GENERACION DE NUMEROS SEUDOALEATORIOS DE CALIDAD CRIPTOGRAFICA (NBCSPRBG)

1. DEFINICIONES

RBG (Random Bit Generator)

Es un dispositivo o algoritmo que genera a la salida una secuencia de dígitos binarios estadísticamente independientes e insesgados.

PRBG (Pseudo Random Bit Generator)

Es un algoritmo determinístico[1] que dada una secuencia realmente aleatoria de k bits de entrada, genera a la salida una secuencia binaria de longitud l >> k que "semeja"[2] ser aleatoria. Los k bits de entrada se definen como la semilla y la salida del PRGB una secuencia seudo aleatoria de bits.

[1] Determinístico significa que dada la misma semilla, la salida es siempre la misma
[2] La salida no es aleatoria, el número de salidas potenciales es a lo sumo una pequeña fracción (= $2^k/2^l$) de todas las secuencias binarias posibles de longitud l (= 2^l)

NBTPRBG (Next Bit Test Pseudo Random Bit Generator)

Un PRBG se define como NBTPRBG si no existe ningún algoritmo de tiempo polinómico[3] que dados los primeros l bits de la secuencia de salida s, pueda predecir el bit (l+1) con probabilidad mayor a ½

[3] El tiempo de corrida está acotado por un polinomio en función de la longitud l de la secuencia de salida

Complejidad algorítmica CLASE NP (Non-deterministic polynomial-time)

Son problemas matemáticos de alta complejidad para los cuales no se conoce un algoritmo de tiempo polinómico[3] que permita su resolución. Esta clase de problemas no son atacables computacionalmente si la longitud de su tamaño (parámetro de orden) crece suficientemente (P.ej., el problema de la factorización de números enteros, base del método criptográfico RSA, base de la plataforma PKI – public key infraestructure)

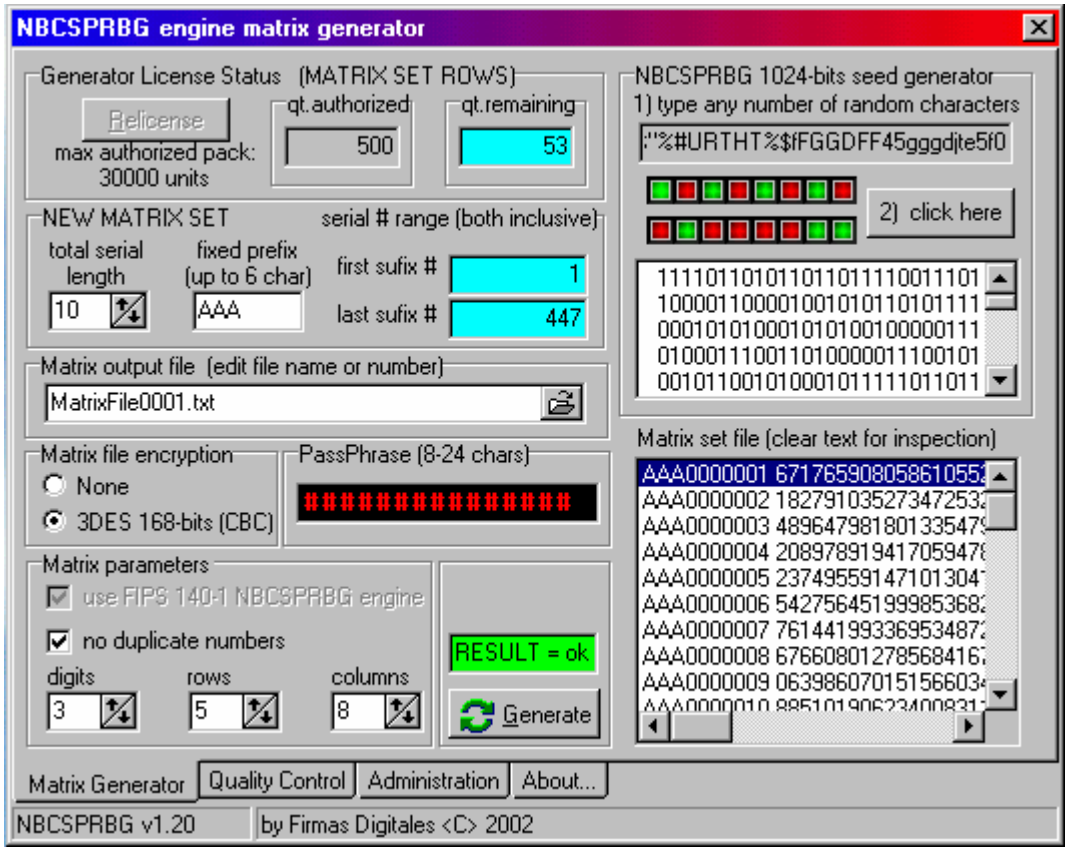
SESGO ESTADÍSTICO (BIAS)

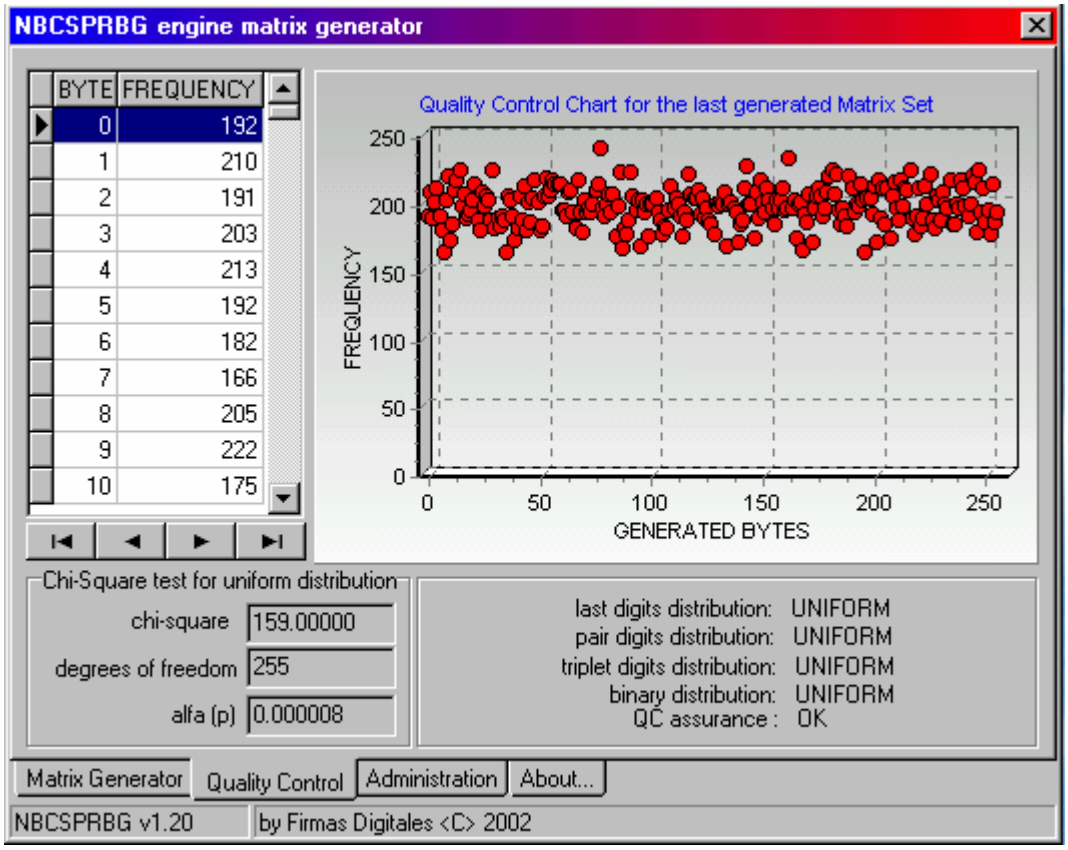
Es una tendencia de la secuencia de salida a generar patrones de auto correlación significativa, por lo cual desmejora sus calidad estadística. Se corrige aplicando iterativamente combinaciones lineales a dos o mas PRBG. Si se combina uno o más CSPRBG, el resultado es también un CSPRBG.

CSPRBG (Cryptographic Secure Pseudo Random Bit Generator)

Un NBTPRBG se define como CSPRBG si pasa la condición NBT (Next Bit Test) basándose en un problema CLASE NP. Esta es la categoría de máxima seguridad que se propone como módulo base del generador de PINES.

2. UNA INTERFASE MÍNIMA POSIBLE DEL MOTOR GENERADOR NBCSPRBG





Una salida modelo:

```
AAA0000001 667CB5B240AAC4419FECD2E3E4CB74E28B232DB7E5F3CBE34EE76F529887FAE535A0390
AAA0000002 A60F2C350E5528305D7CFC0A4BBE3D2AB91B9DF2484D3825CC898610F8A7D72155BCFEF
AAA0000003 1F6795968FE8E84A5A1FFA832321DD84FBD7D2121B92C14E7F6D35472C97F7D95A83B11
AAA0000004 06CAFC6B84E07EDC83559541BF5135C11FB1C72156954ED3BC61B21124D55B660B553CD
AAA0000005 B306EAD4B4B501BCB6D0AE1DBA638D24D8EEF8B5A1C390D98ECFE362935353C4446FF81
AAA0000006 CEC2F37F1D8CFD7A6EE3E3A20A40A3841831457647CDC2AA4BDF4D4C9AC07DDCA58DD7C
AAA0000007 37C5F93B2795F73681E81D901F7D5A728BE1F4665206DEA27572799197F7D406DDE77F3
AAA0000008 B13A96A41FF90FD2CA73F6B601686F1A2EE4C7D0A4965D45B69212E5896A419487E25D
AAA0000009 60EAF341D45C6C6D17E6ED3366E31BE0BBB766D41349F4B805558C474973E07D2CA3D3E
AAA0000010 149D60651A9EF09C7969493FD2B3602337C54A6DF7EDA53DE3C956BB4E05D8369F82B6E
AAA0000011 192116B4C65915AA90699F53E9BEDA964F70D63212851BCDD4225491DC2E516275AADE1
AAA0000012 52EBB6CFBA378DD7F2492F0371E7C1A99FBC5E2C98E47BF512934CF02FEA2BC1BC43A72
AAA0000013 7A531D41B55C2829E2E2C270CCB0AAE3AA6B93EBFB3D49271C2B1CBCF5862288BE01CC6
AAA0000014 B0C3F458589E6E37BB32072386CAB7DE5AF9BF7EC25A0D2040006FCAC1558F64EC6EAB06
AAA0000015 D136A1AB6059335978484721D73BE18EE122303CD2F3C68D617F0E8D7A683418D790231
AAA0000016 4CB2F6C99168F3CC443863BA608B6E0389D57F4A2D31B4AE41C2DC4DEC47843D99E1A2C
AAA0000017 42A1C6B303B75D958ACF15BD1864BA6C664CC1F01F525FDA58017D4353E1300E52E2F98
AAA0000018 25F564299025AA7C90371B1F2712A00AE61C2C373EFF724BD1A0F4547710B272C2FA4B4
AAA0000019 91BF5680B293166DD39F9476CAFB7EFFB8EBDAEDC1D176D08B5B5EABC33345D22601A75
AAA0000020 72EAFCCDF0800E41B59C4342389E23097B439631519D12CF856648BEE62A9492466C915
AAA0000021 FEBD3F3CF25E19FE586CFEFE5D5EA2A749584212 65A60E79C4CD4A0F047DC62B3149280
AAA0000022 CD6266985B9DC06939CFDDA82BDCAF352539D5298F9C6C5307921762 5D6062861B119CC
```

3. DISPONIBILIDAD DE PROGRAMAS DEMO

Estamos en condiciones de distribuir programas demo para evaluar nuestros productos.

4. REGISTRO DE MARCAS Y PROPIEDAD INTELECTUAL: