Using Elliptic Curve Cryptography for Information Security
Using Elliptic Curve Cryptography for Information Security

By Kefa Rabah, krabah@globalopenversity.org

Abstract: The rapid growth of information technology that has resulted in significant advances in cryptography to protect the integrity and confidentiality of data is astounding. Elliptic curve cryptography is gaining wide acceptance as an alternative to the conventional cryptosystems (DES, RSA, AES, etc.). Elliptic curve cryptosystems require less computational power, memory, communication bandwidth, and network connectivity. Elliptic curve ciphers today are based in smartcards, personal digital assistants (PDAs), pagers, and mobile phones, and can be easily implemented with processors clocked in single digits of MHz! This paper describes the basic design principle of elliptic curve crypto (ECC) protocols. The ECC processor is normally used to perform elliptic curve operations for: EC Diffie-Hellman, EC ElGamal and ECDSA protocols. As an example we will implement ECC defined over binary finite field GF(2^m).

Keywords
Elliptic Curve Cryptography (ECC), Internet Security and attacks, Wireless, Secure Socket Layer (SSL)

Follow the link below to access and download the full document:

- Using Elliptic Curve Cryptography for Information Security

Related Articles
1. Data Security & Cryptographic Techniques
2. Introduction to Data Security & Cryptography – CIS301
3. Elliptic Curve Cryptography & Data Security - CIS305
4. Elliptic Curve Cryptography Theory
5. Developing IT Security Risk Management Plan
6. Module 11 - PHP MySQL Database Security
7. HowTo Generate & Setup Secure Connection on Tomcat AS on Linux
8. Secure Connection Tomcat Webserver on Windows
9. Developing IT Security Network Infrastructure Project Charter

Kefa Rabah is the Founder of Global Technology Solutions Institute. Kefa is knowledgeable in several fields of Science & Technology, Information Security Compliance and Project Management, and Renewable Energy Systems. He is also the founder of Global Open Versity, a place to enhance your educating and career goals using the latest innovations and technologies.

© April 2007, Kefa Rabah, Global Open Versity, Vancouver Canada