

3 A PGP Matryoshka Doll

by Brother Myron Aub

Take out your favourite matryoshka doll, neighbour. Now piece by piece, open it until you can open it no longer. Every piece is smaller and closer to the end of the experience, and then—it stops: you can open the smallest piece no more.

But beware, neighbour! Not all matryoshka dolls behave like this. Some matryoshka craftsneighbours are tempted by the devil’s lures. They see no farther than the devil’s unholy promises of extensibility and compactness when they craft a matryoshka doll that can compress a larger one to fit within it! And our good neighbour Phil Zimmerman fell prey to this lure when designing the PGP doll format.²

When you want to send a message, you must first stuff it into a literal doll. You can then enclose that in an encrypted doll, a signed doll, or a compressed doll. How do you assemble these together? However you please! You can put your literal doll inside a signed doll inside an encrypted doll inside a compressed doll. Naturally, ciphertext compresses poorly, so this would be a stupid way to nest a PGP matryoshka doll. Normally you put your literal doll inside a signed doll inside a compressed doll inside an encrypted doll, but you can do it stupidly if you like.

And how do you open a PGP matryoshka doll? Since the sender could have assembled it however they pleased, you must be ready for anything. If you see an encrypted doll, you decrypt it and open the enclosed smaller doll. If you see a signed doll, you verify its signature—throwing it away if it fails to verify—and open the enclosed smaller doll. If you see a literal doll, you’re done and you read the message.

But what if you get a compressed doll? You decompress it—and hope there are no vulnerabilities in your system’s zlib—but unless some idiot tried to compress ciphertext, the enclosed doll will be *bigger* than the doll you just opened.

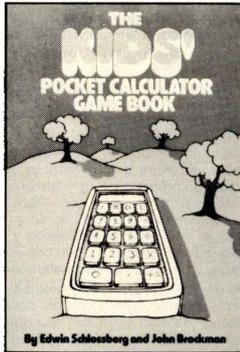
‘Surely,’ you say, ‘if someone assembled a PGP doll for me, it must have a literal doll buried inside it!’ But no, my poor, naïve neighbour! There is no rule that all PGP dolls be assembled like that. With the help of our neighbourly neighbour Russ Cox,³ and with a dab of holy water to dispel the devil’s temptations to misuse this black magic, we can craft a voodoo PGP doll from a quine, a self-reproducing program written in the *Lempel-Ziv compression language*, that bites any who naïvely try to open it up.

Our neighbour Tavis Ormandy discovered similar unholiness in IPsec.⁴ What other matryoshka dolls can you turn into voodoo dolls, good neighbour?

IT ALL ADDS UP TO EDUCATIONAL

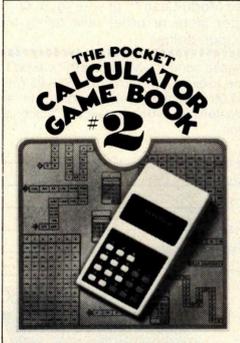
FUN

The creators of the original Pocket Calculator Game Book now present two fun-filled new game books for use with that incredible machine that has found a place in almost every home.



By Edwin Schlossberg and John Brockman

THE KIDS' POCKET CALCULATOR GAME BOOK
by Edwin Schlossberg and John Brockman
A quick trip through elementary mathematics—fun and games with real purpose. The first book of its kind for kids from kindergarten through college. Illustrated with line drawings and cartoons.
\$6.95 hardcover \$3.95 paperbound



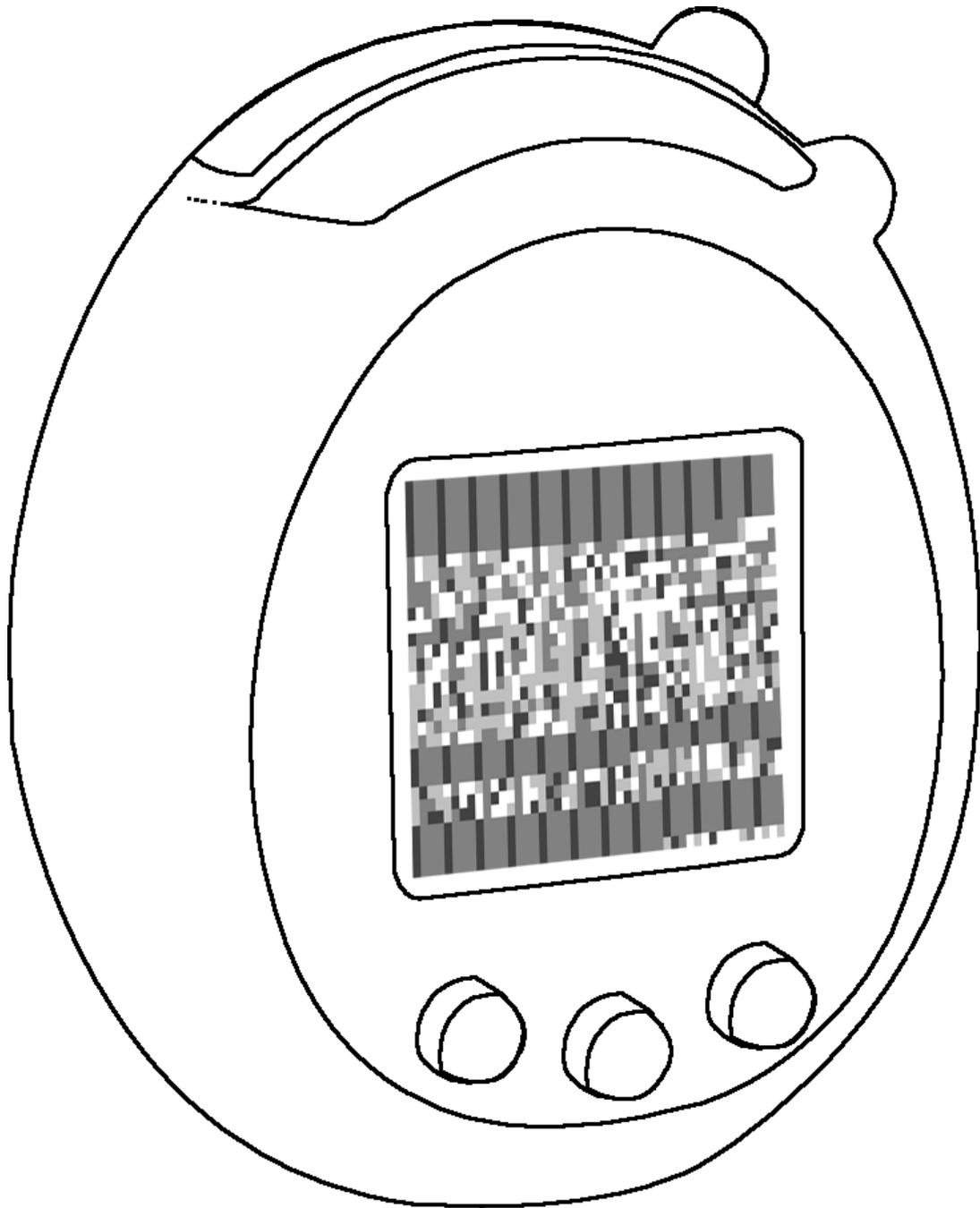
THE POCKET CALCULATOR GAME BOOK #2
by Edwin Schlossberg and John Brockman
Even more popular in approach than its famous predecessor, this book is simpler, more accessible, and its games are more mathematically basic. Illustrated with line drawings and cartoons.
\$6.95 hardcover \$3.95 paperbound

WILLIAM MORROW

²RFC 4880, ‘OpenPGP Message Format’

³Russ Cox, ‘Zip Files All the Way Down’, 2010-03-18

⁴Tavis Ormandy, ‘BSD derived RFC 3173 IPcomp encapsulation will expand arbitrarily nested payload’, CVE-2011-1547, posted to full-disclosure 2011-04-01



Hey kids! Can you reverse engineer this shellcode from the picture?