Course Description

IBM 4758 PCI CRYPTOGRAPHIC COPROCESSOR IMPLEMENTATION CLASS

Charlotte NC, USA March 13 - March 17 , 2000

Presenters: **Andries Mulder (IBM the Netherlands)**
George Dolan (IBM Charlotte, USA)

In this class, each student will learn how the IBM 4758 and CCA products can be used to provide secure cryptographic functions for their unique applications. The instructor will show students how the IBM 4758 and its CCA Support Program feature can be used to provide a high-security cryptographic implementation. After completing the course, students will be able to implement cryptographic security techniques using the IBM 4758 in mixed DES and RSA environments and to configure the Coprocessor for maximum security.

IBM 4758 PCI CRYPTOGRAPHIC COPROCESSOR **Charlotte, NC, USA**
Implementation Class **March 13 - March 17, 2000**

TIME, PLACE, COST

When March 13th until March 17th, 2000
13:30 to 17:00 Monday
09:00 to 17:00 Tuesday-Thursday
09:00 to 13:00 Friday

Where IBM Charlotte, Building 201 (entrance 1 to Main lobby)
8501 IBM Drive
Charlotte, North Carolina, USA

Cost $ 2,200.00 (USD)

COURSE DESCRIPTION

The course includes:

- An introduction to general cryptographic concepts for information security
- The presentation of design objectives for the IBM Common Cryptographic Architecture
- Demonstrations and exercises of how to design and use cryptographic techniques that can be applied to information protection in real environments
- An emphasis on the implementation of security techniques using the IBM 4758 product as a CCA cryptographic node
- Examples that teach students the design philosophy of programs that use DES for data privacy and data-integrity and RSA for digital signatures and symmetric key distribution.

The first half of the class explores the access control and DES aspects of the IBM 4758 CCA product. The latter half of the class focuses on the use of RSA techniques and integration of the IBM 4758 with other IBM products. The course is conducted in a special classroom that is equipped for hands-on training. The classroom is equipped with personal computers that have the IBM 4758 installed.

WHO SHOULD ATTEND

The course is designed for management and staff of IBM customers, system and application developers, and members of IBM organizations who are responsible for specifying and implementing cryptographic systems that use the IBM 4758. The course is also beneficial for system designers, system analysts, system and application programmers, and security personnel.

The skills taught in this course are important for organizations such as banks, merchants, insurance companies, manufacturers, distributors, and governmental agencies that are involved in or employ E-Commerce, automated teller machines, home banking, and e-mail applications. These organizations must safeguard their electronic communications and be able to prove to auditors that they have taken all reasonable steps to protect their information.

The cryptographic techniques taught in this course can be used to protect information against misuse and ensure both the user's and the public's confidence in the system. During the course, students will learn the benefits of using the IBM 4758 and its supporting applications to secure their organizations' information. Because of its high-security design, the IBM 4758 is the right choice for server systems. With software-only implementations of cryptography, cryptographic keys can be at risk. The IBM 4758 provides an essential, extra-measure of security for cryptographic keys as well as improved performance for popular public key techniques.

IBM 4758 PCI CRYPTOGRAPHIC COPROCESSOR **Charlotte, NC, USA**
Implementation Class **March 13 - March 17, 2000**

COURSE LANGUAGE

The course will be taught in English.

ENROLLMENT

You can enroll by providing the listed information through e-mail or fax (fax preferred) to:

Mrs. Vicky Almany
IBM Corporation
8501 IBM Drive
Charlotte, North Carolina, USA
vickia@us.ibm.com (Internet)
Vicki Almany/Charlotte/Contr/IBM (IBM internal)
Telephone: 1-704-594-8813
Fax: 1-704-594-7553

Payment is required at least ten days prior to the class by March 3, 2000.
Note that seats are limited due to the hands-on nature of this class; enroll early.

IBM 4758 PCI CRYPTOGRAPHIC COPROCESSOR **Charlotte, NC, USA**
Implementation Class **March 13 - March 17, 2000**

Enrollment Information

Participant name and title
Company name
Company or department description
Full business address
IBM Customer Number

No enrollment confirmations will be sent until 10 days before the planned start date of the class. If you require an earlier confirmation, please contact Andries Mulder. The class is subject to cancellation in the event of inadequate enrollments; we would appreciate your early enrollment.

Payment Details

The fee for the course is USD$ 2,200.00 Full payment is required ten days prior to the class by check drawn to IBM, or by credit card: American Express, Diners Club, MasterCard, or Visa. When paying by credit card, provide this information:

Card type
Account-holder name as on the card
Account number
Expiration date.

Hotel Accommodations

The IBM Charlotte Education Facility is located in the University Area of Charlotte, NC; make hotel accommodations through your travel representative. Hotel and meal expenses are not included in the course fee.
Hotels in the University area: (near N. Tryon Street or on W.T.Harris blvd)

- University Hilton Charlotte tel. 001-704-547-7444
- Holiday Inn University area tel. 001-704-547-0999
- Homewood Suites Charlotte tel. 001-704-549-8800
  fax 001-704-510-0055
- Residence Inn Charlotte tel. 001-704-547-1122
- Courtyard by Marriot
- Hampton Inn
- Microtel Inn

Alternative Courses

This class is run on a regular basis in Europe and in Charlotte, North Carolina, USA.
If there are more than 3 to 4 attendees from one country or customer, it may be more cost-effective to have a customer-tailored course offered on the custsomer's site.
Interpretation services can be offered in a customer-tailored course.
For more information contact Andries Mulder (see address information at the end of this document)

IBM 4758 PCI CRYPTOGRAPHIC COPROCESSOR **Charlotte, NC, USA**
Implementation Class **March 13 - March 17, 2000**

COURSE OUTLINE

(T) = Theory (P) = Practice

DAY 1 (Monday)

- **Opening** (T)

- **Basic Concepts of Symmetric Cryptography** (T)
  IBM'sCCA implementation
  Configuration examples
  Cryptographic separation & initialization methods
  Requirement for cryptographic function isolation
  Cryptographic isolation via Control Vectors.
  General IBM 4758 Overview (T)

- **A Demonstration of the IBM 4758** (T+P)

DAY 2 (Tuesday)

- **Installing and Customizing an IBM 4758** (T)
  Concepts of customizing an IBM 4758
  The Crypto Node Management Utility (CNM) installation
  How to use the Node Management Utility.

- **Loading the System Software into the IBM 4758** (T)
  Loading the software
  Feature Control Vectors, and how to load them.

- **Access Control in the IBM 4758** (T)
  Roles
  Profiles
  Logon and its Context.

- **Installing and Customizing an IBM 4758** (P)
  Using the CNM-utility
  Testing the DEFAULT role
  Loading other roles
  Loading profiles
  Setting Data and Time
  Customizing with a user program

DAY 3 (Wednesday)

- **CCA Key Management** (T)
  This presentation gives a more detailed discussion on the concepts of cryptographic key-handling in CCA programs.
  - Generation of keys
  - Where to store keys
  - Backup considerations
  - Distributing keys to remote nodes
  - Exporting and importing keys
  - Using key storage.

- **Programming for the CCA API (T)**
  - CCA calling conventions
  - Compiling and linking application programs
  - Some CCA verbs and their use
  - CCA return codes and reason codes
  - CCA pseudo code samples
  - Running CCA programs with Easy58.

- **Testing CCA designs with EASY58 (T+P)**

DAY 4 (Thursday)

- **Setting Up a Symmetric Key Management System** (T)
  In this presentation an example of a real-life key-management-center application based in CCA cryptography is discussed. The programs required on the center and user-nodes are presented using pseudo code so that the ideas behind the actual programs become clear.

- **A Conceptual Overview of RSA** (T)
  Concepts of DES and PKA algorithms
  Application areas of PKA's
  The N-Square problem and the solution to that
  Initial DES key distribution
  Digital Signatures and non-repudiation

- **The IBM PKA Implementation** (T)
  Generating key-pairs
  Importing and exporting keys
  Some CCA CSNDxxx verbs and their use
  How to use a certification center.

- **Initial DES Key Distribution** (P)
  A case study presentation of a DES key distribution system with the use of public key cryptography demonstrates the use and capabilities of the IBM 4758 CCA implementation.

- **Digital Signature Case Study**
  In this case study presentation, all the steps required to generate and verify digital signatures between two nodes in a network are examined.
  Explanation of the steps in the process
  Running the programs.

DAY 5 (Friday)

- **A Positioning of the S/390 CMOS Crypto feature and the IBM 4758 (T)**

- **Master Key Cloning and How to Use It** (T)

- **CDSA and Keyworks**

- **Custom programming overview:** (T)
  User Defined Extensions
  The Custom Programming Toolkits

- **New models of the 4758** (T)
  Hardware changes
  New Software (PKCS)

- **Closing of the Course**

TOPICS OF RELATED COURSE OFFERINGS

On request, course(s) that cover these topics can be quickly offered:

- Securing Workstations in a Practical Way (T)
- Installation and Customization of 4753 NSP (T)
- CCA on the RS/6000 (T)
- CCA on the AS/400 (T)
- PKA92 for TSS, the first CCA RSA implementation (T+P)

For information about these related classes or for information about courses that run in Europe, please contact Andries Mulder:

Mr. A.A.M. Mulder
IBM Nederland NV
PO Box 9999
1006 CE AMSTERDAM
The Netherlands

Tel. +31-20-5134776 , +31-544-374037, or +31-653-763989
Fax +31-544-374969
e-mail: andries_mulder@nl.ibm.com or driesmul@wxs.nl

IBM 4758 PCI CRYPTOGRAPHIC COPROCESSOR **Charlotte, NC, USA**
Implementation Class **March 13 - March 17, 2000**

Snail-mail and FAX Enrollment Form

IBM 4758 PCI Cryptographic Coprocessor Implementation Class, AP058

Name and Title of Participant:. . . . . .

Company Name: . . . . . .

Full address: . . . . . .

City: . . . . . .

Country: . . . . . .

Tel. and Fax numbers:. . . . . .

e-Mail: . . . . . .

IBM Customer Number: . . . . . .

Payment:

___Check Enclosed, drawn to IBM, payable in USA funds
___MasterCard
___Diners Club
___Visa
___American Express

Card Number _____

Expiration Date _____

Name as on card _____

Signature _____

Please Send or Fax to Mrs. Vicky Almany
IBM Corporation
8501 IBM Drive
Charlotte, North Carolina, USA
vickia@us.ibm.com (Internet)
Vicki Almany/Charlotte/Contr/IBM (IBM internal)
Telephone: 1-704-594-8813
Fax: 1-704-594-7553

After sending the fax to mrs Almany, please send an e-mail or make a phone call to verify the proper transmission.