Sorteio Eletrônico de Prêmios da Nota Fiscal Paraná

Descrição do Software de Escolha dos Bilhetes Premiados

RESUMO

O software de Sorteio Eletrônico da Nota Fiscal Paraná foi desenvolvido no Instituto de Pesquisas Tecnológicas do Estado de São Paulo (IPT), pela equipe técnica da Seção de Automação, Governança e Mobilidade Digital (SAGMD), para a Secretaria da Fazenda da Governo do Estado do Paraná - SEFA/PR.

O programa foi desenvolvido na linguagem de programação Java (versão 1.6.0_06), com padrões abertos, como o algoritmo de criptografia AES, utilizado para gerar números aleatórios confiáveis. Este documento apresenta as características de funcionamento do software, considerando os requisitos de geração de números aleatórios de alta qualidade e a otimização do desempenho dos sorteios.

1. GERAÇÃO DE NÚMEROS ALEATÓRIOS

A geração de números aleatórios com computadores só é possível com a ajuda de fontes externas de aleatoriedade, porém não há garantias de que a fonte de aleatoriedade (fonte de entropia) sempre fornecerá bons valores e que possam ser repetidos se necessário, assim como as ondas do mar podem passar por períodos de grande agitação ou relativa calmaria de forma extremamente imprevisível. Se a aleatoriedade for introduzida a cada número gerado, não há muito controle sobre a reprodutibilidade e a qualidade final dos números.

Assim, são utilizados em computação os chamados geradores randômicos pseudoaleatórios, baseados em algoritmos matemáticos conhecidos, que permitem gerar de forma iterativa números aleatórios de qualidade controlada, a partir de uma

fonte de entropia que é fornecida inicialmente, ou seja, uma semente. A semente é usada como parâmetro de inicialização da sequência de números aleatórios.

As sequências de números, geradas a partir de sementes diferentes, são totalmente distintas, sendo um indicador de qualidade do algoritmo, a dificuldade de estimar a semente utilizada. A sequência de números, gerada a partir de uma mesma semente, sempre será a mesma, permitindo a reprodutibilidade e a garantia da qualidade das sequências numéricas. A qualidade da semente é considerada crítica para a geração dos números: a garantia da qualidade e da imprevisibilidade das sequências numéricas será dada pela alta entropia, ou melhor, pela variação de valores da semente, que deve ocorrer da maneira mais aleatória e imprevisível que for possível[1].

Para atender os requisitos necessários no sorteio de prêmios da Nota Fiscal Paraná foi escolhido como semente dezesseis (16) dígitos da extração da Loteria Federal, que possui as características de imprevisibilidade e aleatoriedade, tão necessárias para o perfeito funcionamento do algoritmo.

2. O ALGORITMO AES

O *Advanced Encryption Standard* (AES) é um algoritmo de criptografia (cifra) selecionado pelo *National Institute of Standards and Technology* (NIST[2]) para a proteção de documentos eletrônicos em comunicações confidenciais. O AES é o resultado do concurso para substituir o *Data Encriptation Standard* (DES[3]), o algoritmo anteriormente recomendado pelo NIST. O algoritmo originalmente conhecido como *Rijndael* foi o vencedor da seleção para o AES. Este foi projetado levando em conta experiências dos

[1]Random Number Generators: An Evaluation and Comparison of Random.org and Some Commonly Used Generators: http://www.random.org/analysis/Analysis2005.pdf

[2]NIST http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html

[3]FIPS 46-3 - Data Encryption Standard (DES): http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

autores nos algoritmos *Square* e *Shark*, e incorporou proteção a diversos ataques conhecidos, mantendo a eficiência e simplicidade[4].

O algoritmo AES é uma cifra de bloco simétrica que permite a criptografar e descriptografar de informações baseadas em uma chave secreta (segredo), que pode ter 128, 192 ou 256 bits. As estatísticas realizadas sobre resultados do AES demonstram que não há qualquer correlação sistemática entre os dados originais e os dados criptografados. Características como velocidade, não linearidade, análise teórica criteriosa e portabilidade o fazem extremamente interessante como gerador de números pseudo aleatórios[5].

3. GERAÇÃO DOS NÚMEROS PARA O SORTEIO ELETRÔNICO

A partir do algoritmo AES, foi construído um gerador randômico de números inteiros de 32 bits, que correspondem ao tipo **int** e à classe **Integer** da linguagem **Java**. O Gerador randômico AES é um algoritmo que gera números inteiros com distribuição uniforme, ou seja, há igual probabilidade de qualquer valor ocorrer, sejam grandes, pequenos, positivos ou negativos.

O sorteio consiste em selecionar (premiar) um dos bilhetes gerados pela SEFA/PR, de acordo com seus procedimentos internos. A lista de bilhetes consiste de uma sequência de números inteiros entre 1 (um) e a quantidade de bilhetes distribuídos. A quantidade de prêmios deve ser menor ou igual à quantidade de bilhetes, e cada bilhete pode ser sorteado apenas uma vez.

Devido à restrição de não poderem ser sorteados números repetidos, surgem algumas questões de desempenho, que levaram a serem desenvolvidos dois algoritmos diferentes, construídos a partir do Gerador randômico AES para a realização do sorteio:

[4]FIPS 197, Advanced Encryption Standard (AES): http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[5]Peter Hallekalek e Stefan Wegenkittl: Empirical Evidence Concerning AES: http://random.mat.sbg.ac.at/ftp/pub/publications/peter/aes_sub.ps

o Gerador e o Embaralhador.

O Gerador tem melhor desempenho nos casos em que até metade dos bilhetes candidatos são premiados, mas tem desempenho cada vez pior quando a quantidade de premiados se aproxima da de candidatos. O Embaralhador tem melhor desempenho nos casos em que mais da metade dos bilhetes candidatos são premiados, mas apresenta desempenho cada vez pior quando a quantidade de premiados se aproxima de um. O Embaralhador complementa o Gerador na situação de poucos bilhetes participantes (em relação à quantidade de prêmios), evitando o problema de repetições com ótimo desempenho, mas à custa de crescente ineficiência no uso da memória. O funcionamento dos algoritmos é detalhado a seguir.

4. Gerador

O Gerador trabalha produzindo uma lista de números inteiros positivos (entre 1 e 2^{31}) a partir do Gerador randômico AES. Os números gerados são recalculados de acordo com um algoritmo de mudança de faixa (na verdade, utiliza-se o resto da divisão do número gerado pelo valor máximo permitido, que é definido pela quantidade de bilhetes participantes), gerando números inteiros que estão na faixa dos números de bilhetes fornecida pela SEFA/PR. Os números repetidos, que eventualmente aparecem, são prontamente descartados, pois cada bilhete pode ser sorteado apenas uma vez.

O algoritmo inicia gerando uma lista com 15% a mais de números, para compensar o descarte dos repetidos. Caso não seja atingida a quantidade de números necessária, são gerados iterativamente mais alguns blocos de números inteiros, até atingir a quantidade desejada. Devido à dificuldade crescente de encontrar números não repetidos quando se sorteiam os últimos prêmios para uma quantidade de prêmios muito próxima a de bilhetes, esse algoritmo só é utilizado para situações em que no máximo 50% dos bilhetes sejam premiados, pois nessas situações o desempenho do algoritmo é melhor.

Num paralelo com o mundo real, o Gerador pode ser comparado com uma série de globos, que sorteiam os dígitos, que compõem os números dos bilhetes.

5. EMBARALHADOR

O Embaralhador inicialmente gera uma lista sequencial de números inteiros positivos, com a mesma quantidade de bilhetes da lista fornecida pela SEFA/PR. A lista é então embaralhada, utilizando como fonte de aleatoriedade o Gerador randômico AES. Após o embaralhamento, os números, cuja posição esteja além do limite de prêmios, são descartados.

Este algoritmo não gera números repetidos, pois parte do embaralhamento de uma lista sequencial e tem a característica de armazenar todos os bilhetes a serem sorteados na memória principal do computador. Sendo assim, esse algoritmo só é utilizado para situações em que mais de 50% dos bilhetes sejam premiados, onde apresenta melhor desempenho, pois em outras situações utilizaria muita memória e não utilizaria grande parte dos números gerados inicialmente, o que torna o uso da memória muito ineficiente quando há uma grande quantidade de bilhetes candidatos.

Num paralelo com o mundo real o Embaralhador pode ser comparado a uma urna, contendo todos os bilhetes, que serão misturados várias vezes e depois retirado um a um até o número de prêmios.

6. PROCEDIMENTO FORMAL DE ENTREGA DO SOFTWARE DE SORTEIO DE PRÊMIOS À SEFA/PR

Em 2 de Dezembro de 2015, os representantes do IPT entregaram à SEFA/PR o Live-DVD que contém o sistema operacional Ubuntu Linux customizado e o pacote de software desenvolvido em linguagem Java pelo IPT, versão 1.20.20, revisão 1, cuja assinatura digital (Hash MD5) do arquivo Sorteio.jar é 'E156138D2C4D620B956F8CC3AEB1C561', conforme publicado na edição 9589 do Diário Oficial do Estado do Paraná em 3/12/2015 (Anexo A). Os representantes do IPT/SP e da SEFA/PR realizaram a lacração do notebook e DVD usados para os sorteios, os quais são deslacrados e utilizados somente nos dias dos sorteios, com acompanhamento dos auditores, e novamente lacrados, assim permanecendo até o sorteio seguinte.

Antônio Amorim

IPT/SAGMD

São Paulo, 20 de Dezembro de 2015.

Anexo A – Publicação do hash MD5 do software e da lista de bilhetes participantes do primeiro sorteio no Diário Oficial do Governo do Paraná

116 | 5ª feira | 03/Dez/2015 - Edição nº 9589 Diário OFICIAL Paraná Poder Executivo Estadual

Diário Oficial Certificado Digitalmente
O Departamento de Imprensa Oficial do Estado do Paraná, da garantia de autenticidade deste documento, desde que visualizado através do site http://www.imprensaoficial.pr.gov.br

RESOLUÇÃO SEFA Nº 1.315/2015

SÚMULA: Torna pública a chave única de codificação digital do algoritmo matemático utilizado para apuração dos bilhetes premiados no âmbito do Programa de Estímulo à Cidadania Fiscal do Estado do Paraná.

O SECRETÁRIO DE ESTADO DA FAZENDA, com fundamento no inciso XIV do art. 45 da Lei n. 8.485, de 3 de junho de 1987, e considerando as disposições contidas na Lei n. 18.451, de 6 de abril de 2015, e no Decreto n. 2.069, de 3 de agosto de 2015,

RESOLVE:

Art. 1.º Com o objetivo de assegurar a integridade do arquivo que contém o algoritmo matemático desenvolvido pelo IPT - Instituto de Pesquisas Tecnológicas, para fins de apuração dos bilhetes premiados no âmbito do Programa de Estímulo à Cidadania Fiscal do Estado do Paraná, foi gerada a seguinte chave única de codificação digital - "hash code", obtida com a aplicação do algoritmo MD5 - "Message Digest Algorithm 5", de domínio público: e156138d2c4d620b956f8ce3aeb1c561.

Art. 2.º Esta Resolução entra em vigor na data de sua publicação.

Secretaria de Estado da Fazenda do Paraná, em 2 de dezembro de 2015.

MAURO RICARDO MACHADO COSTA
SECRETÁRIO DE ESTADO DA FAZENDA

107726/2015

RESOLUÇÃO SEFA Nº 1.316/2015

SÚMULA: Disponibiliza a consulta aos bilhetes eletrônicos gerados ao consumidor para fins de sua participação no sorteio de prêmios no âmbito do Programa de Estímulo à Cidadania Fiscal do Estado do Paraná.

O SECRETÁRIO DE ESTADO DA FAZENDA, com fundamento no inciso XIV do art. 45 da Lei n. 8.485, de 3 de junho de 1987, e considerando as disposições contidas na Lei n. 18.451, de 6 de abril de 2015, no Decreto n. 2.069, de 3 de agosto de 2015, e no Regulamento do Sorteio "Nota Paraná" anexo à Resolução SEFA n. 626, de 3 de agosto de 2015,

RESOLVE:

Art. 1.º Ficam disponibilizados no portal "Nota Paraná", endereço eletrônico "www.notaparana.pr.gov.br", os números dos bilhetes eletrônicos gerados para o consumidor para fins de sua participação no sorteio número 001 do Programa de Estímulo à Cidadania Fiscal do Estado do Paraná.

Art. 2.º Com o objetivo de assegurar a integridade do arquivo eletrônico que contém a relação de todos os números dos bilhetes e seus respectivos titulares foi gerado, para fins de sua identificação e autenticação, a seguinte chave única de codificação digital - "hash code", obtida com a aplicação do algoritmo MD5 - "Message Digest Algorithm 5", de domínio público: 3d20738b56e93b0d99c413615bdd5878.

Art. 3.º Esta Resolução entra em vigor na data de sua publicação.

Secretaria de Estado da Fazenda do Paraná, em 2 de dezembro de 2015.

MAURO RICARDO MACHADO COSTA
SECRETÁRIO DE ESTADO DA FAZENDA

107713/2015

ESTADO DO PARANÁ
SECRETARIA DE ESTADO DA FAZENDA
CONSELHO SUPERIOR DOS AUDITORES FISCAIS

ATA DA SESSÃO ORDINÁRIA Nº 12/2015

No **primeiro dia do mês de dezembro de 2015, às 9h,** na sala de reuniões do 9º andar do Edifício Badep, sito na Av. Vicente Machado, 445, Curitiba/PR, foi aberta a **décima segunda Sessão Ordinária** do Conselho Superior dos Auditores Fiscais do exercício de 2015, atendendo a convocação realizada por meio do Edital nº 21/2015, de 25/11/2015, publicado no DIOE nº 9583, de 25/11/2015.

A sessão foi coordenada pelo presidente substituto Renato Mello Milaneze e contou com a presença dos conselheiros convocados, titulares Luiz Carlos Gallo, Edson Luciani de Oliveira e Gilmar Ciriaco da Silva e dos conselheiros suplentes Gerson Luiz Sarturi, Roberto Hideki Ito e Fernando José de Andrade, tendo sido designado o conselheiro suplente Fernando José de Andrade para secretariar e redigir a correspondente Ata da Sessão.

Inicialmente procedeu-se ao **sorteio - para a distribuição** aos Conselheiros - de 2 (dois) protocolados concernentes à área administrativa e/ou disciplinar, indicados no Edital nº 21/2015, de 25/11/2015, cujos expedientes ficaram assim distribuídos:

SID	INTERESSADO / ASSUNTO	CONSELHEIRO
13.857.835-6	Marcos Rogério Portes / Requer vistas e cópia integral do SID 13.786.517-3	Edson Luciani de Oliveira
13.232.484-0	Robinson Franco de Oliveira / Relatório da CPAD instituída pela Resolução SEFA 37/2015	Gilmar Ciriaco da Silva

O processo nº **13.669.328-0** - que constou no referido Edital para distribuição - foi **devolvido ao GRHS/SEFA** em 25/11/2015 - instruído com a Informação CSAF nº 9/2015, pois a análise requerida pela Paranaprevidência já havia sido feita pelo CSAF em 1º/9/2015.

Procedeu-se ainda ao **sorteio - para a distribuição** aos Conselheiros - de 1 (um) protocolado concernente à área administrativa, recebido neste Conselho após a publicação do Edital nº 21/2015, cujo expediente ficou assim distribuído:

SID	INTERESSADO / ASSUNTO	CONSELHEIRO
13.831.390-5	Companhia de Saneamento do Paraná / Renovação de disposição funcional	Luiz Carlos Gallo

Dos trabalhos de apreciação na presente sessão por parte dos senhores conselheiros, resultaram nas seguintes **deliberações**:

PROTOCOLO	INTERESSADO / ASSUNTO	DELIBERAÇÃO
13.741.681-8	Marcelo Muller Melle / Pedido de aposentadoria voluntária	Pedido de vistas
13.813.264-1	Luis Claudio Depes Eiras / Pedido de aposentadoria voluntária	Pedido de vistas
13.784.541-5	Cláudio Tosatto / Pedido de aposentadoria voluntária	Pedido de vistas
13.729.658-6	Marcel Giovani Kroetz / Recursos humanos	Pela abertura de sindicância
13.739.658-0	1ªVara Criminal de Ctba - Ofício 3184-15 / Informação CRE-COR nº 055/2015	Retirado de pauta o relatório não foi concluído pelo Relator
13.674.993-5	8ªDRR - Londrina / Relatório Sindicância	Pelo saneamento diligência à CRE/COR p/ oficiar ao M.P.

O AF Marcos Rogério Portes esteve presente à Sessão, onde acompanhou a distribuição por sorteio do processo nº 13.857.835-6, conforme por ele requerido no referido expediente.

Nada mais havendo a deliberar, às 16h00mim, o Presidente substituto do Conselho submeteu a Ata à apreciação dos presentes, que a aprovaram por unanimidade, subscrevendo-a e ato contínuo, encerrou a sessão.

Curitiba, 1º de dezembro de 2015.

Renato Mello Milaneze
Presidente substituto

Luiz Carlos Gallo
Conselheiro

Gilmar Ciriaco da Silva
Conselheiro

Edson Luciani de Oliveira
Conselheiro

Roberto Hideki Ito
Conselheiro Suplente

Gerson Luiz Sarturi
Conselheiro Suplente

Fernando José de Andrade
Conselheiro Suplente
Secretário *ad hoc*

107169/2015

Coordenação da Receita do Estado - CRE

PORTARIA Nº 372/2015

O DIRETOR DA COORDENAÇÃO DA RECEITA DO ESTADO, no uso das atribuições legais que lhe conferem os incisos X e XV do art. 9º do Regimento da CRE, aprovado pela Resolução SEFA nº 88/2005, resolve:

TIPO DE ALTERAÇÃO DATA OU PERÍODO	NOME RG CARGO NÍVEL	DE (LOTAÇÃO OU CARGO OU FUNÇÃO)	PARA (LOTAÇÃO OU CARGO OU FUNÇÃO)
REMOVER EM **1º.12.2015**	LUIZ CARLOS CABRAL E SILVA COELHO, RG nº 1.555.231-0, AF-1, **Função Gratificada "F"**	Administração Central da Coordenação da Receita do Estado - AGTI	Administração Central da Coordenação da Receita do Estado - IGA

Curitiba, 1º de dezembro de 2015

Mauro Ferreira Dal Bianco
Assessor Geral - CRE/GAB
Delegação de Competência - Portaria 298/2015

107332/2015