NOTE TECHNIQUE 24121999

Rédacteur : Élie AOUAD

Format des exposants secrets en fonction des valeurs de modulos

Le format des exposants secrets d'une bi-clé RSA peut être deviné dans certains cas de modulo. Les octets de début sont facilement définis.

En effet partons des formules des clés RSA :

N = p*q avec p et q premiers

et

S * V = 1 mod ((p-1)(q-1)) / (gcd(p-1)(q-1));

où S, V et N sont respectivement l'exposant privé, l'exposant publique et le modulo.

Comme p = 2*p'+1 et q = 2*p'+1 , le gcd((p-1)(q-1)) = gcd((2p')(2q')) = 2*gcd(p', q')

Pour des raisons de sécurité p' et q' sont premiers=> gcd(p',q') = 1

=>

S*V = (k *(p-1)(q-1))/ 2 + 1

=> Comme p*q = N, alors

S # k* N /V*2 (Approximation sur les grands nombres)

Exemple : Pour k = 1

N	V	Format de S
FF FF FF FF .. xxxxxx	3	2A AA A....
FF FF FF FF.. xxxxxx	10001	00 00 FF F...