

PŘIHLÁŠKA VYNÁLEZU

Zveřejněná podle §31 zákona č. 527/1990 Sb.

(21) Číslo dokumentu:

2022-20

(13) Druh dokumentu: **A3**

(51) Int. Cl.:

H04L 9/06

(2006.01)

(19)
ČESKÁ
REPUBLIKA



ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

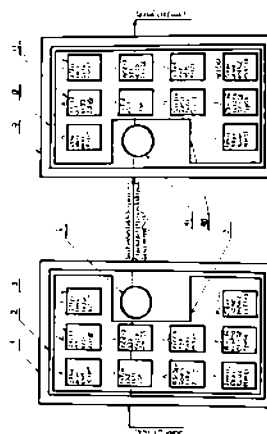
(22) Přihlášeno: **17.01.2022**

(40) Datum zveřejnění přihlášky vynálezu: **26.07.2023**
(Věstník č. 30/2023)

- (71) Přihlašovatel:
Miroslav Tyrpa, Ostrava, Mariánské Hory, CZ
- (72) Původce:
Miroslav Tyrpa, Ostrava, Mariánské Hory, CZ
- (74) Zástupce:
Rott, Růžička & Guttman a spol., Vyskočilova
1566, 140 00 Praha 4, Michle

(54) Název přihlášky vynálezu:
**Způsob kódování a dekódování textových a
multimediálních zpráv a zařízení k
uskutečnění tohoto způsobu**

- (57) Anotace:
Vynález se týká způsobu ochrany textových a multimediálních zpráv, zejména utajovaných zpráv sdělovaných odesílatelem příjemci, a zařízení k uskutečňování tohoto způsobu. Každý zápisný znak, nebo byt, tvořící zprávu, se v pořadí shodném s jeho výskytem ve zprávě nahradí pomocí vysílacího převáděče (2) v pořadí prvním dosud nepoužitým zástupným kódem (7) ze souboru (6) zástupných kódů přiřazeného danému zápisnému znaku nebo bytu a tímto způsobem ze zástupných kódů (7) sestavená zpráva se vysílačem (1) odešle alespoň jednomu určenému přijímači (8), kde se obráceným postupem transformuje zpět do své původní podoby. Vysílač (1) a přijímač (8) tvoří zařízení ke kódování a dekódování zpráv a sestávají z vysílacího převáděče (2) a příjmového převáděče (9).



Způsob kódování a dekodování textových a multimediálních zpráv a zařízení k uskutečnění tohoto způsobu

5 Oblast techniky

Vynález se týká způsobu kódování a dekodování důvěrných textových a multimediálních zpráv, zejména zpráv sdělovaných odesílatelem příjemci, ale také např. záznamů z bezpečnostních čidel a kamer zajišťujících ostrahu objektů, a zařízení k uskutečňování tohoto způsobu. Má zásadní
10 význam pro ochranu sdělovaných důvěrných a utajovaných textových informací a pro ochranu přenášených zvukových, obrazových, případně i jiných dat v komunikaci.

Dosavadní stav techniky

15 K ochraně důvěrných informací, ať už jde o ochranu zpráv sdělovaných mezi odesílatelem a příjemcem nebo o přenos informací zaznamenaných bezpečnostními přístroji do vyhodnocující je centrály se v současné době používá nejčastěji šifrování. K přečtení šifrovaných zpráv se pak použije dešifrování. Původně se šifrovaly jen textové zprávy, jelikož na rozdíl od zpráv zvukových
20 a obrazových byly sestavovány ze známých znaků - písmen, slabik, číslic a jiných symbolů jako jsou diakritické, interpunkční, matematické a další znaky, které bylo možno na dobu přenosu poměrně snadno nahradit znaky měnicemi obsah zpráv nebo činicemi je zcela nesmyslnými. Nastupující digitalizace přenosových systémů umožnila vyjádřit také akustické a obrazové zprávy pomocí šifrovatelných znaků - bytů (bajtů). V současné době se může jednat o jeden ze dvou
25 základních druhů šifrování, a to šifrování a dešifrování symetrické nebo asymetrické. K oběma zmíněným druhům šifrování a dešifrování se využívají šifrovací klíče v podobě šifrovacích či dešifrovacích algoritmů, k jejichž vytvoření se nejčastěji využívají různé matematické operace. Šifrovací klíče jsou stále sofistikovanější a jejich prolomení je sice obtížné, avšak při současných technických a technologických možnostech nikoliv nemožné.

30 Ze zveřejněné patentové přihlášky PV 2008-812 je známý způsob synchronizace alespoň dvou od sebe oddělených generátorů náhodných klíčů určených zejména pro šifrování informací mezi odesílatelem a příjemcem, kde jeden z generátorů je u odesílatele a další u příjemce informací. Odesílatel i příjemce disponují pak identickými množinami náhodných šifrovacích klíčů, které se
35 průběžně synchronně mění náhodným znakem tak, že i po změnách zůstávají identické. Synchronizace měnicích se šifrovacích klíčů se dosahuje pomocí matematických operací předem dohodnutých mezi odesílatelem a příjemcem případně příjemci.

V patentovém spisu US7454016 je popsán systém šifrování dat implementovaný spuštěním
40 šifrovacího programu na počítači vybaveném vyrovnávací pamětí, který obsahuje transformační tabulky, z nichž každá obsahuje předem určený počet záznamů. Všechny nebo nezbytné transformační tabulky se načtou do vyrovnávací paměti před procesem šifrování / dešifrování. To způsobí, že doba šifrování / dešifrování bude v podstatě stejná nezávisle na počtu provozních záznamů pro transformační tabulku.

45 Předmětem technického řešení obsaženého v patentovém spisu US7457413 je způsob generování náhodných čísel pro použití při šifrování zprávy a zařízení pro bezpečný přenos uvedené zprávy z vysílacího zařízení do přijímače. Optický obraz představovaný optickými daty je získáván optickým senzorem a zpracováván za účelem zlepšení matematicky zjiřitelné nahodilosti
50 optických dat. Takto zpracovaná data jsou pak použita pro generování náhodných čísel, která mohou být použita jako šifrovací klíč, nebo pro generování šifrovacího klíče, pro následné použití v šifrovacím algoritmu pro šifrování zprávy.

55 Nevýhodou šifrování zpráv obecně je to, že účinnost ochrany, kterou poskytují předávaným zprávám je přímo úměrná složitosti šifrovacího klíče, která je dána zejména jeho délkou. Na délce

šifrovacího klíče je ale přímo závislá také doba potřebná k šifrování / dešifrování a tím i energetická náročnost celého procesu. Přitom však ani velmi dlouhé a komplikované šifrovací klíče negarantují jejich neprolomitelnost.

5

Podstata vynálezu

Předkládaný vynález nabízí řešení ochrany zpráv jejich kódováním, které nevyžaduje použití žádného klíče. Podstata kódování a dekódování textových a multimediálních zpráv sdělovaných odesílatelem příjemci, které jsou sestaveny z písmen či slabik použité abecedy či použitých abeced případně z jiných použitých symbolů, tedy souhrnně řečeno z použitých zápisných znaků, nebo z bytů v případě multimediální zprávy, podle tohoto vynálezu, spočívá v tom, že každý jednotlivý zápisný znak nebo byt, tvořící zprávu, se v pořadí shodném s jeho výskytem ve zprávě nahradí v pořadí prvním dosud nepoužitým, tedy i pro stejný zápisný znak pokaždé jiným zástupným kódem z předem vytvořeného souboru zástupných kódů, přiřazeného danému zápisnému znaku nebo bytu použitému k vytvoření zprávy. Zpráva sestavená tímto způsobem ze zástupných kódů se pak standardním způsobem odešle alespoň jednomu určenému příjemci, kde se obráceným postupem transformuje zpět do své původní podoby.

Zřejmou a u jiných způsobů se nevyskytující výhodou sdělování zpráv způsobem podle tohoto vynálezu je to, že ke kódování / dekódování zpráv není používán žádný šifrovací či jiný klíč, čímž je zcela znemožněno jeho zcizení či rozkódování případným narušitelem. Mimořádnou předností sdělování zpráv způsobem podle tohoto vynálezu je také skutečnost, že i v případě, že se narušiteli povede nabourat do přenosové sítě a zachytit předávanou zprávu, není schopen dekódovat její obsah, neboť po celou dobu přenosu je tato zpráva sestavena ze zástupných kódů, z nichž každý je tvořen shlukem naprosto nesystémově, nesmyslně, chaoticky seřazeného a početně různorodého množství kódových znaků. Absence šifrovacího či jakéhokoliv jiného klíče znamená také zjednodušení, které ve srovnání se šifrováním přináší zrychlení kódovacího procesu s příznivým dopadem na jeho energetickou a technologickou náročnost.

30

Z dlouhodobého hlediska je výhodné, aby se po použití zástupný kód pouze označil jako použitý a ze souboru zástupných kódů se nevymazával. To proto, že po použití a označení posledního zástupného kódu z příslušného souboru zástupných kódů umístěného vdaném kódovacím paměťovém registru, se pak může označení všech zástupných kódů v tomto souboru jako použitých zrušit, a soubor těchto zástupných kódů lze použít k opětovnému nahrazování příslušného zápisného znaku nebo bytu sdělované zprávy. Tím je umožněno vícenásobné použití jednotlivých souborů zástupných kódů, což v důsledku znamená prakticky neomezenou životnost celého systému při spolehlivém zachování bezpečnosti přenášených zpráv.

Pro účinnost tohoto způsobu kódování a dekódování zpráv je důležité, že soubor zástupných kódů je tvořen množinou vzájemně odlišných a na sobě nezávislých, během jednoho použití souboru jednorázově použitelných unikátních zástupných kódů sestavených z libovolného počtu jakkoliv kombinovaných kódových znaků, tzn. písmen, slabik a jiných symbolů používaných jakýmkoliv abecedami, číslic nebo ostatních znaků schopných zápisu do elektronické paměti. Tato všestranná různorodost kódových znaků použitých pro tvorbu zástupných kódů rozhoduje o jejich jedinečnosti a tím i absolutní nerozlučitelnosti z nich sestavených zpráv.

Podstatou vynálezu je dále zařízení k uskutečňování popsaného způsobu kódování a dekódování textových a multimediálních zpráv. Skládá se z vysílače, který obsahuje vysílací převáděč, který je vybaven elektronickou pamětí vysílače a kódovacím řídicím procesorem a v případě přenosu multimediálních zpráv tvořených analogovým signálem také analogově digitálním převodníkem a z přijímače, který obsahuje příjmový převáděč, který je vybaven elektronickou pamětí přijímače a dekódovacím řídicím procesorem a pro příjem multimediálních zpráv také digitálně analogovým převodníkem. V elektronické paměti vysílače jsou vytvořeny kódovací paměťové registry, z nichž každý je určen pro uložení souboru zástupných kódů určených k nahrazování jednotlivých

55

zápisných znaků nebo bytů, obsažených v textové nebo multimediální zprávě. V elektronické paměti přijímače je vytvořen shodný počet dekódovacích paměťových registrů pro uložení souborů zástupných kódů, které jsou shodné se soubory zástupných kódů uloženými v kódovacích paměťových registrech. Kódovací řídicí procesor je naprogramován a/nebo nakonfigurován k postupnému nahrazování jednotlivých zápisných znaků nebo bytů tvořících zprávu vždy prvním dosud nepoužitým unikátním zástupným kódem ze souboru zástupných kódů uložených v kódovacích paměťových registrech a přiřazených těmto jednotlivým zápisným znakům nebo bytům. Na druhé straně pak je dekódovací řídicí procesor naprogramován a/nebo nakonfigurován k postupnému vyhledání a spárování přijatých zástupných kódů se zástupnými kódy uloženými v jednotlivých dekódovacích paměťových registrech a k jejich následnému zpětnému převedení na jednotlivé zápisné znaky nebo byty použité v původní textové nebo multimediální zprávě.

Počet kódovacích paměťových registrů a dekódovacích paměťových registrů je roven nejméně počtu jednotlivých zápisných znaků, které jsou potřebné k tvorbě textové zprávy určené ke sdělení nebo počtu bytů, včetně ukončovacího bitu, potřebných k tvorbě multimediální zprávy určené ke sdělení. Jelikož však toto zařízení není určeno ke kódování a dekódování jedné zprávy nebo jinak omezeného počtu zpráv, je v praxi minimální počet těchto paměťových registrů dán počtem zápisných znaků obsažených v abecedě daného jazyka a počtu číslic a znaků používané matematické soustavy, v případě multimediálních zpráv pak minimálním počtem bytů nezbytných k jejich vytvoření.

Z hlediska zabezpečení plynulé dlouhodobé provozuschopnosti tohoto zařízení je výhodné aby kódovací řídicí procesor i dekódovací řídicí procesor byly naprogramovány a/nebo nakonfigurovány k označení každého použitého zástupného kódu za účelem zamezení jeho opětovného použití a zároveň tak, aby po použití a označení posledního zástupného kódu z příslušného souboru zástupných kódů se označení všech v něm se nacházejících zástupných kódů jako použitých zrušilo a soubor těchto zástupných kódů se aktivoval k opětovnému nahrazování příslušného zápisného znaku nebo bytu obsaženého ve sdělovaných zprávách. Tím se dá vyhnout potřebě opakované tvorby nových souborů zástupných kódů a nepravidelnému nahrazování jimi vypotřebovaných souborů zástupných kódů.

Jako vysílač a přijímač mohou být po instalaci příslušné aplikace použity počítače, tablety, mobilní telefony nebo jiná elektronická zařízení tohoto druhu. Vzhledem ke zranitelnosti těchto zařízení neoprávněnými zásahy je však vhodnější, je-li kódování a dekódování zpráv s vysokým stupněm utajení uskutečňováno pomocí jednoúčelových zařízení.

V důsledku v zásadě shodné konstrukce vysílače a přijímače mohou tato zařízení plnit obě funkce - vysílací i přijímací. Komunikace mezi nimi může tudíž probíhat obousměrně. V případě obousměrného přenosu multimediálních zpráv musí být vysílač i přijímač vybaveny digitálně analogovým převodníkem.

Objasnění výkresů

Obr. 1 - schematické vyobrazení zařízení a způsobu kódování a dekódování textové zprávy ve znění: TAJNÁ LISTINA podle tohoto vynálezu

Obr. 2 - schematické vyobrazení zařízení pro kódování a dekódování multimediální (zvukové) zprávy

Obr. 3 - schématické vyobrazení kódovacího / dekódovacího paměťového registru a v něm obsaženého souboru zástupných kódů

Příklady uskutečnění vynálezu

Příklad 1

5 Způsob kódování a dekódování textové zprávy je popsán v dále uvedeném příkladu, který se kvůli větší názornosti omezil na popis kódování a dekódování jednoduché informace sestávající pouze ze dvou slov: TAJNÁ LISTINA! Tato informace je tvořena dvěma slovy s osmi různými písmeny, mezerou mezi oběma slovy a vykřičníkem na konci druhého slova. Obsahuje tedy deset různých zápisných znaků. Jedná se o dvě písmena A, jedno písmeno Á, dvě písmena I, jedno písmeno J,
 10 jedno písmeno L, dvě písmena N, jedno písmeno S, dvě písmena T znaménko vykřičníku a znak mezery. Pro sdělení této zprávy způsobem podle tohoto vynálezu bude tedy jak v elektronické paměti 3 vysílače, tak v elektronické paměti 10 přijímače využito po deseti kódovacích / dekódovacích paměťových registrech 5, 12 přiřazených těmto zápisným znakům. Kódovací / dekódovací paměťové registry 5, 12 jsou označeny zápisnými znaky, kterým jsou přiřazeny a jsou seřazeny v abecedním pořadí. Pro určité zjednodušení a zároveň lepší názornost je na obr. 1 znázorněno jen zmíněných deset kódovacích / dekódovacích paměťových registrů 5 a 12 a v každém z nich jsou uvedeny pouze čtyři velmi jednoduché zástupné kódy 7 (v praxi jsou paměťové registry schopny pojmut obrovské množství i mnohem delších a složitějších zástupných kódů obsahujících třeba i písmena a další znaky používané v různých abecedách).

20 Po zahájení psaní výše uvedené zprávy se nejprve pomocí kódovacího řídicího procesoru 4 vyhledá kódovací paměťový registr 5 přiřazený písmenu T a nahradí se tento zápisný znak prvním dosud nepoužitým, tj. prvním v pořadí zástupným kódem 7 z tohoto kódovacího paměťového registru 5, sestávajícím z pěti kódových znaků 7.1 (lovik), poté se vyhledá kódovací paměťový registr 5 přiřazený zápisnému znaku A, který se nahradí prvním zástupným kódem 7 z tohoto kódovacího paměťového registru (jaNe), obdobným postupem se nahradí zápisný znak J prvním zástupným kódem 7 z kódovacího paměťového registru 5 přiřazeného tomuto zápisnému znaku (ryžok), zápisný znak N prvním zástupným kódem 7 z kódovacího paměťového registru 5 pro tento zápisný znak (N5r3zw), zápisný znak Á prvním zástupným kódem 7 z kódovacího paměťového registru 5 přiřazeného tomuto zápisnému znaku (ax:b3), zápisný znak mezery prvním zástupným kódem 7 z kódovacího paměťového registru 5 pro tento zápisný znak (čikoz), následně se nahradí zápisný znak L prvním zástupným kódem 7 z kódovacího paměťového registru 5 pro tento zápisný znak (Vyl8r7), zápisný znak I prvním zástupným kódem 7 z kódovacího paměťového registru 5 pro tento zápisný znak (215rr), zápisný znak S prvním zástupným kódem 7 z kódovacího paměťového registru 5 pro tento zápisný znak (víro4), zápisný znak T prvním dosud nepoužitým, tj. v pořadí druhým zástupným kódem 7 z kódovacího paměťového registru 5 pro tento zápisný znak (583r), stejně tak se nahradí další zápisný znak I druhým zástupným kódem 7 z kódovacího paměťového registru 5 pro tento zápisný znak (zwick), zápisný znak N druhým zástupným kódem 7 z kódovacího paměťového registru 5 pro tento zápisný znak (Gama), zápisný znak A druhým zástupným kódem 7 z kódovacího paměťového registru 5 pro tento zápisný znak (zero) a konečně zápisný znak vykřičníku prvním zástupným kódem 7 z kódovacího paměťového registru 5 pro tento zápisný znak (@-;55). Zároveň s použitím každého zástupného kódu 7 se označí takový zástupný kód 7 jako použitý, aby nemohlo dojít k jeho opakovanému použití. Výsledkem popsaného procesu je zpráva ve tvaru:

45 lovikjaNeryžokN5r3zwax:b3čikozVyl8r7215rrvíro4583rzwikGamazero@-;55.

Po přijetí přijímačem 8 zprávy v tomto tvaru se pomocí jeho dekódovacího řídicího procesoru 11 zahájí opačný proces, tj. proces vyhledávání shodných zástupných kódů 7 v paměťových registrech 12, přiřazování jim odpovídajících zápisných znaků a konečně sestavení z nich sdělené zprávy v původní čitelné podobě.

55 Zařízení ke kódování a dekódování textových zpráv způsobem podle tohoto vynálezu, schematicky znázorněné na obr. 1, je tvořeno vysílačem 1 obsahujícím vysílací převaděč 2, který je vybaven elektronickou pamětí 3 vysílače a kódovacím řídicím procesorem 4 a přijímačem 8 obsahujícím

přijmový převáděč 9, který je vybaven elektronickou pamětí 10 přijímače a dekódovacím řídicím procesorem 11. V elektronické paměti 3 vysílače jsou vytvořeny kódovací paměťové registry 5 pro uložení souborů 6 zástupných kódů k nahrazování jednotlivých zápisných znaků používaných k tvorbě textových zpráv v daném jazyce (písmena příslušné abecedy, diakritické a interpunkční znaménka, značka mezery, číslice, matematická znaménka a jiné symboly). V elektronické paměti 10 přijímače je vytvořen shodný počet dekódovacích paměťových registrů 12 pro uložení identických souborů 6 zástupných kódů se soubory 6 zástupných kódů uloženými v kódovacích paměťových registrech 5 obsažených v elektronické paměti 3 vysílače. Kódovací řídicí procesor 3 je naprogramován k postupnému nahrazování jednotlivých zápisných znaků sdělované textové zprávy prvními dosud nepoužitými unikátními zástupnými kódy 7 ze souborů 6 zástupných kódů přiřazených těmto zápisným znakům, zatímco dekódovací řídicí procesor 11 je naprogramován k vyhledání a spárování přijatých kódů 7 se zástupnými kódy 7 uloženými v jednotlivých dekódovacích paměťových registrech 12 a k jejich postupnému zpětnému převedení na jednotlivé jim odpovídající zápisné znaky a tím k jejich opětovnému sestavení do textové zprávy v původní podobě.

Příklad 2

Způsob kódování a dekódování multimediální zprávy, v tomto konkrétním příkladu hlasové zprávy předávané standardním telefonním hovorem, spočívá vtom, že se nejprve hlasový signál na výstupu z mikrofonu převede pomocí analogově digitálního převodníku 13 na digitální signál v podobě sledu individuálních bytů. Při 8 bitovém kódování a vzorkovací frekvenci 7 kHz vzniká na výstupu standardního a/d převodníku 13 256 různých bytů, vyjadřujících 256 úrovní intenzity vstupního hlasového signálu. Tyto byty se v pořadí v jakém vystupují z a/d převodníku 13 kódují zástupnými kódy 7 ze souborů 6 zástupných kódů, nacházejících se v jim přiřazených kódovacích paměťových registrech 5. Takto zakódovaná zpráva se standardní cestou předá přijímači 8, kde se pak opačným postupem uskutečňuje její dekódování, tzn. zástupné kódy 7, jimiž je vyjádřena hlasová zpráva, se převedou do podoby příslušných bytů a ty se pomocí d/a převodníku 14 převedou z digitální podoby do podoby analogové, tzn. do podoby akustické, sluchem vnímatelné a člověku srozumitelné zprávy.

Zařízení ke kódování a dekódování multimediálních zpráv způsobem podle výše popsaného příkladného provedení je schematicky vyobrazeno na obr. 2. Je tvořeno kódovacím vysílačem 1, obsahující vysílací převáděč 2, který je vybaven, a/d převodníkem 13, jelikož se jedná o zařízení ke kódování a přenos původně analogové zprávy, elektronickou pamětí 3 vysílače, ve které jsou umístěny kódovací paměťové registry 5, a kódovacím řídicím procesorem 4. Dále je tvořeno přijímačem 8 obsahujícím dekódovací příjmový převáděč 9, který je vybaven elektronickou pamětí 10 přijímače, d/a převodníkem 14 a dekódovacím řídicím procesorem 11. V elektronické paměti 3 vysílače je vytvořeno 256 kódovacích paměťových registrů 5 pro uložení souborů 6 zástupných kódů k nahrazování jednotlivých bytů obsažených v digitální podobě sdělovaného telefonního hovoru. V elektronické paměti 10 přijímače je vytvořen shodný počet dekódovacích paměťových registrů 12 pro uložení souborů 6 zástupných kódů identických se soubory 6 zástupných kódů uloženými v kódovacích paměťových registrech 5 vytvořených v elektronické paměti 3 vysílače. Kódovací řídicí procesor 4 je naprogramován k převedení hlasové zprávy pomocí a/d převodníku 13 z analogové podoby do podoby digitální a k postupnému nahrazování jednotlivých bytů tvořících digitální podobu sdělovaného telefonního hovoru prvním dosud nepoužitým unikátním zástupným kódem 7 ze souboru 6 zástupných kódů uloženém v těmto bytům přiřazených kódovacích paměťových registrech 5, zatímco dekódovací řídicí procesor 11 je naprogramován k vyhledání a spárování přijatých zástupných kódů 7 se zástupnými kódy 7 uloženými v jednotlivých dekódovacích paměťových registrech 12 elektronické paměti 10 přijímače a k jejich postupnému zpětnému převedení na jednotlivé jim odpovídající byty, které pak pomocí d/a převodníku 14 převede zpět do srozumitelného akustického signálu.

Pro objasnění obou uvedených příkladů slouží také obr. 3, jehož smyslem je příkladné znázornění obsahu a uspořádání kódovacího paměťového registru 5, resp. dekódovacího paměťového registru

12. Každý takovýto registr 5, 12 obsahuje soubor 6 zástupných kódů 7. Z jednotlivých zástupných kódů 7, jsou na obr. 3 vztahovou značkou kvůli přehlednosti označeny pouze náhodné zvolené dva. Každý zástupný kód 7 pak sestává z jednotlivých kódových znaků 7.1, které opět kvůli přehlednosti jsou názorně označeny pouze u jednoho (posledního) z nich. Taktéž v popisu prvního příkladu je na počet kódových znaků 7.1, tvořících jednotlivé použité zástupné kódy 7 poukázáno pouze u prvního takto použitého zástupného kódu 7 ve tvaru lovík. U všech ostatních použitých zástupných kódů 7 je již v závorce uveden pouze jejich tvar bez údaje o počtu kódových znaků 7.1.

Zařízení ke kódování a dekódování obrazových zpráv, coby dalšího druhu multimediálních zpráv, způsobem podle tohoto vynálezu, je konstrukčně stejné jako zařízení ke kódování a dekódování zvukových (hlasových) zpráv, akorát obsahuje podstatně vyšší počet kódovacích a dekódovacích paměťových registrů 5, 12.

15 Průmyslová využitelnost

Průmyslová využitelnost tohoto vynálezu je zřejmá z popisu jeho podstaty. Největší uplatnění bude mít nepochybně v armádě. Ale i ve strategických hospodářských odvětvích, jako je bankovníctví, energetika, telekomunikace, zbrojní průmysl, najde své uplatnění. Vzhledem k tomu, že zařízení k uskutečňování tohoto vynálezu nebude finančně nějak zvlášť náročné, lze předpokládat i mnohem širší uplatnění ochrany důvěrných zpráv způsobem podle tohoto vynálezu. Zařízení podle tohoto vynálezu je minimálně stejně bezpečné jako přenos zpráv kvantovým kódováním, avšak je neporovnatelně jednodušší, menší a levnější.

PATENTOVÉ NÁROKY

1. Způsob kódování a dekódování textových a multimediálních zpráv, zejména zpráv sdělovaných odesílatelem příjemci, poskytovaných informací a utajovaných zpráv, které jsou sestaveny ze zápisných znaků, to znamená písmen či slabik použité abecedy či použitých abeced případně z jiných symbolů použitých pro zápis textové zprávy nebo z bytů tvořících digitální záznam multimediální zprávy, **vyznačující se tím**, že každý jednotlivý zápisný znak v případě textových zpráv nebo byt v případě multimediálních zpráv, tvořící sdělovanou zprávu, se v pořadí shodném s jeho výskytem ve zprávě nahradí v pořadí prvním dosud nepoužitým zástupným kódem (7) ze souboru (6) zástupných kódů přiřazeného danému zápisnému znaku nebo bytu a tímto způsobem ze zástupných kódů (7) sestavená zpráva se odešle alespoň jednomu určenému příjemci, kde se obraceným postupem transformuje zpět do své původní textové nebo multimediální podoby.

2. Způsob kódování a dekódování textových a multimediálních zpráv podle nároku 1, **vyznačující se tím**, že po použití zástupného kódu (7) pro kódování zprávy se tento zástupný kód (7) označí jako použitý, aniž by se ze souboru (6) zástupných kódů vymazával, přičemž po použití a označení posledního zástupného kódu (7) z příslušného souboru (6) zástupných kódů se označení všech jeho zástupných kódů (7) jako použitých zruší a soubor (6) těchto zástupných kódů se aktivuje k opětovnému nahrazování příslušného zápisného znaku nebo bytu.

3. Způsob kódování a dekódování textových a multimediálních zpráv podle nároků 1 a 2, **vyznačující se tím**, že soubor (6) zástupných kódů je tvořen množinou vzájemně odlišných, na sobě nezávislých, v průběhu jednoho použití souboru (6) jednorázově použitelných unikátních zástupných kódů (7), sestavených z libovolného počtu jakkoliv kombinovaných kódových znaků (7.1) tvořených písmeny, slabikami a jinými symboly používanými jakýmkoliv abecedami, arabskými a/nebo římskými číslicemi nebo jakýmkoliv jinými znaky schopnými zápisu do elektronické paměti.

4. Způsob kódování a dekódování textových a multimediálních zpráv podle nároků 1, **vyznačující se tím**, že zápisnými znaky jsou písmena či slabiky příslušné abecedy případně příslušných abeced včetně příslušných diakritických znamének, interpunkční znaménka, a také číslice, matematická znaménka případně i jiné znaky používané k zápisům textových zpráv.

5. Zařízení k uskutečňování způsobu kódování a dekódování textových a multimediálních zpráv podle nároku 1, **vyznačující se tím**, že na straně odesílatele je tvořeno vysílačem (1) obsahujícím vysílací převáděč (2), který je vybaven elektronickou pamětí (3) vysílače a kódovacím řídicím procesorem (4) a v případě přenosu multimediálních zpráv tvořených analogovým signálem také a/d převodníkem (13) a na straně příjemce je tvořeno přijímačem (8) obsahujícím příjmový převáděč (9), který je vybaven elektronickou pamětí (10) přijímače a dekódovacím řídicím procesorem (11) a v případě příjmu multimediálních zpráv také d/a převodníkem (14), přičemž v elektronické paměti (3) vysílače jsou vytvořeny kódovací paměťové registry (5) z nichž každý je určen pro uložení souboru (6) zástupných kódů k nahrazování jednotlivých zápisných znaků nebo bytů, obsažených v textové nebo multimediální zprávě, a v elektronické paměti (10) přijímače je vytvořen shodný počet dekódovacích paměťových registrů (12) pro uložení souborů (6) zástupných kódů shodných se soubory (6) zástupných kódů uloženými v kódovacích paměťových registrech (5), přičemž kódovací řídicí procesor (4) je naprogramován a/nebo nakonfigurován k postupnému nahrazování jednotlivých zápisných znaků nebo bytů sdělované zprávy prvním dosud nepoužitým unikátním zástupným kódem (7) ze souboru (6) zástupných kódů uložených v těchto zápisných znakům nebo bytům přiřazených kódovacích paměťových registrech (5), zatímco dekódovací řídicí procesor (11) je naprogramován a/nebo nakonfigurován k postupnému vyhledání a spárování přijatých zástupných kódů (7) se zástupnými kódy (7) uloženými v jednotlivých dekódovacích paměťových registrech (12) a tím k jejich následnému zpětnému převedení na jednotlivé zápisné znaky nebo byty použité k původnímu zápisu textové nebo záznamu multimediální zprávy.

6. Zařízení podle nároku 5, **vyznačující se tím**, že počet kódovacích paměťových registrů (5) i počet dekódovacích paměťových registrů (12) je roven nejméně počtu jednotlivých zápisných znaků, které jsou použitelné k tvorbě textových zpráv v konkrétním použitém jazyce či jazycích nebo počtu bytů, včetně ukončovacího bitu, potřebných k tvorbě multimediálních zpráv.

5 7. Zařízení podle nároku 5, **vyznačující se tím**, že kódovací řídicí procesor (4) i dekódovací řídicí procesor (11) jsou naprogramovány nebo nakonfigurovány k tomu, aby každý zástupný kód (7) použitý k nahrazení zápisného znaku nebo bytu sdělované zprávy byl za účelem zamezení jeho opětovného použití jako použitý označen a zároveň tak, aby po použití a označení posledního zástupného kódu (7) z příslušného souboru (6) zástupných kódů se označení všech jeho
10 zástupných kódů (7) jako použitých zrušilo a soubor (6) těchto zástupných kódů se aktivoval k opětovnému nahrazování příslušného zápisného znaku nebo bytu.

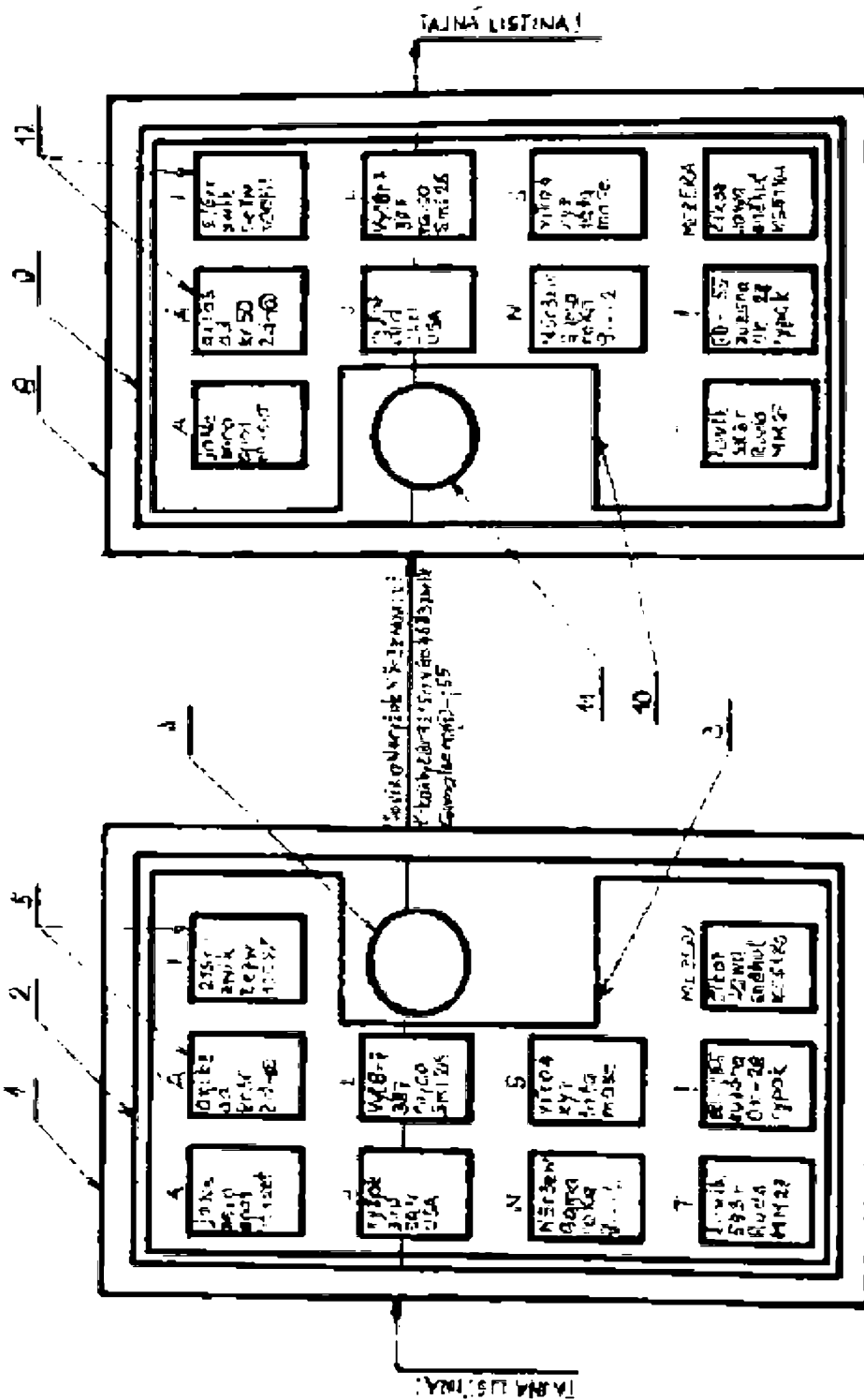
8. Zařízení podle nároku 5, **vyznačující se tím**, že jako vysílač (1) a přijímač (8) mohou být po instalaci příslušné aplikace použity běžné počítače, tablety, mobilními telefony nebo jiná elektronická zařízení tohoto druhu.

15

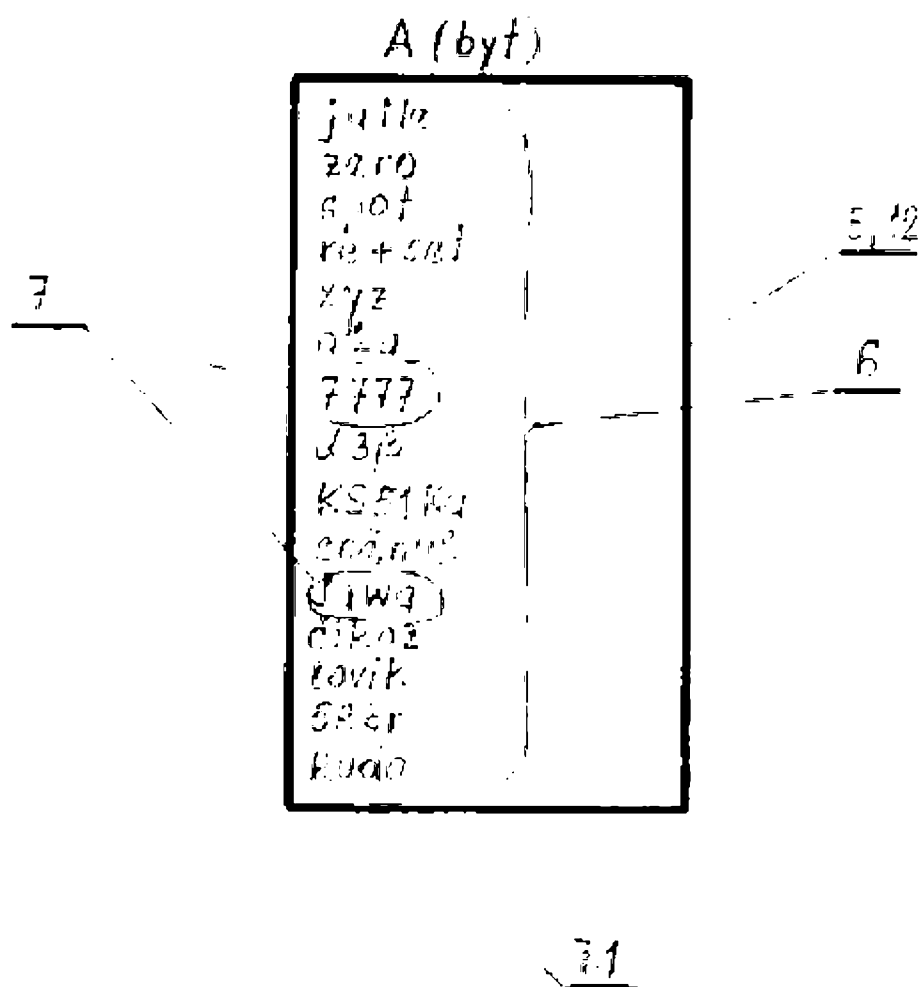
3 výkresy

Seznam vztahových značek:

- 1 - vysílač
- 2 - vysílací převáděč
- 3 - elektronická paměť vysílače
- 4 - kódovací řídicí procesor
- 5 - kódovací paměťový registr
- 6 - soubor zástupných kódů
- 7 - zástupný kód
- 7.1 - kódový znak
- 8 - přijímač
- 9 - příjmový převáděč
- 10 - elektronická paměť přijímače
- 11 - dekódovací řídicí procesor
- 12 - dekódovací paměťový registr
- 13 - a/d převodník (analogově digitální převodník)
- 14 - d/a převodník (digitálně analogový převodník)



Obr. 1



Obr. 3