CMU Computer Club Talk Series

Public Key Cryptography and PGP

RSA

- Published in 1977 by Rivest, Shamir, Adleman
- Based on difficulty of factoring, and finding roots modulo composite numbers

Secret key: Two prime numbers, p, q
Public key: Product pq
Message: m

Encryption: $m^e \bmod pq$
Decryption: $m^{1/e \bmod (p-1)(q-1)} \bmod pq$

State of Internet Security in 1991

- Basically nothing
- No encryption
- No https
- No SSL
- No ssh
- Many exploits

It's dangerous to go alone, take this!

```
-----BEGIN PGP MESSAGE-----
Version: 2.0

sFR6e5RwkQEIbqZBWKFvaP6gyNDlGuUsZFnwOezKxC3pPM8wdm/T2mUzwOzByqBy
ZbuJ8O0aWyijAWUutscSemxXcTnI5Fr6Lckc/Cuh8p0SuVuC4xJmI4agpQqGBRMs
ezYxNHY2HlYFn9t5ViM+OeUqwMiCxX+I4vm0lJZpdqXh9lppMnmeCCwkDlQ6ECw9
cToMCkaEzfz2MpNAY6Ggf1IU0MRHMtvFxA2afKcKyNQzMDdpMifK+ZmX9/k9Pcbo
SJV9uCX/jpxjNPE5FNm7szDCtBhvcqk002fkafPk9XhRaeR+f5JNPBJhw+L+VYKO
JuMQb4AwbqFOfvdN/gaVpoe9Abdz72pP68FLSmBwG+vw9Ktf2rfiOL3yug+zy264
pZy+XjTRdGKsX6fmuGCGa6nQWA/XWVT30DBnml2xtX5O4HdFhHe7fZTqnswPc2/M
nw1ZxL6SqTKHcIDAQ62NIWpKAtK7hUAx7PgjfNKnNMEHOGDDJy5cGTZZLyyN4/9q
GEfPod9kOEliV3WqTQ/FYy2n9fQ+/xeCzuJA0ODRfj5Tu+rDvwRInFF2wdFXLDzG
LB+OQJW2NClgQu05NhxkIZqzHaNX1DHRDn6m/jaSz2nUZ2HJknKH/RBD9765roCV
Pg+C+ozZJw1MtyCibsAXpyRG/+LNS7XhJcBJHA==
=eTLS
-----END PGP MESSAGE-----
```

```
-----BEGIN PGP SIGNED MESSAGE-----

This is a message.

-----BEGIN PGP SIGNATURE-----
Version: 2.0

iQCVAwUBPjlRxWfhK324XxlBAQFdhgP/bdHMqstLCvXG8pGIfc7OzgUySzjewx1T
GU+zi7aJzcj4WWrOxsSqceNyroIMTXpwBOwb1OP8kbBzGr+TW9Kzb+1P/UdMmnHH
qgsZbXAcf3dVUwEPhrgn5XhxXk6mPocAvL0/7VhwHClbGPAefvrcKhkAyrSfxIP2
i697b7szCeU=
=5oN9
-----END PGP SIGNATURE-----
```

PGP Source Code Book