PŘIHLÁŠKA VYNÁLEZU

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

(21) Číslo dokumentu:
2000 -4935

(13) Druh dokumentu: **A3**

(51) Int. Cl.[7]:
H 04 L 9/00

(19)
ČESKÁ
REPUBLIKA

ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

(22) Přihlášeno: **02.07.1998**

(32) Datum podání prioritní přihlášky: **01.07.1998**

(31) Číslo prioritní přihlášky: **1998/108312**

(33) Země priority: **US**

(40) Datum zveřejnění přihlášky vynálezu: **15.08.2001**
(Věstník č. 8/2001)

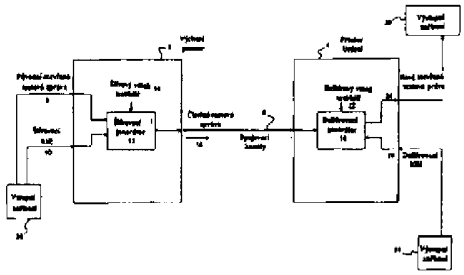
(86) PCT číslo: **PCT/US98/13626**

(87) PCT číslo zveřejnění: **WO00/02340**

(71) Přihlašovatel:
TECSEC, INCORPORATED, Vienna, VA, US;

(72) Původce:
Scheidt Edward M., McLean, VA, US;
Wack C. Jay, Clarksburg, MD, US;

(74) Zástupce:
PATENTSERVIS PRAHA a.s., Jivenská 1, Praha 4, 14000;



(54) Název přihlášky vynálezu:

Šifrovací spojovací systém a příslušné zařízení

(57) Anotace:

Spojovací systém zahrnuje výchozí prostor (2) a spojovací kanál (6), prostor (4) určení spojený s výchozím prostorem (2) pomocí spojovací kanálu (6). Výchozí prostor (2) zahrnuje šifrovací generátor (12) pro generování výstupního symbolu O_t založeného na vstupním symbolu I_t, dále zahrnuje prostředky pro příjem šifrovacího klíče a šifrový vztah (14) text/klíč a vstupní symbol. Prostor určení (4) zahrnuje dešifrovací generátor (18) pro generování dešifrovacího symbolu I'_t založeného na výstupním symbolu přijatého z výchozího prostoru přes spojovací kanál, a dále prostředky pro příjem dešifrovacího klíče (20) a šifrovacího vztahu (22) text/klíč. Šifrový vztah (14) text/klíč řídí šifrovací generátor tak, že $O_t=a_N(t)+p_N[\alpha_{N-1}(t)+\pi_{n-1}[a_{N-2}(t)+.....+p_2[a_1(t)+p_1[I_t+a_0(t)]]]]$, mod W, kde a_N, a_{N-1}.....a_1, a_0 jsou aditivní transformace definované šifrovacím klíčem kde $p_N,p_{N-1},.....p_1$, p_0 jsou N permutace definované šifrovacím klíčem, a kde W reprezentuje počet možností pro každou permutaci definovanou šifrovacím klíčem. Šifrový vztah (22) text/klíč řídí dešifrovací generátor (18) tak, že $I_t'=p_{1-1}[p_{2-1}[p_{31}.....[p_{n-1-1}[\pi_{N-1}[O_t-\alpha'_N(t)]-\alpha^{-N-1}.....\alpha'_3(t)-a'_2(t)]-\alpha'_1(t)]-a'_0(t)$, mod W, kde výraz π_{1-1} inverzní funkce permutace π_1, kde výrazy $a'_N,a'_{N-1},.....a'_1,\alpha'_0$ jsou N+1 aditivní transformace definované dešifrované dešifrovacím klíčem (20), a kde W představuje počet možností každé inverzní permutace definované dešifrovacím klíčem (20).

CZ 2000 - 4935 A3

Šifrovací spojovací systém a příslušné zařízení

Oblast techniky

Vynález se týká šifrovacích systémů. Vynález se zvláště týká systému sloužícího k zašifrování zpráv s otevřeným (nezašifrovaným) textem a k dešifrování zašifrovaných zpráv.

Dosavadní stav techniky

V moderním světě se spojení mezi zúčastněnými stranami realizuje různými způsoby, a to pomocí různých spojovacích médií. Elektronické spojení se stává stále populárnějším a efektivnějším prostředkem přenosu informací, zvláště pak se, jako bezprostřední médium spojení, prosazuje elektronická pošta.

Elektronické spojení má naneštěstí mnoho nedostatků, zvláště v oblasti privátních spojů. Elektronické spojení lze sledovat i nechtěnými příjemci. Bezdrátový přenos, například hovorové spojení pomocí voštinové (celulární) telefonní sítě, stejně jako elektronická pošta, je zvláště náchylný k zachycení nechtěnými příjemci.

Problém soukromého elektronického spojení již byl nastolen, a rovněž se již přistoupilo k hledání řešení tohoto problému. Jednou formou řešení je použít vhodný systém šifrování, který by elektronickému přenosu zpráv zajistil soukromí. Šifrovací systém zahrnuje zašifrování a dešifrování vyslaných a přijatých zpráv. Zpráva se obvykle vyskytuje ve formě digitálních signálů, nebo digitalizovaných analogových signálů. Jestliže je přenos zprávy neautorizovanou entitou zachycen a odposloucháván během přenosu, nebo je vybrán z paměti, je tímto způsobem získaná zpráva pro vetřelce, který nevlastní šifrovací a dešifrovací prostředky, zcela bezcenná.

U systémů, které šifrování používají, šifrující strana spojovacího procesu vlastní šifrovací zařízení nebo šifrovací generátor. Šifrovací zařízení přijímá otevřený text zprávy a šifrovací klíč, zprávu zašifruje pomocí zmíněného klíče a podle šifrovacích pravidel, které jsou předem pro přenos otevřeného textu a klíče stanoveny. Znamená to, že zpráva je klíčem upravena předem stanoveným způsobem, daným vztahem text/klíč, do formy číselného textu (zašifrovaného textu) zprávy.

Podobně platí, že dešifrovací strana spojení zahrnuje dešifrovací (dekódovací) zařízení nebo dešifrovací generátor. Dešifrovací zařízení přijímá číselný text a šifrovací klíč a dešifruje zprávu ve formě číselného textu, a to pomocí dešifrovacího klíče a podle

dešifrovacích pravidel, která jsou předem dána číselným textem zprávy a klíčem. Znamená to, že zpráva je klíčem upravena předem stanoveným způsobem, daným vztahem text/klíč, do formy nového otevřeného textu zprávy, který odpovídá původnímu otevřenému textu zprávy.

Způsob jakým je klíč a vztah aplikován v procesu spojení, a stejně jako způsob zvládnutí klíčů, definuje šifrovací plán nebo projekt. Existuje mnoho běžných šifrovacích projektů, které se v současnosti používají. Například nejpopulárnějším z nich je šifrovací projekt veřejného klíče. Podle tohoto projektu jsou používané klíče kombinací složky veřejného klíče, která je k dispozici každému, nebo velké skupině uživatelů, a složky soukromého klíče, která je specifickou pro konkrétní spojení.

Důležitou úvahou při stanovení, zda je konkrétní šifrovací projekt adekvátní dané aplikaci, je stupeň obtížnosti při pokusu rozluštit použitou šifru, to znamená velikost vynaloženého úsilí neautorizovanou osobou při snaze rozšifrovat zašifrovanou zprávu. Existuje celá řada možností jak se může neautorizovaná osoba vypořádat s problémem dešifrování. Tři nejpopulárnější způsoby „útoku" na systém šifrování zahrnují systém pokusu a omylu, dále diferenciální kryptoanalýzu a algebraický postup. Použití komplikovanějšího vztahu text/klíč a delšího klíče je rovněž cestou jak učinit šifrovací projekt méně zranitelný vůči napadení, přitom výsledkem je ale mnohem nákladnější systém pracující s menší rychlostí. Pokud nebude navržen chytřejší způsob šifrování, který by znemožnil úspěšnému napadení, je nutné při rozhodování o míře zachování soukromí přistoupit na jistý kompromis.

Jakmile se vybere určitý šifrovací systém, který může systém zefektivnit, a který vyhovuje daným omezením konkrétní aplikaci, vztah text/klíč se stává rozhodujícím faktorem úspěšnosti šifrovacího systému při obraně proti napadnutí. Správná volba systému u uživatelských stran rovněž posílí důvěru v to, že systém zůstane soukromým systémem.

Podstata vynálezu

Cílem tohoto vynálezu je poskytnout postup a zařízení k ochraně soukromí elektronického systém spojení.

Dalším cílem tohoto vynálezu je poskytnout postup a zařízení pro zašifrování a dešifrování digitálních dat.

Jedno provedení tohoto vynálezu zahrnuje spojovací systém, který dále zahrnuje výchozí prostor, spojovací kanál a prostor určení spojený s výchozím prostorem spojovacím kanálem. Výchozí prostor zahrnuje šifrovací generátor generující výstupní symbol O_t odvozený od vstupního symbolu I_t, a dále zahrnuje prostředky pro příjem šifrovacího klíče a pro šifrový vztah text/klíč a rovněž pro příjem vstupního symbolu. Prostor určení

zahrnuje dešifrovací generátor ke generování dešifrovaného symbolu I_t' odvozeného od výstupního symbolu přijatého z výchozího prostoru přes spojovací kanál, a dále zahrnuje prostředky pro příjem dešifrovacího klíče a dešifrového vztahu text/klíč. Šifrový vztah text/klíč řídí činnost šifrovacího generátoru tak, že $O_t = \alpha_N(t) + \pi_N[\alpha_{N-1}(t) + \pi_{n-1}[\alpha_{N-2}(t) + \ldots + \pi_2[\alpha_1(t) + \pi_1[I_t + \alpha_0(t)]]\ldots]]$, mod W, kde $\alpha_N, \alpha_{N-1} \ldots \alpha_1, \alpha_0$ jsou N+1 aditivní transformace definované šifrovacím klíčem, a kde W představuje počet možností každé permutace definované šifrovacím klíčem. Dešifrový vztah text/klíč řídí dešifrovací generátor tak, že $I_t' = \pi_1^{-1}[\pi_2^{-1}[\pi_3^{-1}\ldots[\pi_{n-1}^{-1}[\pi_N^{-1}[O_t - \alpha'_N(t)] - \alpha'_{N-1}(t)] - \ldots \alpha'_3(t) - \alpha'_2(t)] - \alpha'_1(t)] - \alpha'_0(t)$, mod W, kde výraz π_1^{-1} je definován dešifrovacím klíčem jako inverzní funkce permutace π_i, kde výraz $\alpha'_N, \alpha'_{N-1}, \ldots \alpha'_1, \alpha'_0$ N+1 aditivní transformace definované dešifrovacím klíčem, a kde W představuje počet možností každé inverzní permutace definované dešifrovacím klíčem.

Podle jednoho aspektu tohoto provedení šifrovací generátor dále zahrnuje W vyhledávací tabulky pro ukládání každé z možných W sad permutací. Podle jiného aspektu tohoto provedení, šifrovací generátor dále zahrnuje M<W vyhledávací tabulky pro ukládání M sad permutací předem vybraných z W sad permutací. Podle jiného aspektu tohoto provedení šifrovací generátor dále zahrnuje N<M <W vyhledávací tabulky pro uložení N sad permutací předem vybraných z dostupných M sad z možných W sad permutací. Podle jiného aspektu tohoto provedení je výraz $\alpha(t)$ krokovou funkcí. Podle jiného aspektu tohoto provedení , výraz $\alpha_x(t)$, X={0, 1, 2,..., N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu, kde t se rovná celému násobku hodnoty R, kde R je prvočíslo. Podle různých aspektů tohoto provedení výraz $a_x(t)$, X={0, 1, 2,.....N-1, N} snižuje sekvenci π_x pro každou hodnotu, kde t se rovná celému násobku R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení, výraz $\alpha_x(t)$, X={0, 1, 2,.....N-1, N} zvyšuje sekvenci π_x pro každou hodnotu t s výjimkou, kdy t se rovná celému násobku R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení , výraz $\alpha_x(t)$, X={0, 1, 2,..., N-1, N}, snižuje sekvenci π_x pro každou hodnotu t s výjimkou ,kdy t se rovná celému násobku hodnoty R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení hodnota I'_t odpovídá hodnotě I_t .

Jiné provedení tohoto vynálezu zahrnuje spojovací systém, který zahrnuje výchozí prostor, spojovací kanál a prostor určení spojený s výchozím prostorem zmíněným spojovacím kanálem. Výchozí prostor zahrnuje přijímač pro příjem vstupního symbolu I_t , šifrovací klíč a šifrový vztah text/klíč, šifrovací generátor ovládaný šifrovacím vztahem text/klíč, který slouží ke generování výstupního symbolu O_t založeného na vstupním symbolu tak, že $O_t = \alpha_N(t) + \pi_N[\alpha_{N-1}(t) + \pi_{n-1}[\alpha_{N-2}(t) + \ldots + \pi_2[\alpha_1(t) + \pi_1[I_t + \alpha_0(t)]]\ldots]]$, mod W, kde α_N ,

α_N^{-1}.....α_1 , α_0 jsou N+1 aditivní transformace definované šifrovacím klíčem, kde výrazy π_N , π_{N-1} , ...π_1 , π_0 jsou N permutace definované šifrovacím klíčem, a kde W reprezentuje počet možností pro každou permutaci definovanou šifrovacím klíčem. Prostor určení zahrnuje přijímač pro příjem dešifrovacího klíče a dešifrového vztahu text/klíč, dále dešifrovací aglomerát ovládaný pro generování dešifrovacího symbolu I'_t založeného na výstupním symbolu přijatého z výchozího prostoru přes spojovací kanál, a to tak, že $I_t' = \pi_1^{-1}[\pi_2^{-1}[\pi_3^{-1}.....[\pi_{n-1}^{-1}[\pi_N^{-1}[O_t - \alpha'_N(t)] - \alpha'_{N-1}(t)]-.....\alpha'_3(t)-\alpha'_2(t)]-\alpha'_1(t)]-\alpha'_0(t)$, mod W, kde výraz π_1^{-1} je definován dešifrovacím klíčem jako inverzní funkce permutace π_i , kde výrazy α'_N , α'_{N-1} , ...α'_1 , α'_0 jsou N+1 aditivní transformace definované dešifrovacím klíčem, a kde W představuje počet možností každé inverzní permutace definované dešifrovacím klíčem.

Podle jednoho aspektu tohoto provedení šifrovací generátor dále zahrnuje W vyhledávací tabulky pro ukládání každé z možných W sad permutací. Podle jiného aspektu tohoto provedení, šifrovací generátor dále zahrnuje M<W vyhledávací tabulky pro ukládání M sad, které jsou k dispozici z možných W sad permutací. Podle jiného aspektu tohoto provedení šifrovací generátor dále zahrnuje N<M <W, vyhledávací tabulky, pro uložení N sad permutací předem vybraných z dostupných M sad z možných W sad permutací. Podle jiného aspektu tohoto provedení je výraz $\alpha(t)$ krokovou funkcí. Podle jiného aspektu tohoto provedení , výraz $\alpha_x(t)$, X={0, 1, 2,..., N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu, kde t se rovná celému násobku hodnoty R, kde R je prvočíslo. Podle různých aspektů tohoto provedení, výraz $a_x(t)$, X={0, 1, 2,.....N-1, N} snižuje sekvenci π_x pro každou hodnotu, kde t se rovná celému násobku R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení, výraz $\alpha_x(t)$, X={0, 1, 2,.....N-1, N} zvyšuje sekvenci π_x pro každou hodnotu t s výjimkou, kdy t se rovná celému násobku R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení , výraz $\alpha_x(t)$, X={0, 1, 2,..., N-1, N}, snižuje sekvenci π_x pro každou hodnotu t s výjimkou, kdy t se rovná celému násobku hodnoty R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení hodnota I'_t odpovídá hodnotě I_t .

Jiné provedení tohoto vynálezu zahrnuje spojovací systém s prvním počítačem, dále zahrnuje spojovací kanál a druhý počítač spojený s prvním počítačem spojovacím kanálem. První počítač zahrnuje vstupní port symbolu pro příjem vstupního symbolu I_t , dále zahrnuje vstupní port šifrovacího klíče pro příjem šifrovacího klíče, dále zahrnuje první paměť sloužící k ukládání šifrového vztahu text/klíč a první mikroprocesor pro generování výstupního symbolu O_t založeného na vstupním symbolu a ovládaného šifrovacím vztahem text/klíč tak, že $O_t = \alpha_N(t) + \pi_N[\alpha_{N-1}(t) + \pi_{n-1}[\alpha_{N-2}(t) + ...+\pi_2[\alpha_1(t) + \pi_1[I_t + \alpha_0(t)]]....]]$, mod

W, kde α_N , α_{N-1} .....α_1 , α_0 jsou N+1 aditivní transformace definované šifrovacím klíčem, kde výraz π_N , π_{N-1} , ...π_1 , π_0 jsou N permutace definované šifrovacím klíčem, a kde W reprezentuje počet možností pro každou permutaci definovanou šifrovacím klíčem. Druhý počítač zahrnuje vstupní port dešifrovacího klíče pro příjem dešifrovacího klíče, dále zahrnuje druhou paměť sloužící k ukládání dešifrovací vztah text/klíč a druhý mikroprocesor pro generování dešifrovacího symbolu I'_t založeného na výstupním symbolu přijatého z výchozího prostoru přes spojovací kanál, a to tak, že $I_t' = \pi_1^{-1}[\pi_2^{-1}[\pi_3^{-1}.....[\pi_{n-1}^{-1}[\pi_N^{-1}[O_t - \alpha'_N(t)] - \alpha'_{N-1}(t)] - .....\alpha'_3(t) - \alpha'_2(t)] - \alpha'_1(t)] - \alpha'_0(t)$, mod W, kde výraz π_1^{-1} je definován dešifrovacím klíčem jako inverzní funkce permutace π_i , kde α'_N , α'_{N-1} , ...α'_1 , α'_0 jsou N+1 aditivní transformace definované dešifrovacím klíčem, a kde W představuje počet možností každé inverzní permutace definované dešifrovacím klíčem.

Podle jednoho aspektu tohoto provedení, první počítač dále zahrnuje W vyhledávací tabulky pro ukládání každé z možných W sad permutací. Podle jiného aspektu tohoto provedení, šifrovací generátor dále zahrnuje M<W vyhledávací tabulky pro ukládání M sad, které jsou k dispozici z možných W sad permutací. Podle jiného aspektu tohoto provedení šifrovací generátor dále zahrnuje N<M <W, vyhledávací tabulky, pro uložení N sad permutací předem vybraných z dostupných M sad z možných W sad permutací. Podle jiného aspektu tohoto provedení je výraz $\alpha(t)$ krokovou funkcí. Podle jiného aspektu tohoto provedení , výraz $\alpha_x(t)$, X={0, 1, 2,..., N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu, kde t se rovná celému násobku hodnoty R, kde R je prvočíslo. Podle různých aspektů tohoto provedení, výraz $a_x(t)$, X={0, 1, 2,.....N-1, N} snižuje sekvenci π_x pro každou hodnotu, kde t se rovná celému násobku R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení, výraz $\alpha_x(t)$, X={0, 1, 2,.....N-1, N} zvyšuje sekvenci π_x pro každou hodnotu t s výjimkou, kdy t se rovná celému násobku R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení , výraz $\alpha_x(t)$, X={0, 1, 2,..., N-1, N}, snižuje sekvenci π_x pro každou hodnotu t, s výjimkou ,kdy t se rovná celému násobku hodnoty R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení hodnota I'_t odpovídá hodnotě I_t .

Tento vynález dále zahrnuje postup spojení mezi výchozím prostorem a prostorem určení. Postup zahrnuje příjem vstupního symbolu I_t ve výchozím prostoru a generování výstupního symbolu O_t založeného na vstupním symbolu a ovládaného šifrovacím vztahem text/klíč tak, že $O_t = \alpha_N(t) + \pi_N[\alpha_{N-1}(t) + \pi_{n-1}[\alpha_{N-2}(t) + ...+\pi_2[\alpha_1(t) + \pi_1[I_t + \alpha_0(t)]]....]]$, mod W, kde α_N , α_{N-1} .....α_1 , α_0 jsou N+1 aditivní transformace, kde výraz π_N , π_{N-1} , ...π_1 , π_0 jsou N permutace, a kde W reprezentuje počet možností pro každou

permutaci. Výstupní symbol je přijat v prostoru určení a generuje se dešifrovaný symbol I'_t založený na přijatém výstupním symbolu tak, že $I_t' = \pi_1^{-1}[\pi_2^{-1}[\pi_3^{-1}.....[\pi_{n-1}^{-1}[\pi_N^{-1}[O_t - \alpha'_N(t)] - \alpha'_{N-1}(t)] - .....\alpha'_3(t) - \alpha'_2(t)] - \alpha'_1(t)] - \alpha'_0(t)$, mod W, kde výraz π_1^{-1} je definován jako inverzní funkce permutace π_i, kde výrazy α'_N, α'_{N-1}, $.....\alpha'_1$, α'_0 jsou N+1 aditivní transformace, a kde W představuje počet možností každé inverzní permutace.

Podle dalšího aspektu zmíněného postupu jsou možné W sady permutací získány z W vyhledávacích tabulek, a to ještě před generováním výstupního symbolu. Podle dalšího aspektu zmíněného postupu jsou přístupné M sady možných W sad permutací získány z M<W vyhledávacích tabulek, a to ještě před generováním výstupního symbolu. Podle dalšího aspektu zmíněného postupu jsou N sady permutací, předem vybrané z přístupných M sad možných W sad permutací, získány z N<M<W vyhledávacích tabulek, a to ještě před generováním výstupního symbolu. Podle jiného aspektu tohoto postupu je výraz $\alpha(t)$ krokovou funkcí. Podle jiného aspektu tohoto postupu , výraz $\alpha_x(t)$, X={0, 1, 2,..., N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu, kde t se rovná celému násobku hodnoty R, kde R je prvočíslo. Podle jiného aspektu tohoto postupu výraz $a_x(t)$, X={0, 1, 2,.....N-1, N} snižuje sekvenci π_x pro každou hodnotu, kde t se rovná celému násobku R, kde R je prvočíslo. Podle jiného aspektu tohoto postupu výraz $\alpha_x(t)$, X={0, 1, 2,.....N-1, N} zvyšuje sekvenci π_x pro každou hodnotu t s výjimkou, kdy t se rovná celému násobku R, kde R je prvočíslo. Podle jiného aspektu tohoto postupu výraz $\alpha_x(t)$, X={0, 1, 2,..., N-1, N}, snižuje sekvenci π_x pro každou hodnotu t, s výjimkou ,kdy t se rovná celému násobku hodnoty R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení hodnota I'_t odpovídá hodnotě I_t

Jiné provedení tohoto vynálezu zahrnuje magnetickou paměť, která zahrnuje interface, a dále ovladač sloužící prostřednictvím interface k ovládání mikroprocesoru, a to za účelem generování výstupního symbolu O_t tak, že $O_t = \alpha_N(t) + \pi_N[\alpha_{N-1}(t) + \pi_{n-1}[\alpha_{N-2}(t) + ...+\pi_2[\alpha_1(t) + \pi_1[I_t + \alpha_0(t)]]....]]$, mod W, kde I_t je vstupní symbol, a kde α_N, α_{N-1} $.....\alpha_1$, α_0 jsou N+1 aditivní transformace definované klíčem, kde výrazy π'_N, π'_{N-1}, $.....\pi'_1$, π'_0 jsou N permutace definované klíčem, a kde W reprezentuje počet možností pro každou permutaci definovanou klíčem.

Podle dalšího aspektu tohoto provedení Podle jiného aspektu tohoto provedení je výraz $\alpha(t)$ krokovou funkcí. Podle jiného aspektu tohoto provedení , výraz $\alpha_x(t)$, X={0, 1, 2,..., N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu, kde t se rovná celému násobku hodnoty R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení, výraz $a_x(t)$, X={0, 1, 2,.....N-1, N} snižuje sekvenci π_x pro každou hodnotu, kde t se rovná celému násobku R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení, výraz $\alpha_x(t)$, X={0, 1, 2,.....N-1,

N} zvyšuje sekvenci π_x pro každou hodnotu t s výjimkou, kdy t se rovná celému násobku R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení , výraz α_x (t), X={0, 1, 2,..., N-1, N}, snižuje sekvenci π_x pro každou hodnotu t, s výjimkou ,kdy t se rovná celému násobku hodnoty R, kde R je prvočíslo.

Jiné provedení tohoto vynálezu zahrnuje magnetickou paměť, která zahrnuje interface a ovladač sloužící prostřednictvím interface k ovládání mikroprocesoru za účelem výroby generovaného I'_t tak, že $I_t' = \pi_1^{-1}[\pi_2^{-1}[\pi_3^{-1}.....[\pi_{n-1}^{-1}[\pi_N^{-1}[O_t - \alpha_N(t)] - \alpha'_{N-1}(t)] - .....\alpha'_3(t) - \alpha'_2(t)] - \alpha'_1(t)] - \alpha'_0(t)$, mod W, kde O_t je přijatý symbol, kde výrazy α'_N , α'_{N-1} , $.....\alpha'_1$, α'_0 jsou N+1 aditivní transformace definované klíčem, kde výraz $\pi_1^{-1} ... \pi_N^{-1}$ jsou N inverzní permutace definované klíčem, kde W představuje počet možností každé inverzní permutace definované klíčem.

Podle jiného aspektu tohoto provedení je výraz α(t) krokovou funkcí. Podle jiného aspektu tohoto provedení , výraz α_x (t), X={0, 1, 2,..., N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu, kde t se rovná celému násobku hodnoty R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení výraz a_x (t), X={0, 1, 2,.....N-1, N} snižuje sekvenci π_x pro každou hodnotu, kde t se rovná celému násobku R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení výraz α_x (t), X={0, 1, 2,.....N-1, N} zvyšuje sekvenci π_x pro každou hodnotu t s výjimkou, kdy t se rovná celému násobku R, kde R je prvočíslo. Podle jiného aspektu tohoto provedení výraz α_x (t), X={0, 1, 2,..., N-I, N}, snižuje sekvenci π_x pro každou hodnotu t, s výjimkou ,kdy t se rovná celému násobku hodnoty R, kde R je prvočíslo.

Přehled obrázků na výkrese

Tyto a jiné cíle, znaky a výhody tohoto vynálezu se ozřejmí pomocí podrobného popisu, který zahrnuje preferovaná provedení, která však vynález nijak nelimitují. Popis je doplněn výkresy, na kterých:

obr.1 znázorňuje blokový diagram spojení s použitým šifrováním,

obr.2 znázorňuje blokový diagram implementace vztahu text/klíč podle tohoto vynálezu.

Příklady provedení vynálezu

Podle obr.1 spojení zahrnuje výchozí prostor 2 a prostor určení 4. Výchozí prostor 2 definuje místo a čas počátku spojení. Prostor určení 4 definuje místo a čas dešifrování (snahy o dešifrování). Výchozí prostor 2 a prostor určení 4 mohou být od sebe vzdálené. Alternativně

mou být umístěné ve stejném místě, ale mohou být oddělené časově. Prostorový a časový vztah mezi výchozím prostorem 2 a prostorem určení 4 závisí na charakteru konkrétního spojení. Výchozí prostor 2 je s prostorem určení 4 spojen společným spojovacím kanálem 6. Tento spojovací kanál 6 může přemosťovat fyzický prostor, například prázdný prostor v případě celulárního (voštinového) telefonického hovoru. Alternativně může být spojovacím kanálem dočasná paměť spojení v době, kdy čas mezi výchozím prostorem 2 a prostorem určení 4 běží , takže zprávu uloženou v paměti na počítači prvního uživatele a určenou pro druhého uživatele, si druhý uživatel může později přečíst na stejném počítači. Spojovacím kanálem 8 může být, v případě přenosu elektronické pošty, kombinace telefonního kabelu a paměti.

Ve výchozím prostoru 2 je původní otevřená zpráva 8 přijata a zašifrována podle šifrovacího vztahu text/klíč 14, a to šifrovacím klíčem 10, s cílem vytvořit zašifrovaný číselný text 16. Zpráva ve formě číselného textu 16 je v prostoru určení 4 přijata prostřednictvím spojovacího kanálu 6. Autorizovaná entita vyzbrojená správným dešifrovacím klíčem 20 tento klíč poskytne prostoru určení 4, kde se použije u číselného textu 16, a to podle šifrového vztahu text/klíč 22, k vytvoření nové otevřené zprávy 24, která odpovídá původní otevřené zprávě 8.

Výchozím prostorem 2 a prostorem určení 4 může být například počítač, dokonce stejný počítač. Vzorový počítač může mít několik paměťových prostorů ve formě paměti, sloužících k ukládání vztahu text/klíč. Mikroprocesor, nebo jiný ovladač může být, spolu s řídící strukturou a pamětí s náhodným přístupem RAM k uložení původního otevřeného textu,a dále s klíčem uživatele, součástí každého prostoru a může realizovat funkce šifrovacího/dešifrovacího generátoru.. Vstupní zařízení 26, 28, například klávesnice, disketová jednotka a CD-ROM jednotka, biometrické čtecí zařízení, nebo zařízení ke čtení modálních funkcí zdroje viditelného světelného signálu, slouží pro příjem klíče a otevřené zprávy od výchozího uživatele a klíče od uživatele v prostoru určení. V prostoru určení 4 se nachází výstupní zařízení 30, například monitor, disková jednotka, hlasový reproduktor, které poskytuje uživateli v prostoru určení novou otevřenou zprávu. Vztah text/klíč lze uložit na disketu nebo jinou přenosnou paměť, a to spíše než na disk počítače, aby se tím umožnila aplikace různých vztahů text/klíč různými uživateli, nebo v různých situacích.

Vztah text/klíč, podle tohoto vynálezu, založený na prokládaném vztahu počtu N permutací společně s počtem N+1 aditivních transformací. V případech, kdy vstupní spojení je zašifrováno do bloků, výstupní otevřená zpráva $\mathbf{I}_t$, složená z t bloků, se dešifruje vzhledem

ke zmíněnému vztahu, a vytvoří se výstupní číselný text zprávy $\mathbf{O}_t$, Permutace, počáteční hodnoty aditivních transformací a jiné parametry vztahu text/klíč jsou určeny klíčem.

Obr.2 znázorňuje přiřazení, podle vztahu text/klíč, které vytváří výstupní symbol $\mathbf{O}_t$ ze vstupního symbolu $\mathbf{I}_t$:

$\mathbf{O}_t = Ft(\mathbf{I}_t) = \alpha_N(t) + \pi_N[\alpha_{N-1}(t) + \pi_{n-1}[\alpha_{N-2}(t) + \ldots\ldots + \pi_2[\alpha_1(t) + \pi_1[\mathbf{I}_t + \alpha_0(t)]]\ldots.]]$, mod W,

kde α_N , α_{N-1} $\ldots\ldots\alpha_1$, α_0 jsou N+1 doplňkové (aditivní) transformace , a kde výrazy π_N , π_{N-1} , $\ldots\ldots\pi_1$, π_0 jsou N permutace, a kde W reprezentuje počet možností pro každou permutaci. Znamená to, že vstupní symbol $\mathbf{I}_t$ je modulo-W přidaní k $\alpha_0(t)$, a výsledek se vyhledá v tabulce permutací π_1 . Výstupem z π_1 vyhledávání je modulo –W přidané k $\alpha_1(t)$ atd. Toto přiřazení vstupního symbolu $\mathbf{I}_t$ v kroku **t** se používá ke generování výstupního symbolu $\mathbf{O}_t$.

Odpovídající dešifrovací operace F_t^{-1} vyžaduje, aby vstupní symbol $\mathbf{I}_t$ v kroku **t** byl odvozen z výstupního symbolu $\mathbf{O}_t$. Dosahuje se toho následovně:

$\mathbf{I}_t = F^{-1}(\mathbf{O}_t) = \pi_1^{-1}[\pi_2^{-1}[\pi_3^{-1}\ldots\ldots[\pi_{n-1}^{-1}[\pi_N^{-1}[\mathbf{O}_t - \alpha_N(0)] - \alpha_{N-1}(t)] - \ldots\ldots\alpha_3(0) - \alpha_2(0)] - \alpha_1(0)] - \alpha_0(0)$, mod W, kde $\pi^{-1}{}_i$ je inverze permutace π_i .

Znamená to že $\alpha_N(0)$je modulo W odečteno od výstupního symbolu $\mathbf{O}_t$ a výraz je vyhledán v tabulce permutací π_N^{-1}. Výsledek vyhledávání $\alpha_{N-1}(0)$ je modulo –W odečtené od tohoto výsledku a vyhledané v π_{N-1}^{-1}, atd.

Permutace π_1 , π_2 ……, π_{N-1} , π_N se berou v prostoru O-W, s výsledkem ve W! možnostech pro π. Pro praktické účely lze pro uživatele zpřístupnit menší počet M z W! možných tabulek pro π, a menší počet N lze vybrat pro konkrétní periodu šifrování, a to s konkrétními N tabulkami založenými na informacích v klíči. Jakmile se najdou N permutace, počáteční body pro aplikaci každé permutace jsou dány informacemi v klíči.

Aditivní transformace α_0 , α_1 ,…….α_{N-1} , α_N jsou hodnoty určující po jakých krocích se budou permutace vyskytovat před tím, než bude vyhledána následující hodnota permutace. Přírůstková funkce poskytnutá aditivními transformacemi může být načítána jako závislá nebo hodnotově závislá. Například načítaná závislá aditivní transformace se může použít pro přidávání sekvence následujících tabulek permutace, a to jedním umístěním vždy R krát v průběhu šifrovacího postupu, kde R je velké prvočíslo. Jiná načítaná závislá aditivní transformace se může použít pro přidání sekvence následující tabulky permutace, a to jedním umístěním vždy J krát v průběhu šifrovacího postupu, kde J je jiné velké prvočíslo. Jiná načítaná závislá aditivní informace se může použít pro pozastavení , to znamená, přidáním sekvence následující tabulky permutace jedním umístěním kdykoliv během šifrovacího

postupu, ale s výjimkou vždy L krát během postupu, kde L je jiné velké prvočíslo. Hodnotově závislá aditivní transformace může přidat sekvenci následující tabulky permutací podle hodnoty předchozího výstupu, například výstupu z předchozí tabulky permutací, nebo předchozího symbolu. Tato hodnota se dá použít nejen pro stanovení, zda následující sekvence bude přírůstkovou sekvencí, ale i pro stanovení rozsahu přírůstku.

Jako nelimitujícím příklad bude popsán konkrétní vztah text/klíč s osmi permutacemi a devíti aditivními transformacemi. Je provedeno osm permutací $\Pi = \pi_1, \pi_2, \pi_3, \pi_4 \ldots \ldots \pi_8$, na symbolech 0, 1, 2, až 255 z 256 bloku symbolů původní otevřené zprávy. V tomto, případě je vybráno osm permutací z uložené sady 25 permutací, a jsou určeny například prvními osmi symboly v šifrovacím klíči. Devět aditivních transformací použitých v kroku t je označeno jako $A(t) = \alpha_0(t), \alpha_1(t), \ldots\ldots\alpha_7(t), \alpha_8(t)$. Počáteční hodnota při t=0 je stanovena například devíti symboly v šifrovacím klíči. Na konci každé aplikace vztahu text/klíč, a to v tomto případě, aditivní transformace A(t) jsou modifikovány determinačně, ale osm vybraných permutací zůstává na místě tak dlouho, dokud se nezmění klíč. Postup změny A(t) se pro různé režimy vztahu text/klíč mění.

Vzorový postup změny A(t) je popsán níže jako část blokového šifrového režimu. $S(t) = S_4(t), S_3(t), S_2(t), S_1(t)$ představuje vstupní otevřený text 4 symbolů v čase t, který se má zašifrovat. Počáteční hodnota otevřeného textu v čase i=0 je vstupní slovo 4 symbolů

$$\mathbf{I}(0) = \mathbf{I}_4(0), \mathbf{I}_3(0), \mathbf{I}_2(0), \mathbf{I}_1(0); \; S_j(0) = \mathbf{I}_j(0), j = 1, \text{až } 4$$

Pro i = 0 až 15 (16 šifrovacích kola je v tomto případě použito na každý blok dat) S(t+1) lze vypočítat například ze stavu S(t) následovně:

$S_4(t+1) = F_t(S_1(t))$,
$S_3(t+1) = S_4(t+1)$,
$S_2(t+1) = S_3(t+1)$
$S_1(t+1) = F_t(S_1(t)) + S(t)$

Kde F_t je t-tou funkcí definovanou pomocí Π a funkce $A(t) = \alpha_0(t), \alpha_1(t), \ldots\ldots\alpha_7(t), \alpha_8(t)$ a je generována následujícím způsobem:

Dané výrazy Π, A(0) a X(4), X(3), X(2), X(1), které se používají ke generování funkce A(t), T=1, 2, 3,....16 z klíče, se použijí k výpočtu výstupních slov 364-symbolů šifrových bloků. Během tohoto celého postupu se ve vztahu text/klíč se používá nastavení A(0) z klíče, které se nemění.

Tím se vytváří celkové množství 144 symbolů, které se následně rozdělí do 169 sekvencí symbolů A(1) až A(16) následujícím způsobem:

A(1)= prvních devět výstupních symbolů

A(2)= druhých devět výstupních symbolů

až

A(16)= Posledních devět výstupních symbolů

Výpočet A(1), A(2) až A(16) se přednostně realizuje v době zavedení klíče. Děje se tak proto, aby se postup maximálně urychlil a minimalizovaly se požadavky na paměť.

Výstup zašifrovaného textu v čase t=16 je výstupem **O**(0), šifrová transformace bloku vstupního slova **I**(0), to je

$S(16) = S_4\ (16), S_3\ (16), S_2\ (16), S_1\ (16) = \mathbf{O}(0) = \mathbf{O}_4\ (0), \mathbf{O}_3\ (0), \mathbf{O}_2\ (0), \mathbf{O}_1\ (0)$

Sekvence A(1), A(2) až A(16) jsou sadou aditiv použitých definování šestnácti permutací k zašifrování v blokovém šifrovém režimu. Pro dešifrování výstupu se používají inverzní permutace a aditiva, a to v obráceném pořadí, to znamená v pořadí A(16), A(15) až A(1).

Bezpečnost blokového šifrového režimu je založena na bezpečnosti vztahu text/klíč a kryptoanalytických odporových třídicích vlastnostech (cryptanalytic resistant mixing properties) opakovaných nelineárních zpětnovazebních funkcí . Vztah text/klíč je permutací symbolu sestávající z produktu N náhodně vybraných permutací, které jsou vybrány se sady M permutací, které jsou vybrány z plné sady W! permutací W prvků. N permutace se mění podle deterministického (ale neznámého) pravidla, a to s každou aplikací funkce. I když se do vztahu text/klíč, během dvou různých cyklů v rámci zpracování jednoho bloku, zavedly stejné symboly, permutace aplikovaná u takového symbolu bude stejná pouze s pravděpodobností 1/W Minimalizuje se tím nejistota u celkového počtu cyklů blokové šifry.

Použití vztahu text/klíč v tomto systému je velmi těžké napadnout. Vstupy mají náhodné složky a jsou omezeny délkově. Výstupy jsou omezeny podskupinou bitů z výsledného výstupu pevné délky. Nikdo by proto neměl přizpůsobovat vstupní-výstupní slova, která jsou běžně potřebná k analýze vztahu tak složitého, jako je bloková šifra podle tohoto vynálezu. Jelikož se klíč může měnit periodicky, například každých 30 minut a pod, počet vstupů zpracovávaných jedním klíčem je omezen. Neúplná podstata pozorovatelného funkčního vztahu spojeného s relativně malým počtem funkčních hodnot způsobuje, že provést kryptoanalýzu blokové šifry, podle tohoto vynálezu, je velmi obtížné.

Počet cyklů (například 16) zpracování, v jednom režimu šifrového bloku, se může vybrat tak, aby se maximalizovalo nelineární setřiďování obsahu registru. Tím se zajistí, aby

se data v každém registru se zpracovávala podle vztahu text/klíč vícekrát. Například symbol, který se nachází původně v prvním stupni, se zpracovává podle vztahu text/klíč v každém ze šestnácti cyklů zpracování, zatímco symbol nacházející se ve čtvrtém stupni registru, a je posledním zpracovávaným symbolem, se bude zpracovávat dvanáctkrát. Obsah každého stupně registru šifrového bloku je včleněn do jiného stupně, nelineární funkce, týkající se výstupu, do vstupu.

Uspořádání zpětné vazby vyúsťuje do alespoň dvou prospěšných jevů. Zaprvé, lineární prvek redukuje jakoukoliv určitost, která může být přítomna. Zadruhé, umístění zpětné vazby rychle přináší rozdíly do nelineárního posouvacího registru a drží je zde, jakmile se jednou objeví, a to s pravděpodobností rovnající se tomu, co se považuje za nahodilé. Jakmile se ve stupni 1 předloží ke zpracování odlišný symbol, vztah text/klíč umístí rozdíl do stupně 4 registru v příštím kroku s jistotou a pravděpodobnostně tento rozdíl vloží do stupně 1 zmíněného registru. Jeden rozdíl ve stupni 1 registru vykazuje účinek v tom, že se s velkou pravděpodobností sám znásobí, a to v příštím kroku zpracování šifrového bloku. Kromě toho zde vždy existuje možnost zrušení, přitom se ale, ve vybraném uspořádání šifrového bloku, taková možnost, že se to stane, rovná nahodilosti. Při počáteční m uspořádání registru ve formě DSSS, dva rozdílné časové úseky, ve kterých počáteční stavy stupně 4 registru obsahují symboly, které se liší, zatímco další tři stupně registru mají stejný obsah. Uspořádání vykazuje, před aplikací vztahu text/klíč, maximální zpoždění. Jelikož každý krok vztahu text/klíč je permutací,a to v šestém kroku zpracování šifrového bloku , obsah registru je DDDD s pravděpodobností p=1. V kroku 10 postupu je obsah registru SSSS s pravděpodobností pouze $(1/2)^{32}$, což se považuje za nahodilost. Existuje však ještě 6 kroků, které musí proběhnout, než se dosáhne výstupní hodnoty. Jakékoliv jiné počáteční vstupní uspořádání vnese do postupu rozdíly ještě dříve. Tato konstrukce je odolná vůči diferenčním kryptoanalytickým technikám

Jestliže například existuje celkově W=156! permutací 256 prvků, ze kterých se vybírá M=25 základních permutací systému, počet sad 25 základních permutací činí přibližně $W^{25}/M!$, což je enormní množství. I když považujeme sadu permutací za známou, i tak je počet klíčů velmi velký. Pokud se vybere 8 permutací z 25 permutací s náhradou, počet možných sad permutací se rovná přibližně $25^8 = 10^{11}$. Nyní je 16 lineárních aditiv, nutných pro šifrový blok, generováno šifrovým blokem , který operuje na neznámém 32 bitovém počátečním stavu registru s pevnou neznámou aditivou definovanou sekvencí 27 bitů . Poskytuje to další možnosti s hodnotou $2^{104}=10^{31}$. Celkový klíčový prostor pro známou sadu 25 permutací je řádově na hodnotě 10^{42}. Toto je klíčový prostor, který je dostatečně velký

k tomu, aby zamezil vyčerpávající hledání klíče v příštím století, a rovněž k tomu, aby odolával jiným zkratovým kryptoanalytickým útokům.

Kromě výběru základní sady permutací na 256 prvcích , ze které by se měly klíčové proměnné vybírat, existuje řada variant šifrového bloku, které jsou pro potvrzování pravosti jedinečné. Každá z těchto variant má dopad jak na výkonnost, tak i na bezpečnost. Například délku nelineárního registru lze měnit tak, aby mohl pojmout delší nebo kratší výzvy. Nelineární zpětná vazba do registru se může změnit, čímž se získá variabilita. Technika generování sady aditiv během zpracovávání šifrového bloku se může měnit tak, že je nezávislá na samotném režimu šifrového bloku..

Pro objasnění myšlenky silného režimu šifrového bloku vztahu text/klíč, budou probrány tří z nejpopulárnějších způsobů napadení, které lze najít ve světové kryptoanalytické literatuře. Tyto způsoby jsou: vyčerpání klíče nebo napadení cestou pokusu a omylu, diferenční kryptoanalýza a algebraické napadení. Délka nelineárního registru se může změnit tak, aby obsáhl delší nebo kratší výzvy. Nelineární zpětnou vazbu do registru lze měnit z důvodu získání variability. Techniku generování sady aditiv během zpracovávání šifrového bloku lze měnit tak, aby neměla k samotnému režimu šifrového bloku žádný vztah.

Pro vysvětlení síly režimu šifrového bloku vztahu text/klíč, budou prodiskutovány tři nejobvyklejší způsoby napadení, které lze nalézt ve světové kryptoanalytické literatuře. Těmito způsoby jsou : vyčerpání klíče nebo napadení cestou pokusu a omylu, diferenční kryptoanalýza a algebraické napadení.

Vyčerpání klíče je brutálním silovým způsobem, u kterého se generuje jakákoliv možná kombinace bitů jako potenciální klíč, přitom se tyto kombinace aplikují na systém, a to s cílem náhodného získání platného klíče. Existuje zde 25 x 24 x 23 x 22 x 21x 20 x 19 x 18 = 43 609 104 000 = 10^{1064} možných výběrů pro pět permutací π_1 , π_2 .....π_8 , a déle existuje $256^9 = 10^{21.67}$ možných výběrů pro devět symbolů A(0) pro počáteční aditivní transformaci. Konečně existuje $256^4 = 10^{9.63}$ možných výběrů pro počáteční naplnění klíče, X(1), X(), X(), X(4) použitých pro vývoj A(t), t=1, 2, 3, ...16.

Rozmanitost klíče nebo mohutnost prostoru klíče se rovná $10^{10.64+21.67+9.63} = 10^{41.94}$. Pokud by se u způsobu pokusu a omylu někdo pokusil použít všechny možné klíče, potom by mohl očekávat, že k dosažení správného klíče by v průměru mohlo dojít již v polovině postupu, nebo po $10^{41.64}$ pokusech. Takový způsob napadení by byl nepraktický, a kromě toho, při použití správné technologie by tento způsob napadení nebyl dokončen ani v průběhu jednoho století. Jestliže je klíč definován jako platný pouze pro pevně stanovenou dobu, například pro 30 minut, vyčerpání klíče by se s velkou pravděpodobností nemohlo realizovat.

Pravděpodobně nejpopulárnějším způsobem kryptoanalytického napadení v dnešní době je diferenciální kryptoanalýza. Základní myšlenkou napadení je porovnávání zašifrované verze dvou (nebo více) vstupních slov, které se od sebe velmi málo liší, a to za předpokladu, že rozdíly na výstupu by mohly záviset na podmnožině klíče, nebo snad na příbuzném klíči s malou odlišností.

Následující nejlepší scénář případu by mohl napadající předvídat:

1. Vybrat pár 32 bitových vstupních slov, které se liší pouze v jednom bitu.
2. Pro každý ze 16-ti kroků v šifrovém bloku porovnat výsledky získané po každém kroku.
3. Najít vztah mezi těmito rozdíly a konkrétními výběry pro 21 symbolů klíče.

V prvních osmi krocích lze pozorovat deterministické rozdíly, které by mohly mít vztah k výběrům klíče. Po devíti ze 16-ti kroků nemůže být rozdílová vzorek z nahodilého výběru 2^{32} možných rozdílových vzorku rozpoznán. Po těchto devíti krocích má algoritmus ještě sedm kroků před sebou, a to než je generován výstup, jehož výsledky by kryptoanalytik mohl použít u jakéhokoliv testování. Zmíněných sedm kroků dále transformuje rozdílové vzorky. Je proto velmi nepravděpodobné, že tento způsob napadení bude mít úspěch.

Výsledek by nebyl lepší ani pro algebraické napadení. Jestliže jsou permutace zapsány ve formě matice permutací, potom výsledkem jsou 0, 1 matice s jednou hodnotou v každé řádce a v každém sloupci. V algebraické reprezentaci vztahu text/klíč, podle tohoto vynálezu, se matice násobí v různých kombinacích s aditivními transformacemi. Výsledkem je, že algebraickým výrazem pro jednotlivé přiřazení vstupu/výstupu je osmý stupeň polynomu. Pro režim šifrového bloku má algebraický výraz výstupu, z hlediska vstupu, vysoký stupeň a je mnohem složitější. I kdyby někdo mohl najít způsob řešení systému s vysokým stupněm polynomů, rovnice režimu šifrového bloku by se prakticky nedala vyřešit.

Jednou praktickou aplikací šifrovacího systému, podle tohoto vynálezu, je systém nazvaný Identification Friend or Foe (IFF – identifikace přítele nebo nepřítele). U takového systému je cíl identifikován a dotazován zašifrovaným dotazovacím signálem. Pokud je cíl přátelský, je vybaven převaděčem, který je schopný dešifrovat zmíněný dotaz, číst informaci obsaženou v dotazu a na základě informace generovat zašifrovanou odpověď pro přenos k žadateli. Jestliže tazatel obdrží správnou odpověď ve správném okně odezvy, odpověď je považována za správnou a cíl je identifikován jako přátelský cíl. Pokud se nepřijme platná odpověď, cíl je považován za nepřátelský cíl.

Protože jsou zašifrované signály přenášeny mezi tazatelem a převaděčem, musí mít oba platný klíč, nebo sadu platných klíčů, jestliže se výměna klíčů realizuje periodicky. V následujícím příkladu jsou klíče z bezpečnostních důvodů měněny každých 30 minut. Každý tazatel a převaděč musí mít 48 klíčů pro každou denní misi. Každý ze 48 klíčů, které denně vstupují do zařízení IFF, představuje 21 symbolů K_1 , K_2 , K_3 , Ö $K_{2\,1}$, které se v tomto příkladu používají následovně:

K_1 , K_2 , K_3 ,.....$K_8 = \pi_1$, π_2 , π_3 ... ...π_8

K_9 , $K_{1\,0}$, $K_{1\,1}$ ....$K_{1\,7} = \alpha_0$ (t), α_1 (t),.....α_7 (t), α_8 (t)

$K_{1\,8}$,.....$K_{2\,1}$ = X(1), X(2), X(3), X(4),

Každý klíč je vložen do zařízení, vypočítají se přidané symboly A(1), A(2),.....A(16), které v IFF zrychlují postup dotaz/odpověď, které se připojí k 21 klíčovým symbolům čímž vnikne celkově 165 symbolů K_1 ,K_2 ,... až $K_{1\,6\,5}$. Požadavky paměti pro 48 klíčů/den činí 48 x 165 = 7920 symbolů, nebo 8K symbolů.

Tak jak to již bylo popsáno, preferovaný klíč pro použití ve spojení s šifrovacím systémem, podle tohoto vynálezu, má tři části:

1. Osm symbolů které jsou náhodně vybrány z celých čísel 1 až 25.
2. Devět nahodilých symbolů
3. Čtyři nahodilé symboly.

Kromě požadavků na to, aby prvních osm symbolů bylo nahodilými symboly v rozmezí 1 až 25, neexistuje žádné omezení týkající se generování klíčů. Generace klíčů musí pozorně sledována, aby se zajistilo, že generace nevytvoří chyby nebo nenahodilé vlastnosti. Žádný ze známých zařízení pro náhodné rozdělování (randomizer) neodpovídá daným požadavkům.

Jakmile jsou klíče vygenerovány, mohou se zašifrovat pro následný přenos. Přednost se dáván tomu, aby byly soustředěny do skupin tak, aby každá skupina zahrnovala jednoměsíční zásobu tj. 31 x 48 = 1488 klíčů.

Každá jednoměsíční skupina klíčů se může zašifrovat šifrovým blokem, tak jak to bylo popsáno dříve, a to použitím Key Encrypting Keyî) (KEK) , který se ručně rozděluje na základě dané periodicity, která má svoji frekvenci, a to tak, že fyzická bezpečnost je adekvátní pro podporu sady kryptoperiody, například jednoroční, pro KEK.

Jiné směrnice jsou určené pro ovládání klíčů v operačním zařízení IFF. Například klíče s pouze dvoudenní platností, jmenovitě dnešní a zítřejší klíče, se ukládají v tomto

zařízení, a to za předpokladu, že zařízení IFF se vrací do hlavní báze v průběhu každých dvou dnů. Jestliže to není tento případ, směrnice může být uvolněna tak, že dva dny nahradí za maximální dobu, po kterou je zařízení mimo bázi. Podobné bezpečnostní úvahy by měly směřovat i do jiných aplikací systému, podle tohoto vynálezu.

Vynález byl popsán pomocí vzorových a preferovaných provedení. Rozsah tohoto vynálezu však není omezen pouze na tato konkrétní provedení. Naopak, tento vynález zahrnuje různé modifikace a podobná uspořádání. Rozsah nároků by měl poskytovat co nejširší možnost interpretace, a to tak, aby zahrnoval všechny modifikace a podobná uspořádání. Například vzorový režim šifrového bloku, podle tohoto vynálezu, byl popsán velmi podrobně. Odborníkům v oboru je však zřejmé, že zde popsaný způsob a zařízení lze snadno aplikovat na otevřenou zprávu přijatou a zpracovanou spíše jako proud než jako blok, aniž by se tím toto zpracování vzdalovalo od duchu a rozsahu tohoto vynálezu.

PATENTOVÉ NÁROKY

1. Spojovací systém zahrnuje:

   a) výchozí prostor,

   b) spojovací kanál,

   c) prostor určení spojený s výchozím prostorem pomocí spojovacího kanálu,

   d) výchozí prostor přitom zahrnuje:

      1) šifrovací generátor pro generování výstupního symbolu O_t založeného na vstupním symbolu I_t ,

      2) prostředek pro příjem šifrovacího klíče a šifrového vztahu text/klíč, a pro příjem vstupního symbolu,

   e) prostor určení přitom zahrnuje:

      1) dešifrovací generátor pro generování dešifrovacího symbolu I'_t založeného na výstupním symbolu přijatého z výchozího prostoru pomocí spojovacího kanálu,

      2) prostředek pro příjem dešifrovacího klíče a šifrového vztahu text/klíč.

   f) přitom šifrový vztah text/klíč řídí šifrovací generátor tak, že

   $O_t = \alpha_N(t) + \pi_N[\alpha_{N-1}(t) + \pi_{n-1}[\alpha_{N-2}(t) + \ldots\ldots + \pi_2[\alpha_1(t) + \pi_1[I_t + \alpha_0(t)]]\ldots\ldots]]$, mod W, kde α_N , α_{N-1} $\ldots\ldots\alpha_1$, α_0 jsou N+1 aditivní transformace definované šifrovacím klíčem, kde výrazy π_N , π_{N-1} , $\ldots\ldots\pi_1$, π_0 jsou N permutace definované šifrovacím klíčem, a kde W reprezentuje počet možností pro každou permutaci definovanou šifrovacím klíčem.

   g) přitom šifrový vztah text/klíč řídí dešifrovací generátor tak, že $I_t' = \pi_1^{-1}[\pi_2^{-1}[\pi_3^{-1}\ldots\ldots[\pi_{n-1}^{-1}[\pi_N^{-1}[O_t - \alpha'_N(t)] - \alpha'_{N-1}(t)] - \ldots\ldots\alpha'_3(t) - \alpha'_2(t)] - \alpha'_1(t)] - \alpha'_0(t)$, mod W, kde výraz π_1^{-1} je definován dešifrovacím klíčem jako inverzní funkce permutace π_i , kde výrazy α'_N , α'_{N-1} , $\ldots\ldots\alpha'_1$, α'_0 jsou N+1 aditivní transformace definované dešifrovacím klíčem, a kde W představuje počet možností každé inverzní permutace definované dešifrovacím klíčem.

2. Spojovací systém podle nároku 1, v y z n a č u j í c í s e t í m , že šifrovací generátor zahrnuje W vyhledávací tabulky pro ukládání každé z možných W sad permutací.

3. Spojovací systém podle nároku 1, v y z n a č u j í c í s e t í m , že šifrovací generátor dále zahrnuje M<W vyhledávací tabulky pro ukládání M dostupných sad z možných W sad permutací.

4. Spojovací systém podle nároku 1, v y z n a č u j í c í s e t í m , že šifrovací generátor dále zahrnuje N<M<W vyhledávací tabulky pro ukládání N sad permutací, předem vybraných z M dostupných sad možných W sad permutaci.

5. Spojovací systém podle nároku 1, v y z n a č u j í c í s e t í m , že $\alpha(t)$ je krokovou funkcí.

6. Spojovací systém podle nároku 5, v y z n a č u j í c í s e t í m , že $\alpha(t)$, X{0, 1, 2,.. N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu, u které se t rovná celému násobku R, kde R je prvočíslo.

7. Spojovací systém podle nároku 5, v y z n a č u j í c í s e t í m , že $\alpha(t)$, X{0, 1, 2,.. N-1, N} snižuje sekvenci π_x pro každou hodnotu, u které se t rovná celému násobku R, kde R je prvočíslo.

8. Spojovací systém podle nároku 5, v y z n a č u j í c í s e t í m , že $\alpha(t)$, X{0, 1, 2,..N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu t s výjimkou , kdy se t rovná celému násobku R, kdy R je prvočíslo.

9. Spojovací systém podle nároku 5, v y z n a č u j í c í s e t í m , že $\alpha(t)$, X{0, 1, 2,..N-1, N}, snižuje sekvenci π_x pro každou hodnotu t, s výjimkou, kdy se t rovná celému násobku R, kdy R je prvočíslo.

10. Spojovací systém podle nároku 1, kde I'_t odpovídá I_t .

11. Spojovací systém zahrnuje:

a) výchozí prostor,

b) spojovací kanál,

c) prostor určení spojený s výchozím prostorem pomocí spojovacího kanálu,

d) výchozí prostor přitom zahrnuje:

1) prostředek pro příjem výstupního symbolu I_t , šifrovací klíč a šifrový vztah text/klíč,

2) šifrovací generátor řízený šifrovým vztahem pro generování výstupního symbolu O_t založeného na vstupním symbolu tak, že $O_t = \alpha_N (t) + \pi_N [\alpha_{N-1} (t) + \pi_{n-1} [\alpha_{N-2} (t) + ...+\pi_2 [\alpha_1 (t) + \pi_1 [I_t + \alpha(t)]]....]]$, mod W, kde $\alpha_N , \alpha_{N-1} .....\alpha_1 , \alpha_0$ jsou N+1 aditivní transformace definované šifrovacím klíčem, kde výraz $\pi_N , \pi_{N-1} , ...\pi_1 , \pi_0$ jsou N permutace definované šifrovacím klíčem, a kde W reprezentuje počet možností pro každou permutaci definovanou šifrovacím klíčem,

e) prostor určení přitom zahrnuje:

1) prostředek pro příjem dešifrovacího klíče a dešifrový vztah text/klíč,

2) dešifrovací generátor řízený pro generování dešifrovaného symbolu I'_t založeného na výstupním symbolu přijatého z výchozího prostoru pomocí spojovacího kanálu tak, že $I_t' = \pi_1^{-1}[\pi_2^{-1}[\pi_3^{-1}.....[\pi_{n-1}^{-1}[\pi_N^{-1}[O_t - \alpha'_N (t)] - \alpha'_{N-1} (t)]-.....\alpha'_3 (t)-\alpha'_2 (t)]-\alpha'_1 (t)]-\alpha'_0 (t)$, mod W, kde výraz π_1^{-1} je definován dešifrovacím klíčem jako inverzní funkce permutace π_i , kde výrazy $\alpha'_N , \alpha'_{N-1} , ...\alpha'_1 , \alpha'_0$ jsou N+1 aditivní transformace definované dešifrovacím klíčem, a kde W představuje počet možností každé inverzní permutace definované dešifrovacím klíčem.

12. Spojovací systém podle nároku 11, v y z n a č u j í c í s e t í m , že šifrovací generátor dále zahrnuje W vyhledávací tabulky pro ukládání každé z možných W sad permutací.

13. Spojovací systém podle nároku 11, v y z n a č u j í c í s e t í m , že šifrovací generátor dále zahrnuje M<W vyhledávací tabulky pro ukládání M dostupných sad z možných W sad permutací.

14. Spojovací systém podle nároku 11, v y z n a č u j í c í s e t í m , že šifrovací generátor dále zahrnuje N<M<W vyhledávací tabulky pro ukládání N sad permutací, předem vybraných z M dostupných sad možných W sad permutací.

15. Spojovací systém podle nároku 1, v y z n a č u j í c í s e t í m , že $\alpha(t)$ je krokovou funkcí.

16. Spojovací systém podle nároku 5, v y z n a č u j í c í s e t í m , že $\alpha(t)$, X{0, 1, 2,.. N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu, u které se t rovná celému násobku R, kde R je prvočíslo.

17. Spojovací systém podle nároku 5, v y z n a č u j í c í s e t í m , že $\alpha(t)$, X{0, 1, 2,.. N-1, N} snižuje sekvenci π_x pro každou hodnotu, u které se t rovná celému násobku R, kde R je prvočíslo.

18. Spojovací systém podle nároku 5, v y z n a č u j í c í s e t í m , že $\alpha(t)$, X{0, 1, 2,..N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu t s výjimkou , kdy se t rovná celému násobku R, kdy R je prvočíslo.

19. Spojovací systém podle nároku 5, v y z n a č u j í c í s e t í m , že $\alpha(t)$, X{0, 1, 2,..N-1, N}, snižuje sekvenci π_x pro každou hodnotu t s výjimkou, kdy se t rovná celému násobku R, kdy R je prvočíslo.

20. Spojovací systém podle nároku 11, v y z n a č u j í c í s e t í m , že I'_t odpovídá I_t

21. Spojovací systém zahrnuje:

a) první počítač

b) spojovací kanál

c) druhý počítač spojený s prvním počítačem pomocí spojovacího kanálu,

d) první počítač přitom zahrnuje:

1) vstupní port symbolu pro příjem vstupního symbolu I_t ,

2) vstupní port šifrovacího klíče pro příjem šifrovacího klíče,

3) první paměť pro uložení šifrového vztahu text/klíč,

4) první mikroprocesor pro generování výstupního symbolu O_t , založeného na vstupním symbolu, řízeného šifrového vztahu text/klíč tak, že $O_t = \alpha_N (t) + \pi_N [\alpha_{N-1} (t) + \pi_{n-1} [\alpha_{N-2} (t) + \ldots + \pi_2 [\alpha_1 (t) + \pi_1 [I_t + \alpha_0 (t)]] \ldots]]$, mod W, kde α_N , $\alpha_{N-1} \ldots \alpha_1$, α_0 jsou N+1 aditivní transformace definované šifrovacím klíčem, kde výraz π'_N , π'_{N-1} , $\ldots \pi'_1$, π'_0 jsou N permutace definované šifrovacím klíčem, a kde W reprezentuje počet možností pro každou permutaci definovanou šifrovacím klíčem,

e) druhý počítač přitom zahrnuje

1) vstupní port dešifrovacího klíče pro příjem dešifrovacího klíče,

2) druhou paměť pro uložení dešifrového vztahu text/klíč,

3) druhý mikroprocesor pro generování dešifrovaného symbolu I'_t založeného na výstupním symbolu přijatého z výchozího prostoru pomocí spojovacího kanálu, řízeného dešifrového vztahu text/klíč tak, že $I_t' = \pi_1^{-1}$ $[\pi_2^{-1}[\pi_3^{-1}.....[\pi_{n-1}^{-1}[\pi_N^{-1}[O_t - \alpha'_N(t)] - \alpha'_{N-1}(t)] - .....\alpha'_3(t) - \alpha'_2(t)] - \alpha'_1(t)] - \alpha'_0(t)$, mod W, kde výraz π_1^{-1} je definován dešifrovacím klíčem jako inverzní funkce permutace π_i, kde výrazy α'_N, α'_{N-1}, $.....\alpha'_1$, α'_0 jsou N+1 aditivní transformace definované dešifrovacím klíčem, a kde W představuje počet možností každé inverzní permutace definované dešifrovacím klíčem.

22. Spojovací systém podle nároku 21, v y z n a č u j í c í s e t í m, že první počítač dále zahrnuje W vyhledávací tabulky pro ukládání každé z možných W sad permutací.

23. Spojovací systém podle nároku 21, v y z n a č u j í c í s e t í m, že šifrovací generátor dále zahrnuje M<W vyhledávací tabulky pro ukládání M dostupných sad z možných W sad permutací.

24. Spojovací systém podle nároku 21, v y z n a č u j í c í s e t í m, že šifrovací generátor dále zahrnuje N<M<W vyhledávací tabulky pro ukládání N sad permutací, předem vybraných z M dostupných sad možných W sad permutací.

25. Spojovací systém podle nároku 1, v y z n a č u j í c í s e t í m, že $\alpha(t)$ je krokovou funkcí.

26. Spojovací systém podle nároku 25, v y z n a č u j í c í s e t í m, že $\alpha(t)$, X{0, 1, 2,.. N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu, u které se t rovná celému násobku R, kde R je prvočíslo.

27. Spojovací systém podle nároku 25, v y z n a č u j í c í s e t í m, že $\alpha(t)$, X{0, 1, 2,.. N-1, N} snižuje sekvenci π_x pro každou hodnotu, u které se t rovná celému násobku R, kde R je prvočíslo.

28. Spojovací systém podle nároku 25, v y z n a č u j í c í s e t í m , že $\alpha(t)$, X{0, 1, 2,..N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu t s výjimkou , kdy se t rovná celému násobku R, kdy R je prvočíslo.

29. Spojovací systém podle nároku 25, v y z n a č u j í c í s e t í m , že $\alpha(t)$, X{0, 1, 2,..N-1, N}, snižuje sekvenci π_x pro každou hodnotu t s výjimkou, kdy se t rovná celému násobku R, kdy R je prvočíslo.

30. Spojovací systém podle nároku 21, v y z n a č u j í c í s e t í m , že I'_t odpovídá I_t

31. Postup spojování mezi výchozím prostorem a prostorem určení zahrnuje:

a) příjem vstupního symbolu I_t ve výchozím prostoru,

b) generování výstupního symbolu O_t založeného na vstupním symbolu tak, že $O_t = \alpha_N(t) + \pi_N[\alpha_{N-1}(t) + \pi_{n-1}[\alpha_{N-2}(t) + \ldots\ldots + \pi_2[\alpha_1(t) + \pi_1[I_t + \alpha_0(t)]]\ldots\ldots]]$, mod W, kde α_N , α_{N-1} $\ldots\ldots\alpha_1$, α_0 jsou N+1 aditivní transformace kde výrazy π'_N , π'_{N-1} , $\ldots\ldots\pi'_1$, π'_0 jsou N permutace, a kde W reprezentuje počet možností pro každou permutaci

c) příjem výstupního symbolu v prostoru určení,

d) generování dešifrovaného symbolu I'_t založeného na přijatém výstupním symbolu tak, že $I_t' = \pi_1^{-1}[\pi_2^{-1}[\pi_3^{-1}\ldots\ldots[\pi_{n-1}^{-1}[\pi_N^{-1}[O_t - \alpha'_N(t)] - \alpha'_{N-1}(t)] - \ldots\ldots\alpha'_3(t) - \alpha'_2(t)] - \alpha'_1(t)] - \alpha'_0(t)$, mod W, kde výraz π_1^{-1} je inverzní funkcí permutace π_i , kde výrazy α'_N , α'_{N-1} , $\ldots\ldots\alpha'_1$, α'_0 jsou N+1 aditivní transformace, a kde W představuje počet možností každé inverzní permutace.

32. Postup podle nároku 31, v y z n a č u j í c í s e t í m , že dále zahrnuje vyvolání M možných sad permutací z W vyhledávacích tabulek, a to před generováním výstupního symbolu.

33. Postup podle nároku 31, v y z n a č u j í c í s e t í m , že dále zahrnuje vyvolání M dostupných sad z možných W sad permutací z M<W vyhledávacích tabulek, a to před generováním výstupního symbolu.

34.Postup podle nároku 31, v y z n a č u j í c í s e t í m , že dále zahrnuje vyvolání N sad permutací předem vybraných z M dostupných sad možných W sad permutací z N<M<W vyhledávacích tabulek, a to před generováním výstupních symbolů.

35.Postup podle nároku 31, v y z n a č u j í c í s e t í m , že $\alpha(t)$ je krokovou funkcí.

36.Postup podle nároku 35, v y z n a č u j í c í s e t í m , že $\alpha(t)$, X{0, 1, 2,.. N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu, u které se t rovná celému násobku R, kde R je prvočíslo.

37.Postup podle nároku 35, v y z n a č u j í c í s e t í m , že $\alpha(t)$, X{0, 1, 2,.. N-1, N} snižuje sekvenci π_x pro každou hodnotu, u které se t rovná celému násobku R, kde R je prvočíslo.

38.Postup podle nároku 35, v y z n a č u j í c í s e t í m , že $\alpha(t)$, X{0, 1, 2,..N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu t s výjimkou , kdy se t rovná celému násobku R, kdy R je prvočíslo.

39.Postup podle nároku 35, v y z n a č u j í c í s e t í m , že $\alpha(t)$, X{0, 1, 2,..N-1, N}, snižuje sekvenci π_x pro každou hodnotu t s výjimkou, kdy se t rovná celému násobku R, kdy R je prvočíslo.

40.Postup podle nároku 31, v y z n a č u j í c í s e t í m , že I'_t odpovídá I_t

41.Paměť zahrnuje:

interface a

prostředek pro řízení mikroprocesoru přes interface, a to s cílem produkce výstupního symbolu O_t tak, že $O_t = \alpha_N(t) + \pi_N[\alpha_{N-1}(t) + \pi_{n-1}[\alpha_{N-2}(t) + \ldots\ldots + \pi_2[\alpha_1(t) + \pi_1[I_t + \alpha_0(t)]]\ldots.]]$, mod W, kde α_N , α_{N-1} $\ldots\ldots\alpha_1$, α_0 jsou N+1 aditivní transformace definované šifrovacím klíčem, kde výrazy π'_N , π'_{N-1} , $\ldots\ldots\pi'_1$, π'_0 jsou N permutace definované šifrovacím klíčem, a kde W reprezentuje počet možností pro každou permutaci definovanou šifrovacím klíčem.

42.Paměť podle nároku 41, v y z n a č u j í c í s e t í m , že $\alpha(t)$ krokovou funkcí.

43. Paměť podle nároku 42, v y z n a č u j í c í s e t í m , že α_x (t), X{0, 1, 2,.. N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu, u které se t rovná celému násobku R, kde R je prvočíslo.

44. Spojovací systém podle nároku 42, v y z n a č u j í c í s e t í m , že α_x (t), X{0, 1, 2,..N-1, N} snižuje sekvenci π_x pro každou hodnotu, u které se t rovná celému násobku R, kde R je prvočíslo.

45. Spojovací systém podle nároku 42, v y z n a č u j í c í s e t í m , že α_x (t), X{0, 1, 2,..N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu t s výjimkou , když se t rovná celému násobku R, kdy R je prvočíslo.

46. Spojovací systém podle nároku 42, v y z n a č u j í c í s e t í m , že α_x (t), X{0, 1, 2,..N-1, N}, snižuje sekvenci π_x pro každou hodnotu t s výjimkou, když se t rovná celému násobku R, kdy R je prvočíslo.

47. Paměť zahrnuje:

interface a

prostředek pro řízení mikroprocesoru přes interface, a to s cílem produkce generovaného symbolu $I_t = \pi_1^{-1}[\pi_2^{-1}[\pi_3^{-1}.....[\pi_{n-1}^{-1}[\pi_N^{-1}[O_t - \alpha'_N(t)] - \alpha'_{N-1}(t)] - .....\alpha'_3(t) - \alpha'_2(t)] - \alpha'_1(t)] - \alpha'_0(t)$, mod W, kde O_t je přijatý symbol, kde výrazy α_N , α_{N-1} .....α_1 , α_0 jsou N+1 aditivní transformace definované šifrovacím klíčem, kde výrazy $\pi_1^{-1}...\pi_N^{-1}$ jsou N permutace definované šifrovacím klíčem, a kde W reprezentuje počet možností pro každou permutaci definovanou šifrovacím klíčem,

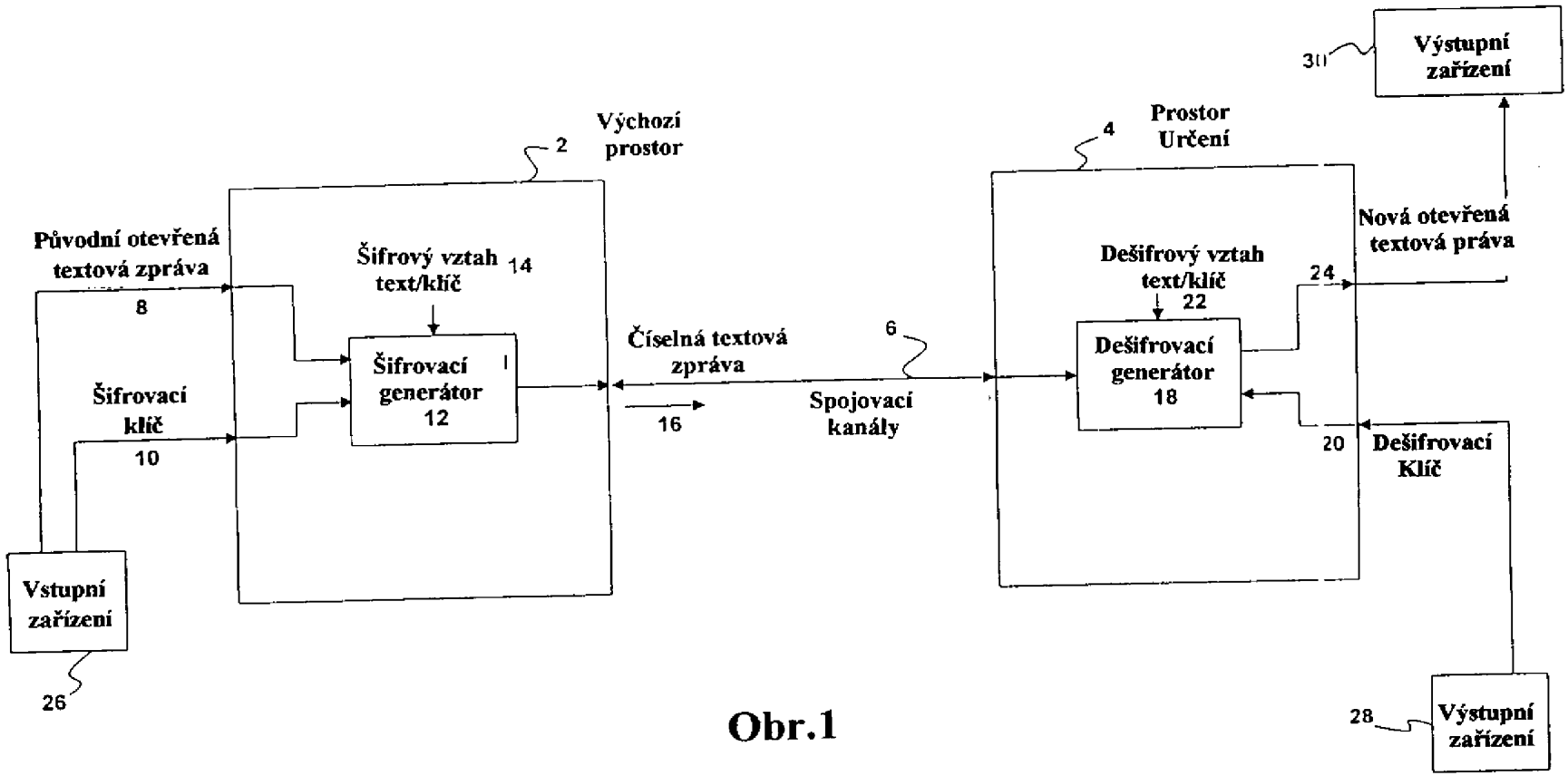
48. Paměť podle nároku 47, v y z n a č u j í c í s e t í m , že α(t) je krokovou funkcí.

49. Paměť podle nároku 48, v y z n a č u j í c í s e t í m , že α_x (t), X{0, 1, 2,.. N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu, u které se t rovná celému násobku R, kde R je prvočíslo.

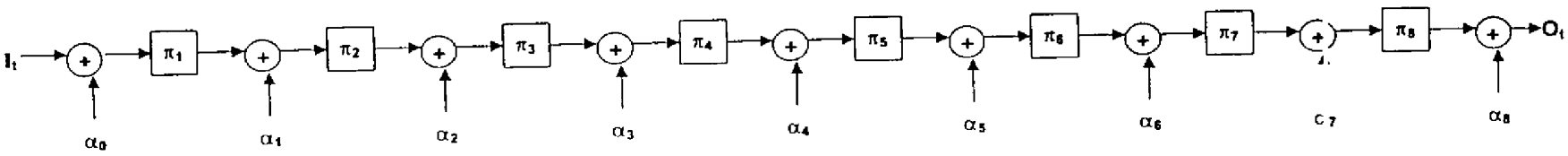
50. Spojovací systém podle nároku 48, v y z n a č u j í c í s e t í m , že α_x (t), X{0, 1, 2,..N-1, N} snižuje sekvenci π_x pro každou hodnotu, u které se t rovná celému násobku R, kde R je prvočíslo.

51. Spojovací systém podle nároku 48, v y z n a č u j í c í s e t í m , že α_x (t), X{0, 1, 2,..N-1, N}, zvyšuje sekvenci π_x pro každou hodnotu t s výjimkou , kdy se t rovná celému násobku R, kdy R je prvočíslo.

52. Spojovací systém podle nároku 42, v y z n a č u j í c í s e t í m , že α_x (t), X{0, 1, 2,..N-1, N}, snižuje sekvenci π_x pro každou hodnotu t s výjimkou, kdy se t rovná celému násobku R, kdy R je prvočíslo.


Výstupní zařízení
30
Výchozí prostor
2
Prostor Určení
4
Původní otevřená textová zpráva
8
Šifrový vztah text/klíč
14
Dešifrový vztah text/klíč
22
Nová otevřená textová práva
24
Číselná textová zpráva
6
Šifrovací generátor 12
Dešifrovací generátor 18
Spojovací kanály
16
Šifrovací klíč
10
20
Dešifrovací Klíč
Vstupní zařízení
26
28
Výstupní zařízení

Obr.1



⊕: **Přidání modulo W**

Obr.2