconnection) [2].

The ciphering of data in the line layer of OSI can be used only for the protection of the connection end- to -end. The advantage of this realisation is the transparency of data for all network protocols and applications. The communication between entity A and B in networks with interface X.25 can be realised according to Figure 1. In the bottom of the picture the model shows which layers of OSI participate in communication according to followed element of network.



Obr. 1 Komunikácia medzi dvoma koncovými stanicami v sieti X.25
Fig. 1 Communication between DTE A and DTE B in X.25 network

Ak si komunikujúce stanice A a B žiadajú svoje dáta kryptograficky zabezpečiť, šifrovanie sa realizuje pred kanálovým kódovaním na strane vysielacej a dešifrovanie za kanálovým dekódovaním na strane prijímacej. Pre urýchlenie prenosu najmä u spojenia prostredníctvom modemu sa dáta pred šifrovaním najprv komprimujú vhodným algoritmom. Výhodou kompresie je aj skutočnosť, že komprimovaný šifrovaný text lepšie odoláva útokom zameraným na jeho dešifrovanie. V príspevku sa so zaradením kompresného kodéra neuvažuje. Ďalej sa predpokladá, že nebola neúmyselne narušená integrita dát v kanáli, pretože opisovaný šifrovací algoritmus možno použiť len pre kanál bez šumu. V prípade šumového kanála treba do prenosového reťazca zaradiť kanálový kodér.

If the entities A and B require to keep privacy of information, the communications system must be expanded by a ciphering encoder before the error-correcting encoder at the transmitter side and the ciphering decoder after error-control coding at the receiver side. For the increasing of data rate (mainly by modem data transmission) it is necessary to use the data compression. The advantage of the compressed cipher text is its resistantancy against some cryptoanalytict's attack. In the paper the authors do not solve problems of data compression. Further, the described algorithm is supposed to be applied only for the noiseless channel. For the noise channel for the elimination of noise must be channel code included.

2 VLASTNOSTI KRYPTOGRAFICKÉHO SYSTÉMU NA BÁZE HAMMINGOVÝCH (n, k) KÓDOV

Odbornej verejnosti je dobre známy princíp kódovania, dekódovania, detekcie a korekcie chýb u lineárnych systematických (n, k) kódov [1], [4]. Základné princípy týchto kódov možno využiť aj na šifrovanie.

2 PROPERTIES OF THE CRYPTOSYSTEM ON THE BASE OF HAMMING (n,k) CODES

Generally it is well known that principles of encoding, decoding, detection and correction of errors with linear systematic (n, k) codes use [1], [4]. The basic principles of these codes can be used also for ciphering.

Kódovanie zdrojovej k-tice $z = (z_1, z_2, ..., z_k)$ lineárneho systematického kódu k x n sa realizuje prostredníctvom rovnosti:

$$u = z \cdot G\,, \tag{1}$$

kde G je generujúca matica k × n lineárneho systematického kódu, ktorá ho jednoznačne určuje.

Hammingove (n, k) kódy patria do množiny lineárnych kódov a pokiaľ ich použijeme na elimináciu šumu v kanáli, majú nasledujúce vlastnosti [4]:
- dĺžka kódu $n = 2^m - 1$,
- počet informačných prvkov $k = 2^m - m - 1$,
- počet zabezpečovacích prvkov $m = n - k$,
- minimálna Hammingova vzdialenosť medzi kódovými zložkami $d_{min} = 3$ (v prípade perfektných kódov) a korekčná schopnosť $t = 1$.

Základná myšlienka použitia lineárnych samoopravných kódov (n, k) pre potreby šifrovania spočíva v „utajení" alebo „zamaskovaní" generujúcej matice G po vynásobení maticami S a P. Takto získame maticu K, ktorá predstavuje kľúč takéhoto kryptosystému:

$$K = S \cdot G \cdot P\,, \tag{2}$$

kde: S je ľubovoľná invertovateľná binárna matica typu $k \times k$,
P je pertmutačná matica typu $n \times n$, ktorá vznikne z jednotkovej matice zámenou poradia riadkov a stĺpcov.

Tento systém možno zaradiť medzi systémy s verejným kľúčom. Súkromný (tajný) kľúč pozostáva z troch matíc S, G a P a verejný kľúč z matice K. Verejný kľúč je spolu s algoritmom zverejnený.

Hammingove (n, k) kódy možno použiť na šifrovanie dát, ak sú dodržané nasledujúce podmienky:
- vysielacia strana pozná maticu K (verejný kľúč),
- prijímacia strana pozná typ Hammingovho (n, k) kódu, matice S, G a P (súkromný - tajný kľúč) a kontrolnú maticu H na korekciu náhodne generovaného chybového vektora.

Príslušné šifrovacie zobrazenie $T_k(z)$ takto definovaného kryptosystému je:

$$T_k(z) = z \cdot K + c\,, \tag{3}$$

kde c reprezentuje vektor dĺžky n náhodne generovaný vysielačom správy pre každý blok správy. Prijímacia strana prijme signál, ktorý je reprezentovaný vektorom $y = T_k(z)$.

Dešifrovanie prebieha podľa nasledujúcich krokov [3]:
- nájdenie inverznej permutačnej matice P^{-1} a výpočet $y \,.\, P^{-1}$,
- eliminácia chybového vektora c pomocou kontrolnej matice H, t. j. výpočet $(y \,.\, P^{-1}) \,.\, H^T$,
- nájdenie kódu $z \,.\, S$ pomocou generačnej matice G,
- nájdenie inverznej matice S^{-1} a výpočet originálneho vektora z.

The encoding of a plain text word $z = (z_1, z_2, ..., z_k)$ is as follows:

$$u = z \cdot G\,, \tag{1}$$

where G is generating matrix of linear systematic code of the size $k \times n$ and u are the code words.

The Hamming (n, k) codes are the linear block codes with following properties:
- code word length is $n = 2^m - 1$,
- message length is $k = 2^m - m - 1$,
- check parity is $m = n - k$,
- minimal Hamming distance $d_{min} = 3$ (for perfect codes),
- error-correcting capability $t = 1$ in each code word.

The main idea of the use Hamming (n, k) codes for ciphering a plain text is based on the masking of the generating matrix G. Generating matrix is transformed by binary matrixes S and P to the matrix K according to:

$$K = S \cdot G \cdot P\,, \tag{2}$$

where: S is the binary convertible matrix of the side $k \times k$,
P is the permutation matrix of the side $n \times n$, which it is created from the eye matrix by changing its rows and columns.

This system can be classified as the public key cryptosystem.

The private key consists of three matrixes S, G and P and the public key of the matrix K only, which is publicly known with the algorithm, too.

The Hamming (n, k) codes can be used as the cipher codes when the following conditions are kept:
- transmitting side knows the matrix K (public key),
- receiving side knows the type of Hamming (n, k) code, the matrixes G, S, P (private key) and the check matrix H for correction of random error vector.

Transformation of this cryptosystem $T_k(z)$ is given by

$$T_k(z) = z \cdot K + c\,, \tag{3}$$

where c is the n-bits error vector of weight $\leq t$, that is at random generated from the transmitting side for every code word. The receiving side receives the signal, which can be represented by vector $y = T_k(z)$

The deciphering process is realised according to the following steps [3]:
- determination of the inverse permutation matrix P^{-1} and calculation $y \,.\, P^{-1}$,
- elimination of error vector c by check matrix H by calculation $(y \,.\, P^{-1}) \,.\, H$,
- determination of the code $z \,.\, S$ by means of the G
- calculation the original vector z by the binary inverse matrix S^{-1} use.

3 ANALÝZA VÝPOČTOVEJ ZLOŽITOSTI ŠIFRY

Kvalita šifry je daná zložitosťou šifrovacieho a dešifrovacieho algoritmu. Zložitosť šifrovacieho a dešifrovacieho algoritmu možno určiť z počtu cyklov priemerne potrebných na dešifrovanie kryptogramu. Čím je šifra zložitejšia, tým viac cyklov bude potrebných na jej prelomenie a to samozrejme zaberie viac času. Dnes je známych mnoho kryptoanalytických útokov [3]. Algoritmus kvalitnej šifry predpokladá len útok hrubou silou, t. j. vyskúšanie všetkých možných kombinácií kľúča.

Kvalita analyzovanej šifry spočíva v tom, že určenie spätnej šifrovacej transformácie $T_k(z)^{-1}$ nie je možné prostredníctvom výpočtu inverznej matice K^{-1}, pretože každý odosielaný blok správy je po zašifrovaní znáhodňovaný n-bitovým chybovým vektorom c. Vzhľadom na to je dešifrovanie bez znalosti tajnej časti kľúča aj pre malé dimenzie (n, k) výpočtovo zložitý problém, ktorý je obtiažne vyriešiť v reálnom čase. Druhá cesta rozlomenia šifry vychádza zo znalosti nielen kľúča K, ale aj algoritmu a znamená nájsť a vyskúšať všetky submatice P, S, G, ktoré sú súčasťou kľúča a na základe kontrolnej matice H eliminovať chybový vektor c.

Autori sa pokúsili určiť výpočtovú zložitosť tohto problému pri použití Hammingových (n, k) kódov, pretože komerčných zariadení tohto typu (pre korekciu jednoduchej chyby) sa v praxi vyskytuje najviac. Hodnoty sú uvedené pre dimenziu od $m = 3$ do $m = 13$ v tab. 1. Z tabuľky vidieť ako klesá redundancia r [%] u väčších dimenzií (od hodnoty $n = 1023$ je $r < 1$ %).

3 ANALYSIS OF CIPHER QUALITY

The cipher quality is given by the complexity of deciphering algorithm. The complexity of deciphering algorithm can be determined by the number of cycles that the algorithm needs for deciphering cryptogram in average. The complexity of the cipher is proportional to time for the breaking of deciphering algorithm. Many of cryptoanalytic attacks are well known today [3]. Quality cipher algorithm assumes the brute force attack only. It means trying all combinations of key.

The quality of analysed cipher algorithm resides in determination of inverse ciphering transformation $T_k(z)^{-1}$. This determination is not able to be realised by inverse matrix K^{-1}, because for every transmitted code word is created the randomisation of cryptosystem by n-bits error vector c. In respect to it deciphering is complicated already for small (n, k) dimension and it is impossible to solve in real time operation.

The second way for breaking deciphering algorithm is based on the knowledge not only of the public key K and also algorithm. It means that potential hacker must find and test all submatrixes P, S, G (which can be the part of key K) and eliminate the error vector by check matrix H.

Authors tried to analyse the cipher quality of cryptographic system based on Hamming (n, k) codes because the commercial equipment with these types of codes (for correction of simply error) is very often used. A list of the valid Hamming code parameters with check parity m from $m = 3$ to $m = 13$ is provided in the Table 1. This table shows how redundancy r [%] decreases for larger dimension of n (for n larger than 1023 is redundancy less than 1 %).

Výpočtová zložitosť šifry na báze Hammingových (n, k) kódov — Tab. 1
Quality of cryptographic system based on Hamming (n, k) codes

m	k	n	r [%]	n!	v_k	P_{RM}
3	4	7	42.86	5040	11811	20160
4	11	15	26.6	$1.30767 \cdot 10^{12}$	$5.71623 \cdot 10^{13}$	$7.68105 \cdot 10^{35}$
5	26	31	16	$8.22283 \cdot 10^{33}$	$4.56733 \cdot 10^{39}$	$9.05446 \cdot 10^{202}$
6	57	63	9.52	$1.98260 \cdot 10^{87}$	$3.05394 \cdot 10^{103}$	$3.21397 \cdot 10^{977}$
7	120	127	5.51	$3.01266 \cdot 10^{213}$	$2.51922 \cdot 10^{253}$	$1.96120 \cdot 10^{4334}$
8	247	255	3.17	$3.35085 \cdot 10^{504}$	$2.36007 \cdot 10^{595}$	$8.04651 \cdot 10^{18364}$
9	502	511	1.76	$6.79158 \cdot 10^{1163}$	$3.66854 \cdot 10^{1360}$	$0.0180495 \cdot 2^{2.52008 \cdot 10^{5}}$
10	1013	1023	0.97	$5.29153 \cdot 10^{2636}$	$1.13471 \cdot 10^{3050}$	$0.0180495 \cdot 2^{1.02617 \cdot 10^{6}}$
11	2036	2047	0.54	$8.16744 \cdot 10^{5890}$	$8.08367 \cdot 10^{6739}$	$0.0180495 \cdot 2^{4.1453 \cdot 10^{6}}$
12	4083	4095	0.29	-	$3.20101 \cdot 10^{14753}$	$0.0180495 \cdot 2^{1.66708 \cdot 10^{7}}$
13	8178	8191	0.16	-	-	-

Poznámka: *Výsledky uvedené v tab.1 boli získané s využitím programového nástroja DERIVE; bežne dostupné programy (napr. MATLAB, EXCEL) dokážu vypočítať max. 170! a obdobné obmedzenia majú aj pre výpočet ďalších hodnôt, čo súvisí s problémom reprezentácie čísla väčšieho ako 10^{308} v pamäti počítača. Hodnoty označené pomlčkou sú programovým prostriedkom DERIVE nevyčísliteľné.*

Note: *The parameters shown in the table were calculated via the programme DERIVE. The commercial programmes (E.g. MATLAB, EXCEL) are able to compute values max. 170!. Similar limits are valid also for computation of further values, what causes the problem to represent a number larger than 10^{308} in computer memory. The values marked by symbol " - " are impossible to compute by DERIVE programme.*

Výpočtovú zložitosť ovplyvňujú nasledujúce faktory:

A. výpočet inverznej permutačnej matice P^{-1}

Permutačná matica je veľkosti $n \times n$ bitov. Nájdenie všetkých permutačných matíc je zložitý problém najmä pre väčšie dimenzie n, lebo počet kombinácií odpovedá hodnote $n!$. V tab. 1 je tento parameter vypočítaný maximálne pre kód (2047, 2036).

Po nájdení všetkých inverzných permutačných matíc treba pre každý prijatý vektor y vyskúšať výpočet $y \,.\, P^{-1}$.

B. eliminácia chybového vektora c

Chybový vektor n-bitový s váhou $w(c) \leq t$, kde t je počet korigovaných chýb. Celkový počet rôznych chybových vektorov $c \,.\, P^{-1}$ pre slová dĺžky n potom je:

$$p = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{t}. \qquad (4)$$

Chybový vektor sa deteguje pomocou techniky známej z teórie korekčných kódov, na základe znalosti kontrolnej matice H veľkosti $n \times (n - k)$, ktorá sa určí z generujúcej matice G veľkosti $n \times k$ a jednotkovej matice I veľkosti $(n - k) \times (n - k)$. Výpočtom $(y \,.\, P^{-1}) \,.\, H^T$ sa zistí, v ktorom stĺpci matice je chyba a táto sa následne eliminuje. (Poznámka: H^T je transponovaná kontrolná matica.)

C. hľadanie pôvodného vektora $z \,.\, S$

Ak G je generačná matica systematického kódu, je tento proces hľadania zjednodušený, pretože z priestoru možných kódových kombinácií V_n stačí sledovať zdrojový podpriestor V_k, v ktorom sa nachádzajú kombinácie informačnej časti. Počet takýchto možností je [3]:

$$v_k = \prod_{j=0}^{k-1} (2^{n-j} - 1) \cdot (2^{k-j} - 1)^{-1}. \qquad (5)$$

D. hľadanie inverznej matice S^{-1}

Matica S je veľkosti $k \times k$ bitov a musí byť invertovateľná. Všetky kombinácie regularných matíc S sa môžu pre nesystematický vypočítať podľa [3]

$$P_{RM} = 2^{k^2} \prod_{j=1}^{k} \cdot (1 - 2^{-j}) \cong 2^{k^2} \cdot 0{,}29\,. \qquad (6)$$

kde k je dĺžka správy.

ZÁVER

Z tab. 1 vidieť, že už pre malé dimenzie Hammingových (n, k) kódov je počet kombinácií pri výpočte čiastkových častí kľúča značný. Výpočet všetkých kombinácií jednotlivých častí kľúča pre dimenzie od (n, k) → (511, 502) je obtiažne realizovateľný v reálnom čase. Pre nájdenie originálneho kľúča je potrebné všetky vypočítané kombinácie správne skombinovať, čo je tiež

The following factors influence the quality of deciphering algorithm:

A. calculation of inverse permutation matrixes P^{-1}

Permutation matrix P is of the side $n \times n$. The determination of all permutation matrixes P is a complicated problem mainly for larger dimension of code word n as the number of all combinations is n factorial. N factorial in Table 1 is computed maximally for (n, k) code (2047, 2036). After the determination of all inverse permutation matrixes P^{-1} it is necessary to calculate $y \,.\, P^{-1}$ for all received vectors y.

B. elimination of error vector c

The error vector c is n-bits vector with the weight $w(c) \leq t$, where t is number of correcting errors. The total number of various errors vectors $c \,.\, P^{-1}$ for code word of length n then is

$$p = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{t}. \qquad (4)$$

The error vector can be detected with the help error-correcting techniques. This algorithm is based on knowledge of the check matrix H of the side $n \times (n - k)$ which can be determined by generating matrix of the side $n \times k$ and from the eye matrix I of the side $(n - k) \times (n - k)$. The column of matrix with error is determined according to expression $(y \,.\, P^{-1}) \,.\, H^T$. In the next step the error is eliminated. (Note: H^T is a transposed matrix of H matrix).

C. determination of original vector $z \,.\, S$

If G is generating matrix of systematic code, this process of determination of vector $z \,.\, S$ is easier as it is enough to examine the combination of source subarea V_k from area of all combination V_n. Number of such possibilities is [3]:

$$v_k = \prod_{j=0}^{k-1} (2^{n-j} - 1) \cdot (2^{k-j} - 1)^{-1}. \qquad (5)$$

D. determination of inverse matrixes S^{-1}

S is a matrix of the side $k \times k$ and must be inverse. All combination of regular matrixes S for non-systematic code can be determined according to [3]:

$$P_{RM} = 2^{k^2} \prod_{j=1}^{k} \cdot (1 - 2^{-j}) \cong 2^{k^2} \cdot 0.29\,. \qquad (6)$$

where k is message length.

CONCLUSION

Table 1 shows that the number of key pieces combination is high already for relatively small code dimensions Hamming (n, k) codes. Computing combinations of all key pieces from dimension (n, k) → (511, 502) is realised problematically in real time operation. To find the original key, it is necessary combine the determined combination correctly, which it is time demanding problem, too.

časovo veľmi náročný problém. Možno konštatovať, že analyzovaný šifrovací systém (za predpokladu útoku hrubou silu) je výpočtovo zložitý.

Uvedený šifrovací systém je vhodný na použitie pre špecializované prenosy v úrovni linkovej vrstvy, kde sa vyžaduje rýchly prenos dát pri zaručenej dôvernosti prenášaných informácií. Výhodné by bolo, keby kodér-dekodér plnil okrem šifrovacej funkcie aj funkciu korekčnú (myslí sa korekcia chýb spôsobených šumom). Pre takúto aplikáciu predpokladáme možnosť využitia algoritmov na báze samoopravných kódov pre viacnásobné chyby akými sú napr. algoritmy BCH kódov. U týchto kódov sa zároveň zvyšuje odolnosť voči prelomeniu šifry aj pri použití iných kryptoanalytických útokov.

Táto práca bola riešená v rámci grantových projektov číslo:

- 1/5255/98 s názvom: „Teoretický aparát pre analýzu a syntézu systému protokolov komunikačného systému s osobitným sortimentom služieb“,
- 1/5230/98 s názvom: „Teoretický aparát pre analýzu a syntézu s definovanou úrovňou bezpečnosti“.

Recenzenti: D. Levický, P. Tomašov

We can say that the analysed cipher system is complex of computation (assuming only brute force attack). We would recommend its use in special applications for fast and confidential transmission in the line layer of the OSI.

If cipher-decipher algorithms had also the error-correcting coding function (i. e. elimination influences of channel), it would be a big advantage. For this application we assume using of multi-error correcting coding algorithms, e. g. algorithm of BCH codes, whose ciphering algorithm is more resistant against the other cryptoanalytick attacks.

This work is a part of grant research projects:

1/5255/98 with the title “Theoretical apparatus for analysis and synthesis of communication system protocol with special service set“,

1/5230/98 with the title: “Theoretical apparatus for analysis and synthesis of system with defined level of safety“.

Reviewd by: D. Levický, P. Tomašov

LITERATÚRA - REFERENCES

[1] CLARC, G. C., CAIN, J. B.: Error Correcting Coding for Digital Communications, Plenum Press, New York, 1988
[2] DOBDA, L.: Ochrana dat v informačních systémech, GRADA, Praha, 1998
[3] GROŠEK, O., PORUBSKÝ, Š.: ŠIFROVANIE, GRADA, Praha, 1992
[4] KONVIT, M.: Teória oznamovania, ALFA, Bratislava, 1989
[5] NOVÁK, L.: Duhová série (Rainbow Series), Hodnocení informační bezpečnosti, Seminár AFOI, Praha, 1995, str. III-1 - III-15
[6] STAUDEK, J.: Kryptografie a bezpečnost, LanCom, február 1998, str. 14 - str. 22