Sorteios de Prêmios da Nota Fiscal Paulistana

Descrição do Software de Escolha dos Bilhetes Premiados

Conteúdo

O software de Sorteio Eletrônico da Nota Fiscal Paulistana foi desenvolvido no Instituto de Pesquisas Tecnológicas do Estado de São Paulo (IPT), pela equipe técnica da seção de Redes e Segurança Digital (SRSD), para a Secretaria de Finanças da Prefeitura Municipal de São Paulo - SF/PMSP. 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 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 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 sementes iguais, 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.[1]

Para o sorteio de prêmios da Nota Fiscal Paulistana foram escolhidos como semente dezesseis (16) dígitos da extração da Loteria Federal, que possui as características de imprevisibilidade, 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 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 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

---

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

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

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, correspondente 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 SF/PMSP, de acordo com seus procedimentos internos. A lista de bilhetes consiste de uma sequência 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.

Devido a restrição de não poderem ser sorteados números repetidos, surgem algumas questões de desempenho, que levaram a ser desenvolvidos dois algoritmos diferentes, construídos a partir do Gerador randômico AES para a realização do sorteio: 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 ótima desempenho, mas às custas 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 fornecida pela SF/PMSP. Os números repetidos, que eventualmente aparecem, são

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

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 da SF/PMSP. 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 após retirado um a um até o número de prêmios.

6 Procedimento Formal de entrega do software de sorteio de prêmios à SF/PMSP

Em 20 de Setembro de 2011 os representantes do IPT, juntamente com a equipe de auditoria externa e representantes da SF/PMSP realizaram a lacração do notebook que será usado para os sorteios, juntamente com o Live-DVD contendo o sistema operacional Ubuntu Linux e o pacote de software desenvolvido em linguagem Java pelo IPT, os quais serão deslacrados e utilizados somente nos dias dos sorteios, com acompanhamento dos auditores. Qualquer atualização do software será enviada à SF/PMSP para posterior publicação, seguindo os mesmos critérios acima citados.