Modular exponentiation and the computational complexity of factoring large numbers

A D A
Now some folks think all your secrets should be exposed to view,
D A E7 Esus4E7
Like what you read, and what you think, and who's in bed with who.
D A Asus4A Asus2 A
Now they've built a chip called Clipper to help them tap your phone,
D A E7 Esus4E7
And read the private e-mail, that's meant for you alone.
D A
They say they're after terrorists and child pornography;
E7 A E7
They say they'll get a search warrant before they steal your key.
DA D G D
They say it's voluntary; and if you believe that tale
G D G A D
I hope you brought your checkbook 'cause I have a bridge for sale

DA D G D A D G D A D
Sink the Clipper! Keeping secrets keeps us free. They can have my private key
G D A DA D
When they pry it from my cold dead fingers' grip. Sink the Clipper!
G D A D GD A D G D A D
You can tell the NSA, the FBI and the CIA Just where the hell to shove that Clipper chip...

But with simple mathematics you can make a pair of keys;
Each unlocks the others' messages; it's easy as can be.
Just keep one tightly guarded, spread the other far and wide,
And not even nosy bureaucrats can read what you can hide.
If I want to send a message that is only meant for you,
I encrypt it with your public key and send the message through.
Your private key unlocks it, then you use my public key
To prove my private signature has damned well come from me.

Now, the next verse would have had the algorithm in it, but if I did that I'd get into trouble, and besides it's already been written, so I'll give you the links instead. If you're in the US you can FTP Phil Zimmermann's Pretty Good Privacy from `soda.berkeley.edu` *or buy a commercial version from Viacrypt. Don't ship it over the border, though, or they'll bust your ass for exporting munitions without a license. That's gun running, folks. I'm not making this up.*

So if you're outside *the US, you can get it from* `ftp.demon.co.uk`. *If you're* in *the US, though, don't touch it, or Public Key Partners will* sue *your ass for infringing their patent on the RSA algorithm, in spite of the fact that algorithms aren't supposed to be patentable.*

Get all that? Hope you encrypted it; there'll be a raid right after this set.
So put no faith in governments, for that's how freedom ends;
Trust proven mathematics, large numbers and your friends.
And tell no living soul the words that guard your private key;
Kick the cops off your computer using strong crypytography.
'Cause you wouldn't give the local cops the key to your front door;
Your thoughts are much more personal, so guard them all the more.
If they ask you for your private key then tell them where to go,
And if they offer you a Clipper chip then Just—Say—No!
refrain/coda
DA G D A
Get the Clipper Chip and the NSA, The FBI and the CIA
G D G D A
Packed off to Davey Jones today—Remember keeping secrets keeps us free;
G A D
And we'll—sink—the Clipper—in the sea.

The “cold dead fingers” quote is from John Perry Barlow of the Electronic Frontier Foundation.