The Case of the RSA FUCK-A-DUCK certificate

Nadia Heninger
Zakir Durumeric
Eric Wustrow
J. Alex Halderman

N=pq

SSL certificates

- We scanned the Internet

SSL certificates

- We scanned the Internet
  - (It was awesome)

SSL certificates

- We scanned the Internet
  - (It was awesome)
    - Until amazon kicked us off

SSL certificates

- We scanned the Internet
  - (It was awesome)
    - Until amazon kicked us off
- 5,845,247.141592… certificates downloaded

SSL certificates

- Interesting results!


FACTOR ALL THE KEYS!

SSL certificates

- ~~Interesting results!~~
- Funny results!

"-----BEGIN RSA PRIVATE KEY-----" -openssl

Search

About 274,000 results (0.24 seconds)

Everything
Images
Maps
Videos
News
Shopping
More

All results
Related searches
More search tools

-----BEGIN RSA PRIVATE KEY - Pastebin.com - #1 paste tool since ...
pastebin.com/TbaeU93m
19 Apr 2010 – ... the difference. Copied. -----**BEGIN RSA PRIVATE KEY**-----.
MIICXwIBAAKBpenis1ePqHkVN9IKaGBESjV6zBrIsZc+XQYTtSlVa9R/4SAXoYpl ...

-----BEGIN RSA PRIVATE KEY - Pastebin.com - #1 paste tool since ...
pastebin.com/sC7bGw30
18 Apr 2010 – ... difference. Copied. -----**BEGIN RSA PRIVATE KEY**-----.
MIIEogIBAAKCAQEAvxBalhzKMewLvmIr1ptID1gO7EWGFyudzOAHLqm3+0+gpPbk ...

site:pastebin.com "-----BEGIN RSA PRIVATE KEY-----" - Posterous
cdevers.posterous.com/sitepastebincom-**begin-rsa-private-key**-google
20 Apr 2010 – Apr 19, 2010 ... -----**BEGIN RSA PRIVATE KEY**-----
MIICXwIBAAKBpenis1ePqHkVN9IKaGBESjV6zBrIsZc+ XQYTtSlVa9R/4SAXoYpl .

help/en/howto/sftp – Cyberduck
trac.cyberduck.ch/wiki/help/en/howto/sftp
Private keys containing a DSA or RSA private key in PEM format are supported (look for -----BEGIN DSA PRIVATE KEY----- or -----**BEGIN RSA PRIVATE KEY**----- ...

SSH access with a private RSA key [Archive] - VanDyke Software For…
forums.vandyke.com/archive/index.php/t-2185.html
2 Sep 2011 – -----**BEGIN RSA PRIVATE KEY**-----
MIIEogIBAAKCAQBujdbtxyIX4KaQPeTf5F/
aOSBwSpZN4MjTixU2Yq8JkipjMYpYwpNj1TODzRJf ...

Pastebin

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvxBalhzKMewLvmIr1ptID1gO7EWGFyudzOAHLqm3+0+gpPbk
JRfsItdn2xvp8Ye8KEcfZjb2kW80yCnkKFf4ecnzxI12m1y2IXOmu4SdWrPErabU
HmK6whIlkqCZAglF11Ntd6McXMt+aEFXEZ4fv1Tzg0wT4Lm4RwLQKDlMgyvSxi6Z
8lQ8IWuzQkYkYqYiSQCfPacFsmy1tV4O4CKT4Er+5+8cVCi50ETiRixHCqEHSve9
XuRMz5LfEqFsmHNj5QkICz4oANx1Ymop4qKz+q3ePq6bZeVRVFWedv01B56sWv8f
LkNekQChP5CedSuIc3N4SY7bKXUt43Z740WOqzQIBIwKCAQEAuZrbp8QyId38x5Q
/FxUoTD4jb/hWFZBhTFmEBKVd8mx/1Y8tlHA0WOJdcNYSbcOjYbrTVn21mwHY1vk
8/2vjECGZypV9gJKhuVgI9/pUMvjoWA7xb7+kKPp/Cb7CUrWIaGASFVOwIsqVqXf
9NsoE4DcFeC0eOmCOwwKhRgtFmohZw/puFrsSQKBgB0LEwIjmZ4m3LEAlfbSZt5e
wxGKk/EI7+EN7wQCTX4rlZBjXo8HwVPUjwBgWW65110vyA9ZS+4u4q/TodQIw2AC
RpUkk79XruzZOB5uQLMgXOLgFEz7ZZvnvMJsNbVBWUlAlKe7kZBmlGHfp8LsIhZ+
uckGBBC448hPppzBBkOFWJmk+EgpW8uA5vxnAKl9rhQAyTfyugo=
-----END RSA PRIVATE KEY-----
```

Pastebin

-----BEGIN RSA PRIVATE KEY-----

MIICXwIBAAKBpenis1ePqHkVN9IKaGBESjV6zBrIsZc+XQYTtSlVa9R/4SAXoYpI

upNrIjkCLd6DLDqfTO429xLDmYO4Ojzox7xiNcSMlBn8+TqTjf3TqAJmIOpgQVhJ

vW9is30teT7l2ynAyMYvGqwR0liCToMc/lOltlhPIFixw2AKUd0M5W76dwIDAQAB

AoGBAKDl8vuA9zUn2lTDddujAzBRp8ZEoJTxw7BVdLpZtgLWLuqPcXroyTkvBJC/

rbfPgYDdmgWc/lkpMufFe/-----BEGIN RSA PRIVATE KEY-----

FUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A

….

DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCKFUCK A DUCK5VKnb4

Psg1RMTRceI/z3d/3BiuDjiUiRICFqOXDscCQQDFea/ocg8VVLvH/6pn7oNTQfbx

tkqCSSne3XgjAM+eA6TXbIo49d+3gsM3U1mGHR9ZBMy0O68ijhIqM7/7nJtBAkEA

jmkwiP2Fy0tQ9heq4rx90ZfmixcWf/H6JldRy7kJ/qG6uDnPvH55mTRuGPpas044

7sJphlPEY8ofkwJj7K/ZKQJBAIc75HQi/Br1lRC4qPmF2vwYgwpyF9RbZWO56Eo7

ipgts4FLFajgogOD+JxkkT1CXtEv7MqM6ihSxGVBD6UHN7I=

-----END RSA PRIVATE KEY-----

Unfucking the duck

```
-----BEGIN RSA PRIVATE KEY-----
MIICXwIBAAKBpenis1ePqHkVN9IKaGBESjV6zBrIsZc+XQYTtSlVa9R/4SAXoYpI
upNrIjkCLd6DLDqfTO429xLDmYO4Ojzox7xiNcSMlBn8+TqTjf3TqAJmIOpgQVhJ
vW9is30teT7l2ynAyMYvGqwR0liCToMc/lOltlhPIFixw2AKUd0M5W76dwIDAQAB
AoGBAKDl8vuA9zUn2lTDddujAzBRp8ZEoJTxw7BVdLpZtgLWLuqPcXroyTkvBJC/
rbfPgYDdmgWc/lkpMufFe/5VKnb4
Psg1RMTRceI/z3d/3BiuDjiUiRICFqOXDscCQQDFea/ocg8VVLvH/6pn7oNTQfbx
tkqCSSne3XgjAM+eA6TXbIo49d+3gsM3U1mGHR9ZBMy0O68ijhIqM7/7nJtBAkEA
jmkwiP2Fy0tQ9heq4rx90ZfmixcWf/H6JldRy7kJ/qG6uDnPvH55mTRuGPpas044
7sJphlPEY8ofkwJj7K/ZKQJBAIc75HQi/Br1lRC4qPmF2vwYgwpyF9RbZWO56Eo7
ipgts4FLFajgogOD+JxkkT1CXtEv7MqM6ihSxGVBD6UHN7I=
-----END RSA PRIVATE KEY-----
```

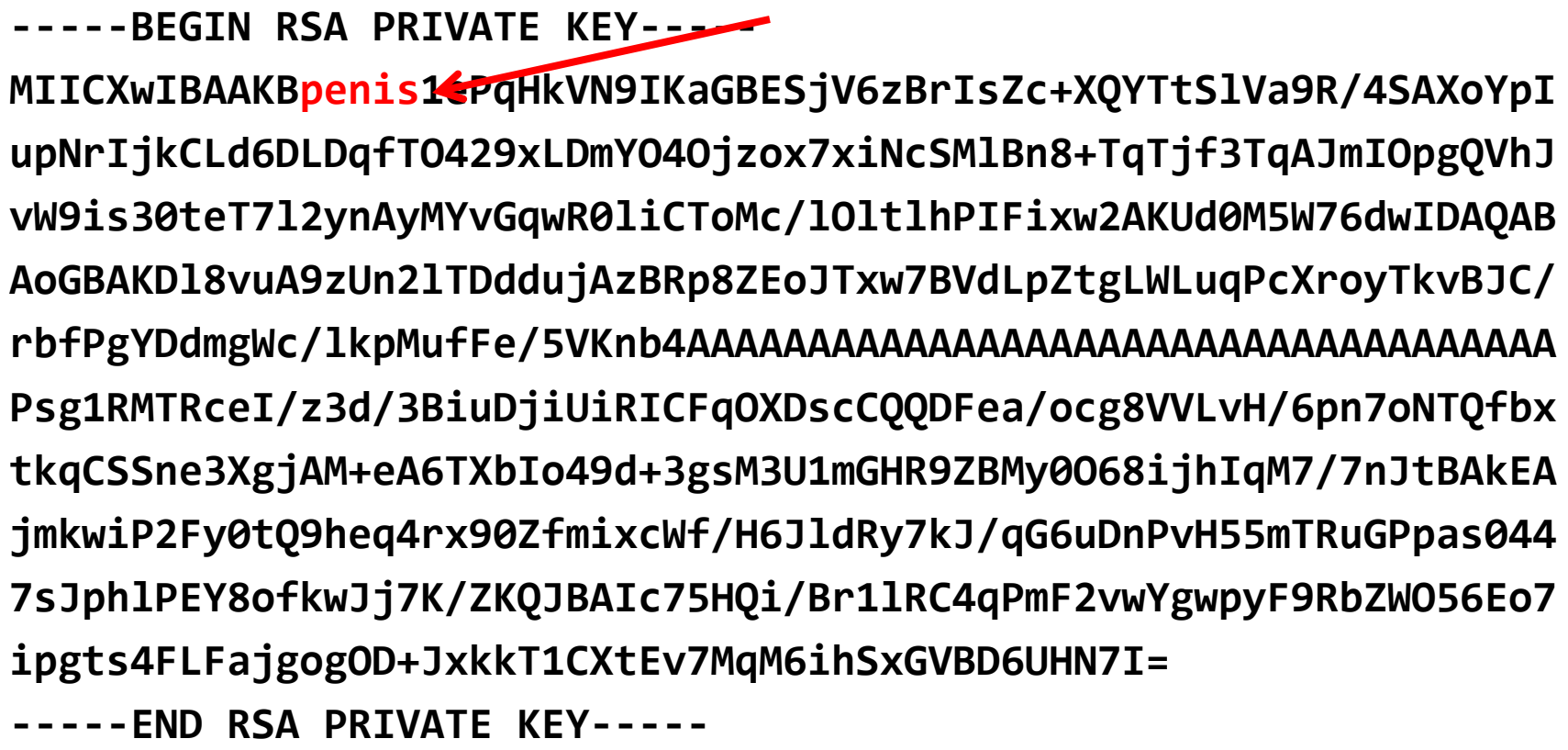
Unfucking the duck

```
-----BEGIN RSA PRIVATE KEY-----
MIICXwIBAAKBpenis1ePqHkVN9IKaGBESjV6zBrIsZc+XQYTtSlVa9R/4SAXoYpI
upNrIjkCLd6DLDqfTO429xLDmYO4Ojzox7xiNcSMlBn8+TqTjf3TqAJmIOpgQVhJ
vW9is30teT7l2ynAyMYvGqwR0liCToMc/lOltlhPIFixw2AKUd0M5W76dwIDAQAB
AoGBAKDl8vuA9zUn2lTDddujAzBRp8ZEoJTxw7BVdLpZtgLWLuqPcXroyTkvBJC/
rbfPgYDdmgWc/lkpMufFe/5VKnb4
Psg1RMTRceI/z3d/3BiuDjiUiRICFqOXDscCQQDFea/ocg8VVLvH/6pn7oNTQfbx
tkqCSSne3XgjAM+eA6TXbIo49d+3gsM3U1mGHR9ZBMy0O68ijhIqM7/7nJtBAkEA
jmkwiP2Fy0tQ9heq4rx90ZfmixcWf/H6JldRy7kJ/qG6uDnPvH55mTRuGPpas044
7sJphlPEY8ofkwJj7K/ZKQJBAIc75HQi/Br1lRC4qPmF2vwYgwpyF9RbZWO56Eo7
ipgts4FLFajgogOD+JxkkT1CXtEv7MqM6ihSxGVBD6UHN7I=
-----END RSA PRIVATE KEY-----
```

Add padding

```
-----BEGIN RSA PRIVATE KEY-----
MIICXwIBAAKBpenis1ePqHkVN9IKaGBESjV6zBrIsZc+XQYTtSlVa9R/4SAXoYpI
upNrIjkCLd6DLDqfTO429xLDmYO4Ojzox7xiNcSMlBn8+TqTjf3TqAJmIOpgQVhJ
vW9is30teT7l2ynAyMYvGqwR0liCToMc/lOltlhPIFixw2AKUd0M5W76dwIDAQAB
AoGBAKDl8vuA9zUn2lTDddujAzBRp8ZEoJTxw7BVdLpZtgLWLuqPcXroyTkvBJC/
rbfPgYDdmgWc/lkpMufFe/5VKnb4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Psg1RMTRceI/z3d/3BiuDjiUiRICFqOXDscCQQDFea/ocg8VVLvH/6pn7oNTQfbx
tkqCSSne3XgjAM+eA6TXbIo49d+3gsM3U1mGHR9ZBMy0O68ijhIqM7/7nJtBAkEA
jmkwiP2Fy0tQ9heq4rx90ZfmixcWf/H6JldRy7kJ/qG6uDnPvH55mTRuGPpas044
7sJphlPEY8ofkwJj7K/ZKQJBAIc75HQi/Br1lRC4qPmF2vwYgwpyF9RbZWO56Eo7
ipgts4FLFajgogOD+JxkkT1CXtEv7MqM6ihSxGVBD6UHN7I=
-----END RSA PRIVATE KEY-----
```

Unfucking the duck



Removing the private part

- “penis” -> gQDET
  - Length field (known)
  - ASN1 header field (known)
- “AAAAAAAAAAAA” -> ???
  - Half the bits of one of the primes (prime2, unknown)
    - prime2 = modulus / prime1

Huzzah!

```
-----BEGIN RSA PRIVATE KEY-----
MIICXwIBAAKBgQDET1ePqHkVN9IKaGBESjV6zBrIsZc+XQYTtSlVa9R/4SAXoYpI
upNrIjkCLd6DLDqfTO429xLDmYO4Ojzox7xiNcSMlBn8+TqTjf3TqAJmIOpgQVhJ
vW9is30teT7l2ynAyMYvGqwR0liCToMc/lOltlhPIFixw2AKUd0M5W76dwIDAQAB
AoGBAKDl8vuA9zUn2lTDddujAzBRp8ZEoJTxw7BVdLpZtgLWLuqPcXroyTkvBJC/
rbfPgYDdmgWc/lkpMufFe/TC+KgIDlWo50Pm/cwcChaM9nEINbFF1dqoA5gVxv6g
yUWQNKVKerToh/L3OpbiApArfB2aiimXUDH0eiGev6i6h0ShAkEA/MCm4KwarMP9
gPy2V/9qlJ1mEgZXMjHG4nWBfgPQE+9Lq1+e6kMePpuFgAC5ZJC8an4PC0LU5QIV
XBUW2uLG0QJBAMbVClSWms3llVT5IjKFNLdz0ShSu0Fh5UzRpMkxtEGYsO5VKnb4
Psg1RMTRceI/z3d/3BiuDjiUiRICFqOXDscCQQDFea/ocg8VVLvH/6pn7oNTQfbx
tkqCSSne3XgjAM+eA6TXbIo49d+3gsM3U1mGHR9ZBMy0O68ijhIqM7/7nJtBAkEA
jmkwiP2Fy0tQ9heq4rx90ZfmixcWf/H6JldRy7kJ/qG6uDnPvH55mTRuGPpas044
7sJphlPEY8ofkwJj7K/ZKQJBAIc75HQi/Br1lRC4qPmF2vwYgwpyF9RbZWO56Eo7
ipgts4FLFajgogOD+JxkkT1CXtEv7MqM6ihSxGVBD6UHN7I=
-----END RSA PRIVATE KEY-----
```


https://cyberground.hu

Conclusion

- “FUCK-A-DUCK” is not good crypto
- Pastebin is not a secure cloud store
- Probably shouldn’t put your private key in a “secure” cloud store anyway
- Probably shouldn’t fuck a duck