

Lyrics ©1995 Stephen Savitzky. Some Rights Reserved¹
 To the tune of "To Anacreon in Heaven"

A
 Oh, say, PGP, and RSA public key
 A A₂ A E A B E
 Cryptosystems are simple, with primes q and p ;
 A A₂ A B E
 Call the product of one less than each of them k
 A A₂ A E A
 I pick d and e , whose product is 1 mod k .

A A₄ A A₄ A E A E7
 Now I just publish d , and the product qp ,
 A A₂ A E7 A B E
 You raise d to the power of message block b ;
 A E A EA DEA E
 Take that modulo pq and send it to me.
 A E A D A E A D E7 A
 And I'll use it as the exponent of private key e .

Now this program can fit into three lines of code,
 Using `perl` and `dc`, though the logic's distorted.
 Cryptographic machines are a weapon of war,
 And the government says they must not be exported.

Make a barcoded card, or if you are a bard
 run the code through a modem, it's not very hard.

Now, if I were being mean I'd stick some modem tones in here

Then this song would be a munition, its music you could never take
 From the land of the free, and the home of the brave.

The description of the RSA public key cryptography algorithm is mathematically accurate; though it's worth noting that any practical implementation will do the exponentiation and modules in a single operation. Perhaps the only obscure point occurs when specifying that $de \equiv 1 \pmod{(p-1)(q-1)}$. The twisted phraseology that defines k as $(p-1)(q-1)$ is particularly kludgy, but what the hell, it scans.

¹This work is licensed under a Creative Commons Attribution-Noncommercial-Share Alike 4.0 License.
 From the Songbook of Steve Savitzky 19950605 Hyperfpace Express