

Sorteio de Prêmios da Nota Fiscal Paulista

Descrição do Software de Escolha dos Bilhetes Premiados

O software de Sorteio Eletrônico da Nota Fiscal Paulista foi desenvolvido no Instituto de Pesquisas Tecnológicas do Estado de São Paulo (IPT), pela equipe técnica do Centro de Tecnologia da Informação, Automação e Mobilidade (CIAM), para a Secretaria da Fazenda do Estado de São Paulo (SeFaz).

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.

Introdução

A geração de números aleatórios com computadores só é possível com a ajuda de fontes externas de aleatoriedade, porém não há garantias 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 calma 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 pseudo-aleatórios, 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. As seqüências 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 seqüência de números, gerada a partir de sementes iguais, sempre será a mesma, permitindo a reprodutibilidade e a garantia da qualidade das seqüências numéricas. A qualidade da semente é considerada crítica para a geração dos números: a garantia da qualidade e da imprevisibilidade das seqüências numéricas será dada pela alta entropia, ou melhor, pela variação de valores da semente.¹

Para o sorteio de prêmios da Nota Fiscal Paulista (Not@FiscalPaulista) foi escolhido como semente dezesseis (16) dígitos da extração da Loteria Paulista, que possui as características de imprevisibilidade, tão necessárias para o perfeito funcionamento do algoritmo.

Algoritmo AES

O Advanced Encryption Standard (AES) é um algoritmo de criptografia (cifra) selecionado pelo

¹ Random Number Generators: An Evaluation and Comparison of Random.org and Some Commonly Used Generators:

<http://www.random.org/analysis/Analysis2005.pdf>

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 Encryption Standard (DES ³), o algoritmo anteriormente recomendado pelo NIST. O algoritmo originalmente conhecido como Rijndael foi o vencedor da seleção para o AES. Ele foi projetado levando em conta experiências dos autores nos algoritmos Square e Shark, e incorporou proteção a diversos ataques conhecidos, mantendo a eficiência e simplicidade ⁴.

O AES é uma cifra de bloco simétrica que permite a encriptação e a decriptação 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.

Geração dos números para o Sorteio Eletrônico

A partir do algoritmo AES, foi construído um gerador randômico de números inteiros de 32 bits, correspondente ao tipo **int** e à classe **Integer** da linguagem **Java**. O gerador randômico 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 SeFaz, de acordo com seus procedimentos internos. A lista de bilhetes consiste de uma seqüência de números inteiros entre um e um valor máximo. A quantidade de prêmios deve ser menor ou igual à quantidade de bilhetes, e cada bilhete pode ser sorteado apenas uma vez.

Foram desenvolvidos dois algoritmos diferentes para a realização do sorteio: o Gerador e o Embaralhador.

Gerador

O Gerador trabalha produzindo uma lista de números inteiros positivos (entre 1 e 231) a partir do gerador AES. Os números gerados são recalculados de acordo com um algoritmo de mudança de faixa (na verdade, uma simples regra de três), gerando números inteiros que estão na faixa fornecida pela SeFaz. Os números repetidos, que eventualmente aparecem, são descartados prontamente, 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

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>

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

números não-repetidos quando a quantidade de prêmios é muito próxima a de bilhetes, esse algoritmo só é utilizado para situações em que no máximo 50% dos bilhetes sejam premiados.

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.

Embaralhador

O embaralhador trabalha gerando uma lista de números inteiros positivos seqüencial, com a mesma quantidade de bilhetes da lista da SeFaz. A lista é então embaralhada, utilizando como fonte de aleatoriedade o gerador 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 seqüencial. Esse algoritmo 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. Como a quantidade de prêmios foi inicialmente fixada em um milhão, esse algoritmo deve ser executado quando existirem até dois milhões de bilhetes. Esse algoritmo complementa o Gerador na situação de poucos bilhetes, evitando o problema de repetições com ótima eficiência.

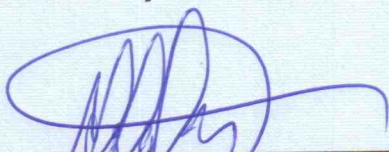
Num paralelo com o mundo real, o embaralhador pode ser comparado a uma urna contendo todos os bilhetes, que serão misturados várias vezes e após retirado um a um até o número de prêmios.

Procedimento Formal de entrega do software de sorteio de prêmios à SeFaz

Em 1º de dezembro de 2008 um representante do IPT, juntamente com a auditoria e representantes da SeFaz realizaram a lacração do notebook que realizará o sorteio, juntamente com o DVD, contendo o sistema operacional e o pacote de software desenvolvido pelo IPT, os quais serão executados no dia do sorteio.

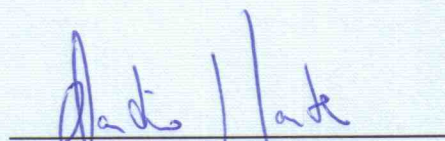
Qualquer atualização do software será enviada à SeFaz para posterior publicação, seguinte os mesmos critérios acima citados.

CENTRO DE TECNOLOGIA DA INFORMAÇÃO,
AUTOMAÇÃO E MOBILIDADE - CIAM



Alessandro Santiago dos Santos, MSc
Pesquisador Nre 8511-7
Responsável pela Seção de
Redes e Segurança Digital

CENTRO DE TECNOLOGIA DA INFORMAÇÃO,
AUTOMAÇÃO E MOBILIDADE - CIAM



Engº Claudio Luiz Marte, Dr.
Diretor do CIAM
CREA 060.178.361.9 – Nre 8458-2