A Secure Mobile System to Interchange Electronic Medical Records in HL7

Diego F. Sierra, Yeison F. Torres, Jorge E. Camargo
Universidad Antonio Nariño, Bogotá, Colombia
{diesierra, yeitorres, jorgecamargo}@uan.edu.co

***Abstract*—Electronic medical records are a very important asset that must be secured in such a way that only patients and authorized personal can access them. The HL7 (Health Level 7) is a set of standards to transfer clinical and administrative data among hospital information systems. One of the main concerns of interchanging medical information is related to security. A system that transfers medical information needs to be secured to avoid information disclosure. The increasing use of mobile devices arises different challenges in terms of information security. Access to clinical information from a mobile device requires security mechanisms that allow to guarantee confidentiality, integrity and availability. In this paper we built a system prototype in which electronic health records can be interchanged between a mobile device and a medical information system in a secure way. Results show that health records can be properly secured in a mobile scenario with good performance in terms of computational resources.**

***Index Terms*— HL7, CDA, clinical health records, security, mobile devices, cryptography**

I. Introduction

With the increasing use of mobile devices users want to access different types of services from tablets and smartphones. This phenomena is known as ubiquitous access [1] in which users want to access their information in any place, any time and from any device. Health services are not the exception. Doctors and patients want to access medical information to speed up processes and reduce workload by making information accessible. Although healthcare institutions have implemented electronic information systems, those systems are mainly focused on internal processes. However, mobility is a new need for users. For instance, a patient would like to access medical information to remember specific information of certain treatment or medics. This information generally can be accessed only by doctors through health systems in which medical records are stored, but they are not accessible to patients.

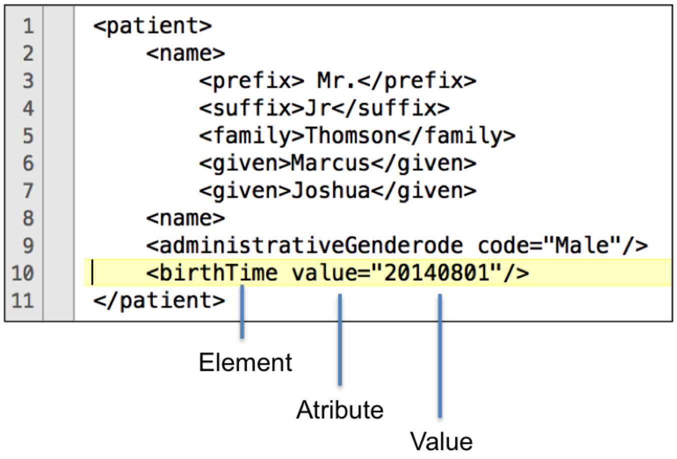
978-1-4799-6717-9/14/$31.00 © 2014 IEEE

An electronic medical record (EMR) is a document of restricted use that contains important and sensible patient's information. Hospitals and health centers have to store and manage EMRs in physical and digital formats, therefore they have to guarantee that only patients and authorized personal can access them. Laws in countries generally regulate the access to medical information with the main goal to protect patient's confidentiality as a fundamental right.

Health institutions have been broadly using security mechanisms to protect sensible information in systems such as PACS (Picture Archiving and Communication Systems) and EMR (Electronic Medical Record systems). Those systems are mainly based on client/server architectures in which users access medical information through a desktop or browser client and secure networks protect sensitive information. However, in mobile environments security is a concern that has called attention of research community to develop mechanisms that allow to protect confidentiality of patients. Mobile devices are sensitive to be stolen and lost, and mobility makes they change regularly of networks (telco operator, public wireless, enterprise networks, etc.)

A. Background

HL7 [13] is a set of standards internationally accepted by most of hospital and health centers to transfer clinical and administrative data. These standards focus on the layer 7 of the OSI (Open Systems Interconnection) mode and they are produced by the Health Level Seven International organization. One of the standards of HL7 is the CDA standard



```
<patient>
    <name>
        <prefix> Mr.</prefix>
        <suffix>Jr</suffix>
        <family>Thomson</family>
        <given>Marcus</given>
        <given>Joshua</given>
    <name>
    <administrativeGenderode code="Male"/>
    <birthTime value="20140801"/>
</patient>
```

Figure 1. XML patient structure according to the Electronic Health Record standard.

[4], which defines an exchange model for clinical documents in XML (Extensible Markup Language) [2] format intended to specify the encoding, structure and semantics of clinical documents. A CDA [16] can contain any type of clinical content such as electronic medical records (EMRs), in which medical information of patients is stored and transmitted between hospital systems. Figure 1 illustrates an example of patient information according to the Electronic Health Record specification of the HL7 standards. The XML structure organizes patient information in a hierarchy of elements, attributes and values.

The exchange of medical information requires of suitable mechanisms to digitally secure EMRs. Cryptography is an area that has developed strong mechanisms to secure digital information. There are two main families of encryption algorithms that are based on symmetric and asymmetric approaches [6], [14]. In symmetric algorithms, a private key is used to encrypt and decrypt a message. In asymmetric algorithms, a pair of keys are used: private key is used to encrypt and public key to decrypt. In this paper we focused on symmetric algorithms, which are suitable to protect a EMRs when they are exchange through the network.

B. Related work

Four our surprise, there are not much works that address the problem of secure electronic medical records in a mobile scenario. Haque et al. [9] recently proposed a platform to secure communication between mobile devices and EMR systems. A web XML-based CDA prototype was proposed by Paterson et al. [17] to move discharge summaries from hospitals to family practice locations. In [7] it was proposed an infrastructure to deliver health records to mobile phones in which security is not addressed. In such as infrastructure a web-mobile application was developed to display patient information. This proposal has the restriction of having an Internet connection. In [16], authors propose a cross-institutional implementation of a web service to interchange clinical data. Although this proposal takes into account HL7/CDA standards and addresses security concerns, the proposal applies only in non-mobile environments.

C. Contribution

In this paper we present an evaluation of asymmetric encryption algorithms to determine the efficiency and effectiveness in terms of memory, processor and execution time. We also developed a system prototype to evaluate the feasibility of securing electronic medical records when they are accessed from mobile devices.

This paper is organized as follows: Section 2 describes material and methods in which we describe the proposed system; In Section 3 we present results; and Section 4 concludes the paper.

II. Materials and Methods

This work has two main objectives: The first one consisted in evaluating the performance of a set of algorithms in terms of efficiency in order to determine which is the most suitable in a mobile environment; and the second one was focused on building a system prototype in which medical records are secured when they are interchanged between a mobile device (client) and a medical record system (server).

A. Experimental design

1) Data set: We used an anonymized data set[1] of health records including 5,000 patients and 500,000 observations provided by the OpenMRS project, which is one of the most popular open source medical record systems. This data set was pre-processed to build 50,000 CDA files in XML format.

[1] https://wiki.openmrs.org/display/RES/Demo+Data

2) Encryption algorithms: We selected four symmetric algorithms to be evaluated in terms of performance based on the comparative study performed in [10]. We used the Java Cryptography Extension (JCE)[2] in which these algorithms are implemented.

DES (Data Encryption Standard). Algorithm developed in the early 1970s at IBM based on an earlier design by Horst Feistel. This algorithm takes a fixed-length string of plaintext bits and transforms it through a series of operations into another ciphertext bit-string of the same length. Th block size is 64 bits, form which 56 bits are used by the algorithm and 8 for checking party. The decryption process uses the same structure as encryption but the keys used in reverse order. This algorithm was used for decades and it is considered one of the most influential in the advancement of modern cryptography.

AES (Advanced Encryption Standard). Algorithm developed by Joan Daemen and Vincent Rijment in 2001 through a contest organized by the National Institute of Standards and Technology (NIST). It uses a combination of both substitution and permutation operations in a sized block size of 128 bits, and a key size of 128, 192, or 256 bits.

RC4. It is the most widely used stream cipher algorithm and it is used in protocols such as Transport Layer Security (web browsers) and WEP (wireless networks). It was designed by Ron Rivest of RSA Security in 1987 and it is recognized for its simplicity and speed in software. The algorithm is based on generation of pseudorandom stream of bits to cipher the plaintext using bit-wise exclusive-or operations.

Triple DES. This algorithm consists in applying three times the DES algorithm to each data block using three keys. Those keys can be independent or identical. This algorithm appeared in 1998 as a more secure alternative than DES.

3) Performance measures: The 50,000 medical records were encrypted using selected algorithms. The following performance measures were evaluated in each algorithm:

- **Computing time**: Time in seconds spent by the computer to encrypt a set of electronic medical records using each encryption algorithm.
- **Used memory**: Main computer memory in KB used by the computer to encrypt a set of electronic medical records using each encryption algorithm.
- **Processor consumption**: Percentage of processor used by the computer to encrypt a set of electronic medical records using each encryption algorithm.

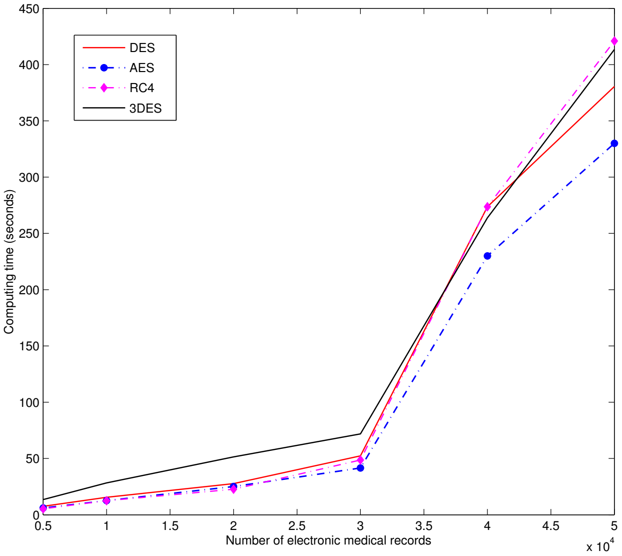


Figure 2. Computing time used for each algorithm to encrypt 50,000 electronic medical records

These performance measures were calculated increasing by 5,000 the number of electronic medical records starting in 5,000 and ending in 50,000. For each performance measure a plot was generated including the four selected algorithms.

4) Execution environment: Experiments were run in a PC with Linux, Intel Core 2 Duo Processor 1,6 x 2 GHz and 2 GB in RAM.

B. Results

Figure2 shows the obtained plots for the computing time measure. In the first 30,000 the four algorithms show a linear trend, however after this quantity, they show an exponential trend. Note that the AES algorithm obtained the lowest computing time, which is indicates that it is a candidate to be selected using computing time criteria.

Figure 3 shows the obtained plots for the computer memory measure. Results show that all curves have a linear trend. Until 2,000 electronic medical records RC4 has the lowest use of memory. After 3,000 EMRs, AES performs much better than the other algorithms.

[2] http://en.wikipedia.org/wiki/Java_Cryptography_Extension

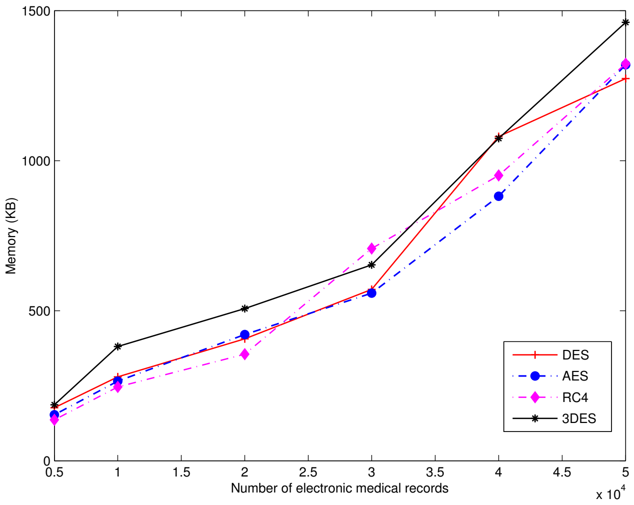


Figure 3. Memory used for each algorithm to encrypt 50,000 electronic medical records

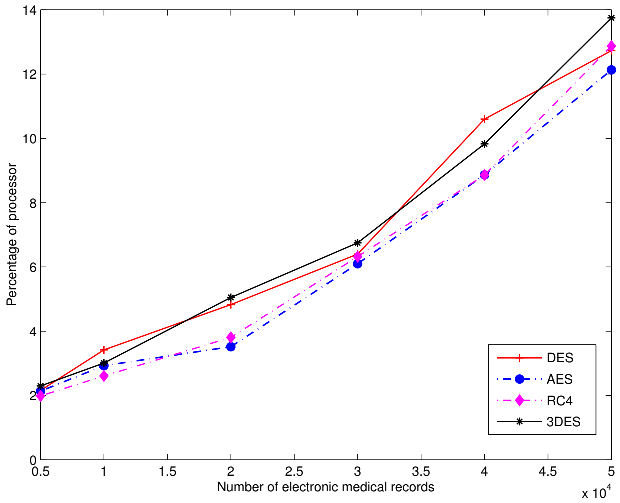


Figure 4. Processor used for each algorithm to encrypt 50,000 electronic medical records

Figure 4 shows the obtained plots for the processor consumption measure. Results show that all curves have a linear trend. Until 1,500 electronic medical records RC4 has the lowest use of processor. In general AES performs much better than DES and 3DES, and slightly better than RC4.

In general, the AES algorithm performs better than DES, 3DES and RC4, so this algorithm is the best in terms of efficiency. With respect to effectiveness, AES is the most secure algorithm according to the comparison performed by Hambdan et al. [10].

C. System prototype

We built a system prototype to evaluate the feasibility to implement the AES algorithm in a mobile environment. To do that, we developed a system prototype composed of two components: mobile client and server. Figure 6 illustrates the general architecture of the system. In the following paragraphs we briefly describe each functionality of each component:

1) Server component: The server component stores the collection of electronic medical records. The following are the functionalities that were implemented Tomcat 7.0 to bring access to clients to the electronic medical records. The following are the steps performed by the server:

- Original electronic medical records are stored in MySQL database, so they are converted to files under the CDA standard.
- These CDA files are encrypted using the AES algorithm.
- After encryption process it is possible that special characters are generated, so it is necessary to encode them with the Base64 encoding algorithm.
- Encoded records are exposed as a web service to be consumed by the mobile component.

2) Mobile component: The mobile component offer a graphical user interface (GUI) in which users can access electronic medical records through the Internet. This component was developed natively for Android 4.x or superior. The following are the steps performed by the client:

- The user configures connection parameters to access the server (IP address and port).
- The GUI offers a text box to enter the identifier of a electronic medical record.
- The mobile device sends a request to the web service using the identifier.
- The server returns an encoded electronic medical record.
- The mobile decode the obtained record (decoding with Base64).
- A decryption process is performed using the AES algorithm.
- The electronic medical record is shown to the user in clear text.

Figure 6 shows a set of screen shots of the mobile component.

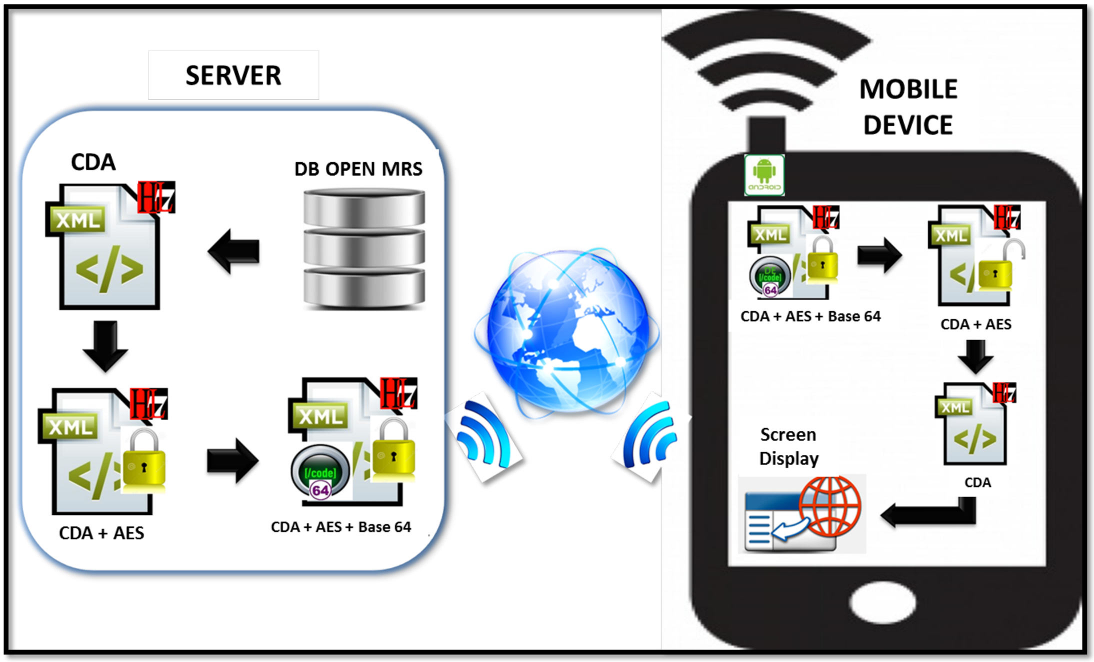
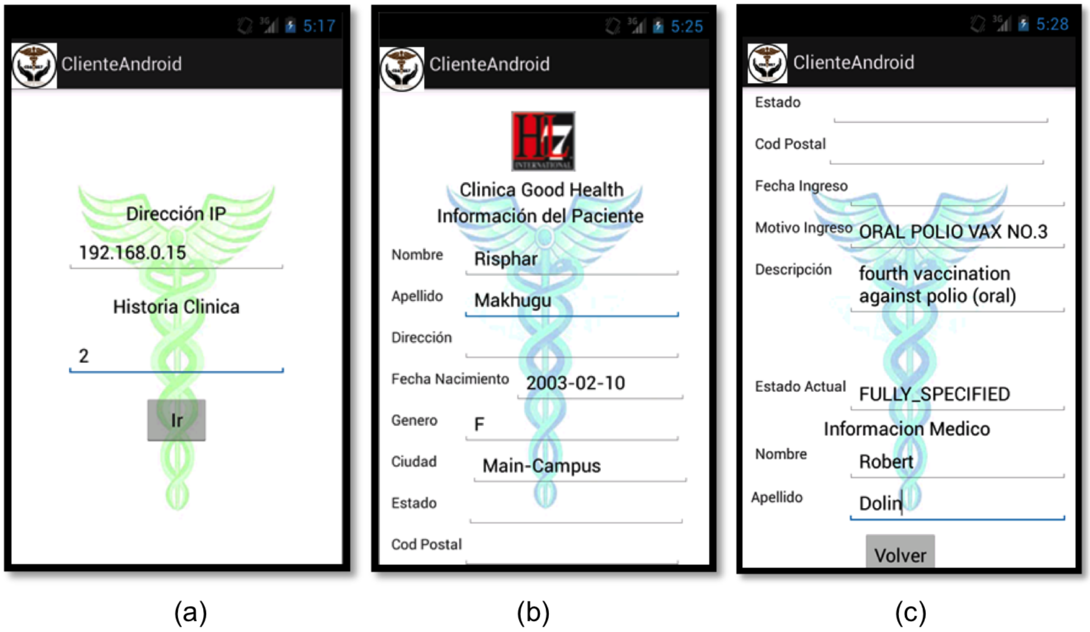


Figure 5. System overview. In the server component electronic medical records are stored, encrypted, encoded and transmitted. In the mobile component EMRs are decoded, decrypted and displayed to patients.



Dirección IP
192.168.0.15
Historia Clinica
2

(a)

Clinica Good Health
Información del Paciente
Nombre Risphar
Apellido Makhugu
Dirección
Fecha Nacimiento 2003-02-10
Genero F
Ciudad Main-Campus
Estado
Cod Postal

(b)

Estado
Cod Postal
Fecha Ingreso
Motivo Ingreso ORAL POLIO VAX NO.3
Descripción fourth vaccination against polio (oral)
Estado Actual FULLY_SPECIFIED
Informacion Medico
Nombre Robert
Apellido Dolin

(c)

Figure 6. Screen shots of the mobile component: (a) Connection parameters and ID of the electronic medical record to be accessed; (b) and (c) Electronic medical record returned by the server corresponding to the ID provided by the user.

III. Discussion

Encryption algorithms are commonly replaced for other more secure algorithms. The security provided for a new algorithm is relative. Any algorithm can be broken using suitable computing resources and time. One of the mechanisms to do an algorithm stronger consists in providing large encryption keys. However, this mechanism is not practical in scenarios in which computing resources are limited, as it is the case of mobile environments. Although nowadays mobile devices have high memory, multiple cores and gigabytes of storage, communication channels such as 4G LTE (Long Term Evolution) which offers high speed data transfer in megabytes, mobile computing resources have to be carefully administrated to bring security to mobile applications. The evaluated algorithms in this paper have been reported by the industry as insecure because they have been broken in the past. However, when these algorithms are combined, the security is improved. Therefore, they are being used today in some scenarios such as wireless routers, authentication protocols, network and transport protocols (TLS and SSL), among others.

IV. Conclusions and future work

With the increasing use of mobile devices, security is a concern that has to be addressed in the construction of new systems in order to guarantee patients confidentiality. In this paper, we presented a system to secure electronic medical records in a mobile scenario. We conducted an evaluation with four symmetric algorithms to determinate the most efficient of them in terms of memory, processing and computing time. Results showed that the AES algorithm was the most efficient according to some performance measures. We implemented a system prototype in which electronic medical records are securely exchanged between server and mobile client. The system prototype was developed for the Android platform, which offers a graphical user interface to access electronic medical records stored in an EMR. To the best of our knowledge, this paper is one of first initiatives to address security concerns to securely exchange electronic medical records under HL7/CDA in mobile scenarios. As future work we want to implement the proposed system in a hospital to validate it in a real scenario. We expect to develop the mobile app in other mobile platforms. We want also to study the combination of asymmetric and symmetric algorithms to formulate a robust secure infrastructure to protect sensitive patient information at different levels.

References

[1] Abraham, C., Richard, W., Boudreau, M.-C. Ubiquitous Access: on the front lines of patient care and safety. Communications of the ACM 51(6), 95–99 (2008)

[2] Brewton J., Yuan, X.; Akowuah, F., XML in Health Information Systems. Department of Computer Science, North Carolina A and T State University, Greensboro, North Carolina USA, 2012.

[3] Daltabuit, E. La seguridad de la información, México, Limusa 2007.

[4] Dolin R., Alschuler L., Boyer S., Beebe C., Behlen F., Biron P., SHABO A. HL7 Clinical Document Architecture, Release 2. Journal of the American Medical Informatics Association Volume 13 Number 1 Jan / Feb 2006.

[5] Fernández, S. La Criptografía Clásica, Revista SIGMA 2004.

[6] Giner, F. Implementación de un esquema criptográfico para gestionar de forma segura las historias médicas de los pacientes a través de una red de comunicaciones, Cataluña, 2007.

[7] Ghose, A., Bhaumik, C., Agrawal, A.K.: Mobile Healthcare Infrastructure for Home and Small Clinic. In: Proceedings of the 2nd ACM International Workshop on Pervasive Wireless Healthcare, New York, pp. 15–20 (2012)

[8] Gómez, Álvaro. Enciclopedia de la seguridad informática, México, 2007.

[9] Haque W., Horvat D., and Verhelst L., A Secure Mobile Platform Integrated with Electronic Medical Records. University of Northern British Columbia, Prince George BC, Canada. 2014.

[10] Hamdan, O.; Zaidan, B.B.; Zaidan, A.A.; Hamid A.Jalab, M. Shabbir and Y. Al-Nabhani. New Comparative Study Between DES, 3DES and AES within Nine Factors, 2010.

[11] Hayrinen, K., Definition, structure, content, use and impacts of electronic health records: A review of the research literature. International Journal of Medical Informatics, Volume 77 , Issue 5 , 291 – 304

[12] Hernández, S. Fundamentos de La Metodología de Investigación. Editorial McGraw-Hill. 2014

[13] Health Level Seven International: HL7 CDA Release 2 (2005), http://www.hl7.org/implement/standards/ (Accessed Jun 25, 2014)

[14] Lombardo, Roberto. Sistema de Historia Clínica Digital. Sociedad de Cardiología de San Juan Federación Argentina de Cardiología, 2008.

[15] López, M. Criptografía, UNAM, Facultad de Ingeniería, 2009.

[16] Müller, M., Ückert, F., Bürkle, T., Prokosch, H.-U.: Cross-institutional data exchange using the clinical document architecture (CDA). International Journal of Medical Informatics 74(2-4), 245–256 (2005)

[17] Paterson, G., Sheperd, M., Wang, X., Watters, C., Zinter, D.: Using XML-Based Clinical Document Architecture for Exchange of Structured Discharge Summaries. In: Proceedings of the 35th Hawaii International on System Sciences, Maui (2002)

[18] Sklavos, N. Wireless Security and Cryptography Specifications and Implementations, 2010.