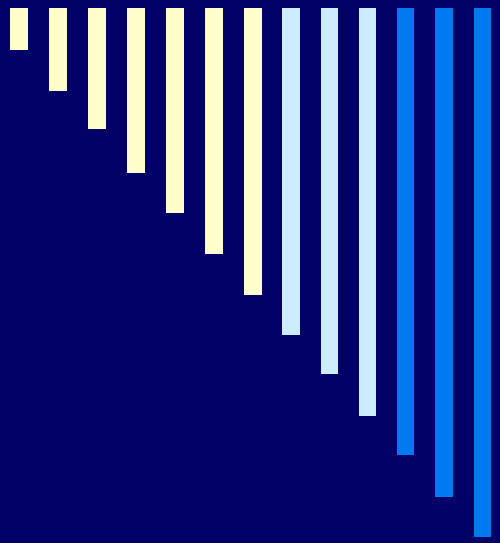
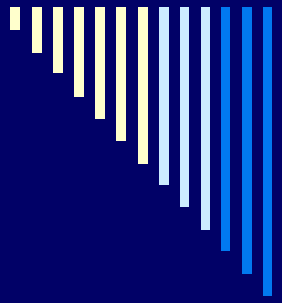


PGP (Pretty Good Privacy) INTRODUCTION

ZHONG ZHAO



In The Next 15 Minutes, You May Know…

- What is PGP?
- Why using PGP?
- What can it do?
- How did it evolve?
- How does it work?
- How to work it?
- What's its limitation?

What is PGP?

- A popular program widely used by individuals and corporations…(free and commercial version)
- Giving your electronic mail PRETTY GOOD PRIVACY by encrypting your mail
- When encrypted, the message looks like a meaningless jumble of random characters
- The result: nobody but only the intended person can revert and read the e-mail…
- Prove to be capable of resisting even the most sophisticated forms of analysis aimed at reading the encrypted text
- Can also digitally sign information to ensure its authenticity

Random Characters

American
FINANCE

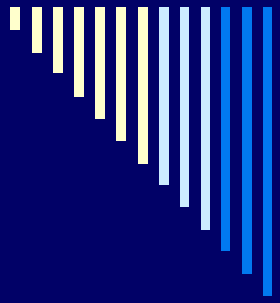
To: John Price (jprice@americanfinance.com);
From: Lizzy King (eking@americanfinance.com);
Subject: Immediate RIFs

John,
Do you know who they're thinking about cutting next? I thought you said there weren't going to be any changes until next week. If others found out, there's no telling what they would try to pull. Our client has to be told before the others get in touch with them first!

Lizzy

Why PGP?

- Security
- Legal issue: Privacy
- Increasing risk: On every node through witch the email is transferred there is a chance that it can be intercepted unintentionally or intentionally
- Authentication



PGP Features

- Encrypt/sign and decrypt/verify within any application;
- Create and manage keys;
- Create self-decrypting archives (SDAs);
- Permanently erase files, folders, and free disk space;
- Secure network traffic;

PGP Milestones

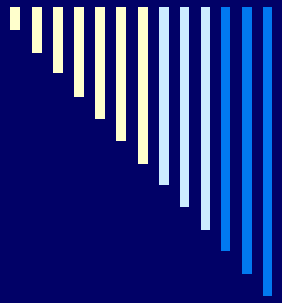
- 1991
  - Phil Zimmermann releases version 1.0 of Pretty Good Privacy;
- 1996
  - PGP 4.5 released with simple user interface and a mail plug-in for Eudora;
- 1997
  - PGP 5.0 released; first complete product code rewrite since version 1.0;
  - PGP 5.5 released for both Business and Personal with PGP Admin;
- 1998
  - PGP 6.0 released with PGP Disk for Windows and a mail plug-in for Microsoft Outlook, witch is still free for non-commercial use. A graphical interface was written for the Windows and Mac versions

PGP Milestones (Cont')

- 1999
  - PGP 6.5 released with Virtual Private Network (VPN) and full X.509 support;
- 2000
  - PGP 7.0 released based on new MS Windows code. Major version includes PGP Firewall, ICQ Instant Messenger plug-in, Windows 2000 support, Notes mail plug-in, and PGP Admin for large deployments;
  - PGP 7.0.3 released for Individual and Freeware users; PGP 7.0.4 released for Enterprise users;
- 2001
  - PGP 7.1 released, including a Corporate Desktop Suite (PGP Mail, PGP Disk, PGP VPN, and PGP Firewall);
- 2002
  - PGP 8.0 released for Macintosh and Windows;
  - PGP Corporation releases source code for peer review;

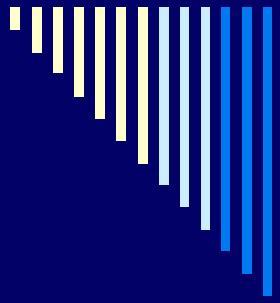
PGP Milestones (Cont’)

- 2003
  - PGP Personal 8.0 named Best Encryption Software and one of CNET's Top 100 Products;
  - PGP Enterprise 8.0 receives Reader Trust Award for Best Encryption, SC Awards Council's Best Encryption Solution (Highly Commended), and SC Awards Council's Best Email Security (Highly Commended) from *SC Magazine;*
  - PGP Corporation signs distribution agreement with Ingram Micro, the largest global wholesale provider of technology products and supply chain management services;
  - PGP Corporation announces and ships PGP Universal, a new self-managing security architecture and product line



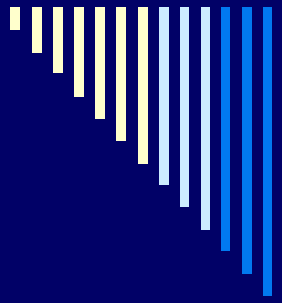
Cryptography: The Two Basic Encryption Techniques

- Symmetric and asymmetric (public-key)
- The latter is widely accepted
- PGP is based on it



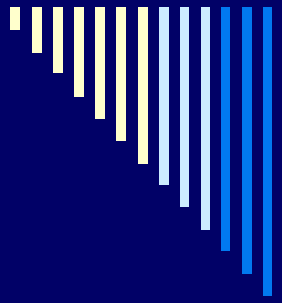
Symmetric Encryption

- Involves only one key, which is used by both the sender for encrypting and the recipient for decrypting
- Symmetric algorithms: blowfish, Triple-DES, AES (Advanced Encryption Standard), CAST (Carlisle Adams and Stafford Tavares) , IDEA (International Data Encryption Algorithm, legally restricted, but the other algorithms may be freely used)
- A key size of 128 bits is currently considered to be sufficiently secure, key sizes of 56 bits or less can be considered crackable
- Problem: the means of distributing the key



Asymmetric (Public-Key) Encryption

- Solves the problem of distributing keys by using one pair of complimentary keys, one public and the other private
  - Public: freely exchanged to others without fear of compromising security
  - Private: only you have access, should be carefully protected
- A message is encrypted to a recipient using the recipient's public key, and it can only be decrypted using the corresponding private key



Asymmetric (Public-Key) Encryption (Cont')

- Public key algorithms were developed in the 1970's in two main camps
  - The first, RSA (Rivest, Shamir, and Adleman), was patented in the U.S. making its implementation restricted legally (till September 2000)
  - The second, DH (Diffie-Hellman), is not legally encumbered in this way
- A key size of 2048 bits is sufficiently secure

RSA Algorithm—Factorization

- p, q—prime numbers (secret and normally > 100 digits);
- n=pq, function $\Phi(n)=(p-1)(q-1)$ (that's the number of numbers that ≤ n and prime to n);
- Let a big integer "e" (<n, public) be "encryption index" that prime to $\Phi(n)$;
- Equation $ed=1 \bmod \Phi(n)$; figure out "decryption index" "d";
- X=Plaintext while Y=Ciphertext;
  - Encryption process: $Y=X^e \bmod n$
  - Decryption process: $X=Y^d \bmod n$
- Keys: (n, e)—public key, (n, d)—private key;
- To get X, have to get "d" directly, otherwise…

Can You figure It Out???

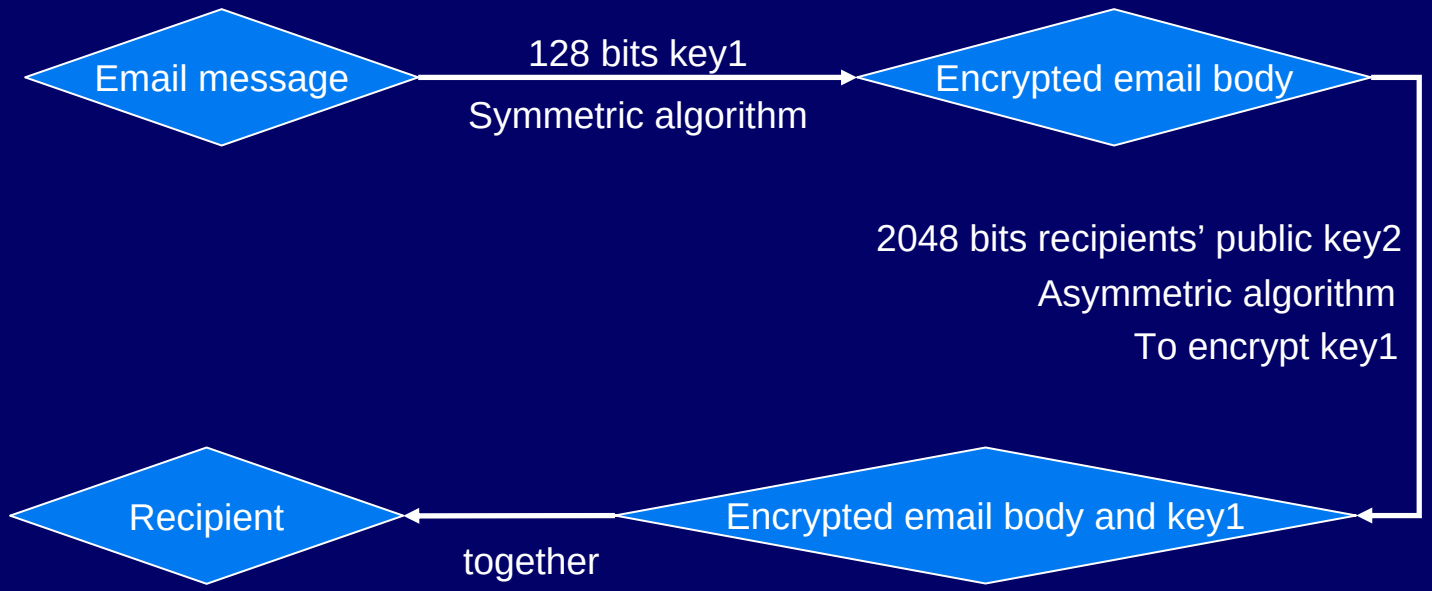
- Given the computing cycle of 1μs ($1x10^{-6}$ second), the time needed to factorize the binary number “n” (finding “d”):

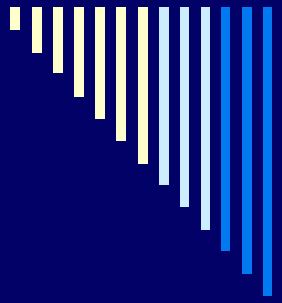
Digit	100	200	300	500	750	1000
Time needed	30 seconds	3 days	9 years	1 million years	$2x\ 10^{9}$ years	$6x\ 10^{15}$ years

- Factorization is impossible if “n” is big enough…

PGP Protocol

- PGP chooses to use a kind of hybrid public key encryption for the protocol, incorporating both symmetric and asymmetric encryption methods

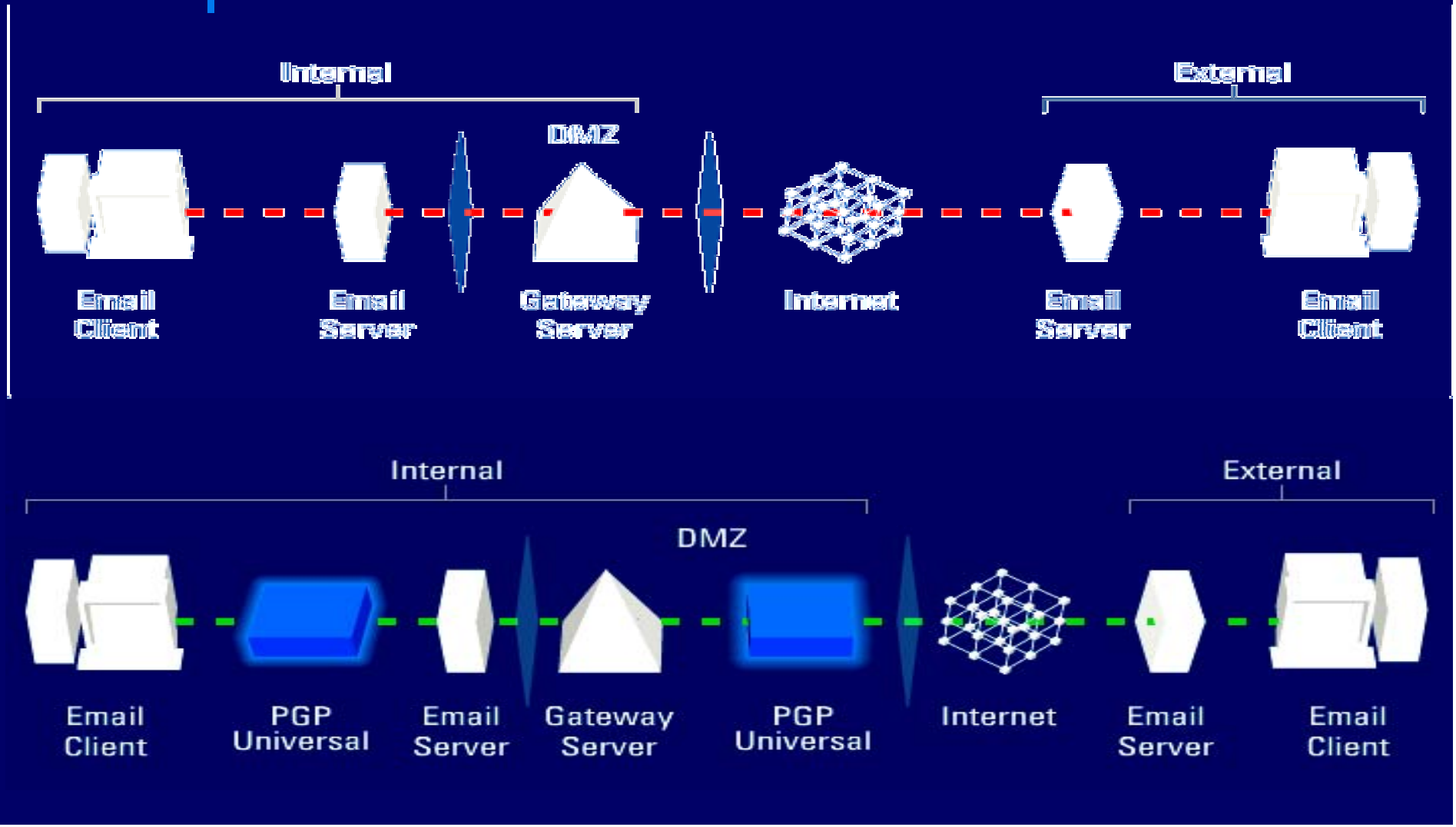




Four Key Parts of PGP Security System

- A symmetric encryption algorithm: IDEA (International Data Encryption Algorithm)
- A asymmetric encryption algorithm: RSA (Rivest, Shamir, and Adleman)
- A one-way hash algorithm: SHA-1 (Secure Hash Algorithm) or MD5 (Message Digest 5)
- A random number generator

Before and After (PGP Universal)



PGP Showtime

- Create a private and public key pair;
  - Passphrase is a string of characters or words you want to use to maintain exclusive access to your private key;
  - The generated key pair is placed on the public and secret key rings;
  - Backup;
- Exchange public keys with others;
  - Make your public key available through a public key server (e.g. ldap://keyserver.pgp.com, http://search.keyserver.net);
  - Include your public key in an email message;
  - Export your public key or copy it to a text file;
- Validate others' public keys;
  - Compare the unique fingerprint on the copy of someone's public key to the fingerprint on that person's original key;
  - Also can accept a key as valid based on the presence of a signature from a trusted introducer (e.g. Certificated Authority);

Search Result From http://www.keyserver.net

PGP Public Key Block Sample

mQGiBD+2kHoRBAD0iwwIikVaM3JCX/InHuYRfKlGsiUswThGa6DCoJDuY5+XW22s
i9PY3WlukSUa+HLuqcy+Jr92JMSETdXNbrcweaNa0RNSFGTWmZGk34aNrrvqigMO
2jTPN+kzBFzjgsOk+/zZpMds3olTCeoReV1sJlqTSqwtL4hNsl2ecMft3wCg/yq5
RHNkdoEqi9/PesyNI9HtX/sEANsI5mcKx2tElH0A/PxS0l4hZ5djwVO1f2fZr43p
Ek9TOGzys0RGARWaLr/hMwar83ET5ur4SE8VizobIqW2606TqFNHdsCHYQYM+kp0
1MrpfQzTMYHWsrrT4py4386QUIKoiIwYy2vdkrVRpSHkBVM515aFndiEU9wkwyy
6eMIBADZzW55J9GLGHlgb2T7HXt/XzHjwXZsH+WC7vW3DqVr1J4nFqGWSNCT049q
t6YQdiGaK/87y82qT0xSJZt7iaDvtlohQn43JLqK1m4F/MPkF3ZYzK5NNfcc2/gy
Mnw+Ezwe5rE9IpglwOwS9EAXqvPd6eDGAQ33A/rHMfy+wk65erQiWmhhbyBaaG9u
ZyA8emhhb196aHpoQGhvdG1haWwuY29tPohXBBARAgAXBQI/tpB6BwsJCAcDAgoC
GQEFGwMAAAACgkQrJUXP1WWgzuDggCdH5SoopI3rCkqxrt8LbIY/V+kUUQAoKh8
XwGb/SFpxciXURfmAag8vMWVuQINBD+2kHoQCAD2Qle3CH8IF3KiutapQvMF6PlT
ETlPtvFuuUs4INoBp1ajFOmPQFXz0AfGy0OplK33TGSGSfgMg71l6RfUodNQ+PVZ
X9x2Uk89PY3bzpnhV5JZzf24rnRPxfx2vIPFRzBhznzJZv8V+bv9kV7HAarTW56N
oKVyOtQa8L9GAFgr5fSI/VhOSdvNILSd5JEHNmszbDgNRR0PfIizHHxbLY7288kj
wEPwpVsYjY67VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBgRjXyEpwpy1obE
AxnIByl6ypUM2Zafq9AKUJsCRtMIPWakXUGfnHy9iUsiGSa6q6Jew1XpMgs7AAIC
B/9Y7P5vT5Vq3En0KnQIc0QREvjEqJnWk4IJrPrusdml/4mbZjBwpj8JzG4JxU7D
MIfN5M83UZRkQMJ0Tpqv13Rafazt/j40+HWuiKEWx14Lt00Q86eA05JXQV84SogB
EkcHBwuNRW1HSlD1TBde6lygdF2CleNtF6+m5ntbkWkv1kPO4D8H0dsL2bk4NMjk
Hy+5vCR71JQIhfkYMgRJrkrWGANMoDDjL5JsOpxrhcOG3tOkOTQV4w+mfQHi++57
tRJpFBDD4L/OEPvJme7QD1slcrNDcvv6LqaYIvXEG0Qdy2fdNdYuaKgTB7+r02X8
4vkRSqiUZogLgVjaBzylfjUqiEwEGBECAAwFAj+2kHoFGwwAAAACgkQrJUXP1WW
gzvFyACfertRYlbnRMw6abjFqTHIwbufyhIAnRZMLdH0aCr2bnL5lAEo4vDJ2cBw =SGbl

PGP Showtime (Cont')

- Encrypt and sign email and files;
  - Encrypt: use others' public keys so that the recipients can decrypt using their unique privates keys;
  - Sign: use your private key so that the recipients can know it's from you using your public key
- Decrypt and verify email and files;
  - Should verify any appended signature to make sure that the data is originated with the alleged sender and that it has not been altered

PGP Limitations

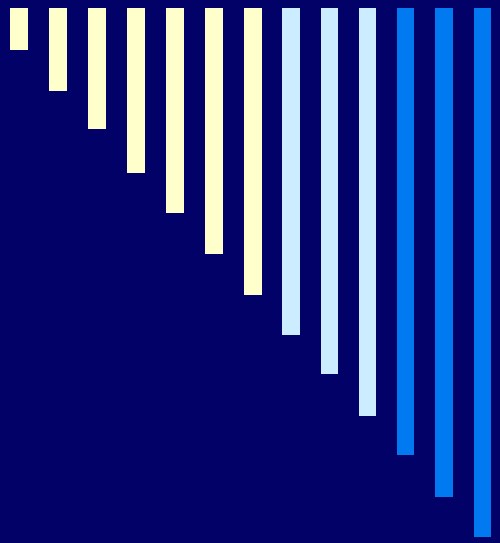
- “No data security system is unbreakable…”—Phil Zimmermann;
- Bugs:
  - ADK (additional key that allows the third party to read part of encrypted information) was found security hole in 2000;
  - In 2002, PGP was found that it couldn’t handle properly some special email sent by hackers for malicious purpose, replying the email would have the risk of information exposure;
  - …
- Lose private key, lose all;
- An old topic: should remember the long “passphrase”;
- The biggest threat: tampering and imitation of public keys;
- Time-consuming process based on some algorithm
- Algorithms may be eliminated through selection
- …

Summary

- PGP is excellent at encryption/decryption
- 12 years' history and is still developing
- Public key (PK) and private key (SK)
- Various Algorithms are RATHER intricate
- PGP protocol
- Practical demonstration
- Flaws that cannot be avoided

Reference

- Arnoud Engefriet, “The comp.security.pgp FAQ”, 2001, http://www.pgp.net/pgpnet/pgp-faq/pgp-faq-general-questions.html
- http://www.pgp.net/pgpnet/pgp-faq/pgp-faq-general-questions.html
- “PGP Freeware for Windows 95, Windows 98, Windows NT, Windows 2000 & windows Millenium, Users’ Guide Version 7.0”, 2001
- ChinaITLab, “PGP for Windows Introduction”, 2002, http://www.chinaitlab.com/www/news/article_show.asp?id=5475
- PGP Corporation, “An Introduction to Cryptography”, 2003
- *Computer World* Newspaper, “Security Factors of EC and Related Technology”, http://www.tradecab.com/cn/ec/ec42.htm
- “Introduction to PGP Encryption”, http://www.lugod.org/presentations/pgp/
- Loking, “PGP Security”, 1997
- PGP Corporation, “PGP 8.0 for Windows Users’ Guide, 2003
- PGP.com, “Phil Zimmermann on PGP”
- Ellen Messmer, “Security Flaw Discovered in Network Associates PGP Software”, 2000, http://www.nwfusion.com/news/2000/0824naipgp.html?nf



Thanks For Your Patience!

16/11/2003 15:16:42