República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

(11) (21) **PI 0604035-7 A**

(22) Data de Depósito: 05/09/2006
(43) Data de Publicação: **22/04/2008**
(RPI 1946)

(51) Int. Cl.:
H04L 9/14 (2008.04)

(54) Título: **SISTEMA DE REENCRIPTAÇÃO DE VÍDEOS DIGITAIS**

(71) Depositante(s): Adalberto Pereira Marques (BR/SP)

(72) Inventor(es): Adalberto Pereira Marques

(57) Resumo: SISTEMA DE REENCRIPTAÇÃO DE VÍDEOS DIGITAIS Patente de invenção, cria um sistema de reencriptação de filmes digitais, possibilitando que os filmes sejam distribuídos em uma criptografia impossível de ser reproduzida por qualquer aparelho, para que os mesmos possam ser assistidos deverão ser reescritos na criptografia especifica de cada aparelho reprodutor. Para que tal processo seja possível o sistema de reencriptação fornecerá no ato da aquisição do filme os recursos necessários para que o usuário grave o filme no formato e linguagem que apenas seu aparelho poderá reproduzir.

SISTEMA DE REENCRIPTAÇÃO DE VIDEOS DIGITAIS

A presente patente de invenção tem por objetivo apresentar um novo formato na distribuição de filmes digitalizados, cuja característica principal é o combate às cópias ilegais (piratas), pois a partir dele os reprodutores domésticos passarão a exibir única e exclusivamente cópias criptografadas produzidas especificamente para cada aparelho.

Atualmente os filmes distribuídos possuem uma mesma codificação, o que permite que qualquer aparelho reprodutor reproduza seu conteúdo, pois a informação "A" esta escrita como "A" e será lida como "A". No modelo desenvolvido cada filme passará a ser distribuídos com uma criptografia própria cuja chave não será revelada, tornando impossível sua leitura por qualquer aparelho reprodutor; para os aparelho reprodutor será atribuído uma chave de decriptação individual, que também não será revelada, sendo assim, não poderá ler nenhum vídeo distribuído diretamente. O sistema possibilitará que o vídeo já criptografado seja reencriptado diretamente para um determinado aparelho reprodutor.

Para melhor compreensão é preciso, antes de tudo, entender o que é criptografia.

Criptografia é a ciência que usa matemática para encriptar e desencriptar dados. A criptografia possibilita que você guarde ou transmita informações através de sistemas inseguros (como a Internet, discos etc) de tal forma que a informação não pode ser lida, a não ser pelo aparelho que é pretendido. Um algoritmo de criptografia é uma função matemática usada no processo de encriptação e de desencriptação. Um algoritmo de criptografia trabalha em

conjunto com uma chave para encriptar os dados, os mesmos dados podem gerar diferentes dados encriptados usando chaves diferentes, ou seja, se mudarmos a chave para um mesmo conjunto de dados geramos, dados encriptados diferentes, assim sendo, se partirmos da informação "A" utilizando a função criptográfica através da chave 1 (Fc1) obteremos o resultado "X", e para desencripta-lo utilizamos função decriptográfica com a chave 1 (Fd1) e transformamos novamente em "A", se utilizarmos a mesma função criptográfica através da chave 2 (Fc2) obteremos o resultado "Y", e para desencripta-lo utilizamos função decriptográfica com a chave 2 (Fd2) e transformamos novamente em "A".

Proponho que os filmes fornecidos sejam criptografados com uma chave (Fc1) enquanto os aparelhos reprodutores estão configurados pára ler as informações a partir de outra chave (Fd2), logo os aparelhos serão incapazes de ler diretamente os filmes, para que isto seja possível precisamos reescreve-los através da função de reencriptação composta entre chaves 1 e 2 (Fr1->2).

Sendo assim a informação "A" será criptografada com Fc1 e distribuída como "X", através da função de reencriptação Fr1->2 será reescrita como "Y" e o aparelho reprodutor correspondente utilizando-se de Fd2 exibirá a informação "A".

No anexo, Descrição Matemática, comprovo matematicamente a consistência da proposta acima, a parte 1 mostra as equações puras utilizando Algoritmo RSA, na parte2, utilizo um exemplo prático para demonstrar e eficácia do sistema.

Para que o sistema seja operacional a empresa responsável dividirá o

processo em 3 fases: Filmes, Aparelhos reprodutores e Sistema de reencriptação.

Filmes: Será fornecido aos Produtores o recurso para que cada filme seja distribuído com uma criptografia própria (Fc1), guardando as respectivas chaves.

Aparelho reprodutor: Será fornecido aos Fabricantes o recurso e/ou chips para que cada aparelho produzido tenha sua própria decriptografia (Fd2), guardando para si as respectivas chaves.

Sistema de reencriptação: A empresa responsável pelo sistema manterá em seu banco de dados todas as chaves e disponibilizará um provedor de acesso via Internet. Disponibilizará aos usuários um programa de acesso ao sistema, que possibilite uma nova gravação. Desta forma o usuário ao adquirir um filme fornecerá ao programa a identificação de seu aparelho e do filme adquirido, que acessará o provedor e receberá a variável de reencriptação (Fr1->2) e gravará o filme na nova criptografia que somente seu aparelho poderá ler e conseqüentemente reproduzir.

O Fluxograma anexo demonstra o funcionamento operacional do sistema.

REIVINDICAÇÃO

"SISTEMA DE REENCRIPTAÇÃO DE VÍDEOS DIGITAIS" Possibilita que os filmes sejam distribuídos em uma criptografia impossível de ser reproduzida por qualquer aparelho, para que os mesmos possam ser assistidos deverão ser reescritos utilizando uma criptografia especifica para cada aparelho reprodutor, impossibilitando assim a comercialização ou distribuição de cópias ilegais (piratas). Tal processo só é possível caracterizada pelo fato de, ao adquirir um filme o sistema fornecer a função de reencriptação composta entre chave criptográfica daquele filme e a chave decriptográfica do aparelho do usuário, permitindo que o mesmo grave o filme no formato e linguagem que apenas seu aparelho possa reproduzir.

DESCRIÇÃO MATEMÁTICA UTILIZANDO COMO BASE O SISTEMA RSA

Como funciona:

São escolhidos dois números primos extensos, p e q, (geralmente maiores que 10^{100})

Calcula-se:

$n = p * q$

$z = (p-1) * (q-1)$

Escolhe-se um número primo d, em relação a z

Encontramos "e" de forma que (e * d) mod z = 1

Para criptografar a mensagem, "A", é calculado $C = A^e \pmod n$.

Para decriptografar C, é calculado $A = C^d \pmod n$.

É possível provar que, para todo "A", as funções de criptografia e decriptografia são inversas entre si. Para realizar a criptografia, é necessário ver o "e" e "n", ao passo que para a decriptografia, são necessários "d" e "n".

Portanto as chaves são "e" e "d".

Parte 1: Comprovação matemática.

Sendo "A" o algoritmo original,

Sendo "Y" o algoritmo de entrada do Aparelho de reprodutor,

Sendo "f" e "g" as chaves em n1 para o Filme e "W" sua forma critografada,

Sendo "h" e "k" as chaves em n2 para o Aparelho reprodutor e "Y" sua forma critografada,

$W=A^f \pmod{n1}$ criptografa o filme

$A=W^g \pmod{n1}$ decriptografa o filme

$Y=A^h \pmod{n2}$ criptografa o Aparelho

$A=Y^k \pmod{n2}$ decriptografa o Aparelho

A função de reencriptação FrW->Y será:

$(W^{g} (\text{mod } n1))^{h} (\text{mod } n2)$

Comprovação:

sendo $(W^{g} (\text{mod } n1))^{h} = A$

=> $(W^{g} (\text{mod } n1))^{h} (\text{mod } n2) = A^{h} (\text{mod } n2) = Y$

Desta forma a nova gravação estará escrita em Y que é a forma criptografada do Aparelho reprodutor que por sua vez exibirá a informação "A"

Parte 2: Exemplo prático.

Para um melhor entendimento veremos resumidamente o uso do método em um exemplo.

Os números escolhidos para "p" e "q", geralmente são maiores que 10^{100} para viabilizar este exemplo utilizaremos números pequenos e diferentes para o Filme e Aparelho reprodutor.

Para o Filme escolheremos p = 3 e q = 11

Calculando n1 = p * q .....e..... z = (p-1) * (q-1)

.....n1 = 3 * 11 .....z = 2 * 10

.....n 1= 33 .....z = 20

O valor escolhido como número primo, em relação a z é 7, visto que 7 e 20 não possuem fatores comuns desse modo d = 7

Para que a equação (e * d) mod z = 1 seja verdadeira o "e" = 3

Logo as chaves são "f"=7 e "g"=3

Para o Aparelho Reprodutor escolheremos p = 7 e q = 17

Calculando n2 = p * q .....e..... z = (p-1) * (q-1)

.....n2 = 7 * 17 .....z = 6 * 16

.....N2 = 119 .....z = 96

O valor escolhido como número primo, em relação a z é 17, visto que 17 e 86 não possuem fatores comuns desse modo d = 17

Para que a equação (e * d) mod z = 1 seja verdadeira o "e" = 17

Logo as chaves são "h"=17 e "k"=17

Tomando-se de base o número 18 como um algoritmo qualquer do filme origina.

Teremos as seguintes transformações:

Filme a ser distribuido

$W=A^{f}(\text{mod } n1) = 18^{3}(\text{mod } 33) = 5832(\text{mod } 33) = 24$

Na gravação do usuário

$Y= (W^{g}(\text{mod } n1))^{h} (\text{mod } n2)$ =>

$Y = (24^{7}(\text{mod } 33))^{17}(\text{mod } 119)$ =>

$Y = (4586471424 (\text{mod } 33))^{17}(\text{mod}119)$ =>

$Y = (18)^{17} (\text{mod}119) = 2185911559738696531968 (\text{mod } 119)$ =>

Y= 86

Na hora da exibição do filme pelo aparelho do usuário

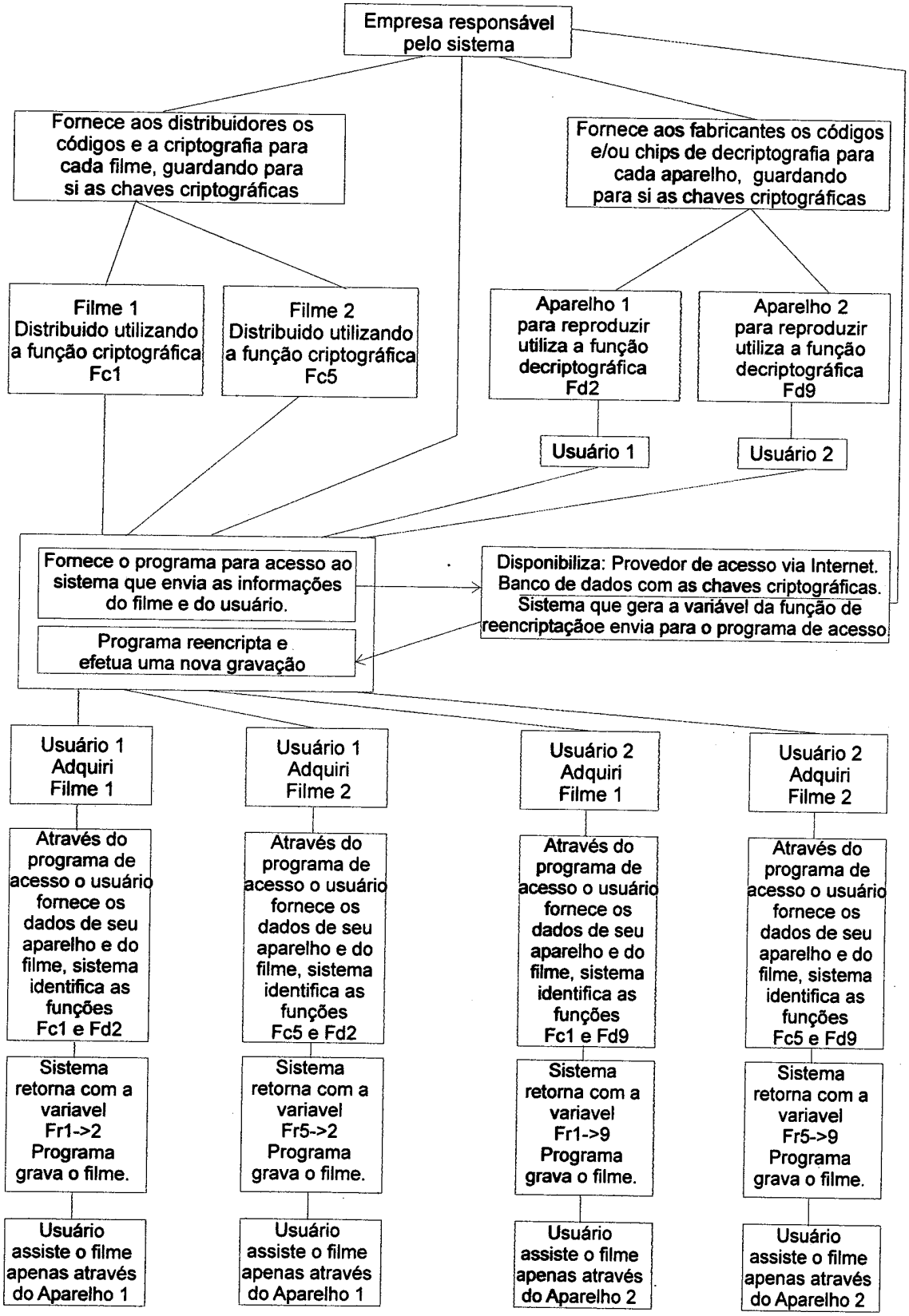
$A = Y^{k} (\text{mod } n2) = 86^{17}(\text{mod } 119)$ =>

A = 7,69969763956872972714580855095 3e+32 (mod 119) =>

A = 18

Portanto o aparelho reprodutor do usuário exibirá a informação original após ter passado por todas etapas propostas.

FLUXOGRAMA:


Empresa responsável pelo sistema
Fornece aos distribuidores os códigos e a criptografia para cada filme, guardando para si as chaves criptográficas
Fornece aos fabricantes os códigos e/ou chips de decriptografia para cada aparelho, guardando para si as chaves criptográficas
Filme 1 Distribuido utilizando a função criptográfica Fc1
Filme 2 Distribuido utilizando a função criptográfica Fc5
Aparelho 1 para reproduzir utiliza a função decriptográfica Fd2
Aparelho 2 para reproduzir utiliza a função decriptográfica Fd9
Usuário 1
Usuário 2
Fornece o programa para acesso ao sistema que envia as informações do filme e do usuário.
Programa reencripta e efetua uma nova gravação
Disponibiliza: Provedor de acesso via Internet. Banco de dados com as chaves criptográficas. Sistema que gera a variável da função de reencriptaçãoe envia para o programa de acesso
Usuário 1 Adquiri Filme 1
Usuário 1 Adquiri Filme 2
Usuário 2 Adquiri Filme 1
Usuário 2 Adquiri Filme 2
Através do programa de acesso o usuário fornece os dados de seu aparelho e do filme, sistema identifica as funções Fc1 e Fd2
Através do programa de acesso o usuário fornece os dados de seu aparelho e do filme, sistema identifica as funções Fc5 e Fd2
Através do programa de acesso o usuário fornece os dados de seu aparelho e do filme, sistema identifica as funções Fc1 e Fd9
Através do programa de acesso o usuário fornece os dados de seu aparelho e do filme, sistema identifica as funções Fc5 e Fd9
Sistema retorna com a variavel Fr1->2 Programa grava o filme.
Sistema retorna com a variavel Fr5->2 Programa grava o filme.
Sistema retorna com a variavel Fr1->9 Programa grava o filme.
Sistema retorna com a variavel Fr5->9 Programa grava o filme.
Usuário assiste o filme apenas através do Aparelho 1
Usuário assiste o filme apenas através do Aparelho 1
Usuário assiste o filme apenas através do Aparelho 2
Usuário assiste o filme apenas através do Aparelho 2

RESUMO

"SISTEMA DE REENCRIPTAÇÃO DE VÍDEOS DIGITAIS" Patente de invenção, cria um sistema de reencriptação de filmes digitais, possibilitando que os filmes sejam distribuídos em uma criptografia impossível de ser reproduzida por qualquer aparelho, para que os mesmos possam ser assistidos deverão ser reescritos na criptografia especifica de cada aparelho reprodutor. Para que tal processo seja possível o sistema de reencriptação fornecerá no ato da aquisição do filme os recursos necessários para que o usuário grave o filme no formato e linguagem que apenas seu aparelho poderá reproduzir.