MOBILE PAYMENTMETHODBASED ON PUBLIC-KEY CRYPTOGRAPHY

Adnan A. Hnaif and Mohammad A. Alia

Faculty of Science and Information Technology – Al-Zaytoonah University of Jordan

ABSTRACT

Mobile payment is defined as mobile money, which is considered as an attractive alternative for cash, cheque, or credit. In this paper we propose a new secure mobile paymentmethod. This method is summarized in three processes: firstly, the authentication process, which involves the authentication phases for the applied customers. Secondly, the member recognition process which tests and ensures the customer membership by the market server. Finally, payment processwhich will be done by ciphering the customer information using public-key encryption cryptosystem (RSA), to be submitted over an insecure network to the market server. Actually, this mobile payment methodis more efficient than otherpayment methods since the customer can pay from his/her own mobilephone without any extra cost and effort. The RSA public-key encryption system ensures the security of the proposed method. However, to prevent a brute force attack, the choice of the key size becomes crucial.

KEYWORDS

Mobile Payment, Cryptography, Information security, and Encryption.

1. INTRODUCTION

In business, shop offers goods or services to customers for selling. In shopping,retailers presents their available products to be purchased by customers. Meanwhile, the shopping can be affected by variant factors including how the customer is treated, convenience, the type of goods being purchased, and payment technique[1].

On other hand, payment is the activity of transferring item of value from one party to another for the provision of goods, servicesor both.However, barter is the oldest form of payment, in which good or service can be exchanged between parties. In the modern world, cheque, debit, credit, or bank transfer, are common means of payment. In complex transactions between businesses, payments can take the form of stock or other more complicated arrangements.Change coin, money and banknote in terms of the price is defined as exchanging payment. While provisioning payment is quoted as the other form of payment since it is used to transfer money from one account to another. In fact, a third party must be involved in some payment methods such as electronic payments methods. Methods such as credit card, debit card, cheques, money transfers, and recurring cash are alsoconsidered electronic payments methods. Moreover, magnetic stripecard, smartcard, contactless card and mobile handset are proposed as advanced electronic payments technologies. Specifically, mobile handset based payments are called mobile payments.

DOI : 10.5121/ijcnc.2015.7207

A credit card is a payment system that allows the cardholder to pay for goods and services based on the legitimate contract between the cardholder and the credit card provider [1]. The cardholder must create an account to be granted a line of creditby credit card provider as a cash advance for electronic payment.As mentioned earlier, credit card is typically electronic payment that involves a third party. The third party pays the seller and is reimbursed by the buyer.

As mentioned earlier, a credit card service provider (such as a bank or credit union) issues the credit cards for costumers,respectively after the customer account has been approved by the credit provider. Whereby, cardholders can use their credit cards to make purchases atmerchants who acceptcredit card. Usually, merchants advertise their acceptable cards by showing credit cards marks or logos. However, credit card user must agree his/her purchases to pay the card issuer. Since the merchant asks the cardholder to entering a personal identification number (PIN) and sometime to sign the receipt with a record of the card details. Currently, most merchants accept telephone authorization and internet authorization. These kind of authorization is commonly known as a card not present transaction (CNP).

Instantaneously, most of the electronic verification systems allow merchants to verify the card validation and covering the purchase in a few seconds. However, a credit card payment terminal or point-of-sale (POS) system with a communications link to the merchant's acquiring bank perform the electronic verification. The magnetic stripe or chip on the card involves secured and private information about the card. Monthly, card provider sends a regular statement indicating the purchases undertaken with the card, any outstanding fees, and the total amount owed to the cardholder.Electronic statements are also offered by banks in addition to the physical statements.Electronic statement can be simply viewed at any time by the cardholder via the provider's website. Normally, card provider notifies the cardholders about their purchases amount,and statementsby email or mobile SMS.

On other hand, credit cards can be a significant financial asset in certain cases. Whereby, credit cards can land a consumer in a tough financial situation when it is used unwisely. Thereare some benefits and risks defined with credit cards.However, credit cards benefits are basically presented as; easy to access, customersdon't have to reapply when the payment is down or off, almost accepted everywhere, and it can help to build a solid credit history and rating. Whereby, some credit card risks are highlighted as; it has high interest rates, it may find difficulties in monitoring the spending of the credit card when the cardholder exceeds the levels of debt, extra interest should be added if the cardholder doesn't pay his/her bill on the limited time, and cardholder who has lots of cards will definitely fight administrative nightmare.

Mobile payment is also referred toelectronic payment. It is defined as mobile money, mobile money transfer, and mobile wallet. In modern payment methods, mobile payment comes to be an attractive alternative for cash, cheque, or credit cards payment methods. Since the costumer can easily use his/her standard mobile phone to pay for a wide range of services and purchases. Widely,the use of mobile payment becomes prevalent since 2008. Therefore, this study proposes a new payment method for store shopping by using standard mobile phone. This study is actually focused on the secure mobile payment, since the proposed method is basically based on public key cryptosystem.

2. RELATED WORKS

Recently, electronic payment has been widely applied in most shopping center and sites. However, there are several successfulavailable models for mobile payments, among them:

Premium SMS based transactional payments, Direct Mobile Billing, Mobile web payments (WAP), Contactless NFC (Near Field Communication), and Direct carrier/bank co-operation.These mobile payment solutions have been implemented by Financial institutions and credit card companies[2] as well as Internet companies [3] and a number of mobile communication companies, and major telecommunications infrastructure [4][5].

2.1 SMS/USSD-based transactional payments

In this model (refer to Figure 1), consumers request a premium charge to be applied to their phone bill or their online wallet by sending a payment request via an SMS text message or an USSD to a short code. Consequently, the involved merchantis informed of the payment success and can then release the paid for goods.Since these goods are most frequently digital, the merchant replying using a Multimedia Messaging Service (MMS) to deliver the purchased music, ringtones, wallpapers, etc. Another form of deliver using MMS is the barcode,which can be used as an electronic ticket for access to cinemas and events or to collect hard goods. These barcodes can then be scanned for confirmation of payment by a merchant. However, poor reliability, slow speed, security, and high cost are weaknesses encountered using SMS/USSD payment method [2, 6].

Figure 1: Mobile Channel Series: USSD[7]

2.2Direct mobile billing

This model is used with e-commerce sites, in which the consumer uses the mobile billing option during checkout to make a payment. The payment needs a two-factor authentication that includes a PIN and One-Time-Password (*OTP*), to charge the consumer's mobile account. This type of mobile payment is an alternative payment method that avoid banks involvement, since it does not require the use of credit/debit cards or pre-registration at an online payment solution [8].

2.3Mobile web payments (WAP)

This payment model uses WAP (Wireless Application Protocol) as an underlying technology. To make a payment, the consumer uses web pages or applications downloaded and installed on the mobile phone.However, the mobile account should be directly charged through a mobile network operator. Otherwise, the use of a credit/debit card or pre-registration at online payment solution still required [9].

2.4Near Field Communication (NFC)

NFC model (refer to Figure 2) is a payment method used in physical stores or transportation services. In this payment method, the consumer use a special mobile phone equipped with a smartcard. Furthermore, the consumer mobile is wavedif he/she stays close to the reader module. Some transactions require authentication using PIN, before transaction is completed. The payment could be deducted from a pre-paid account or charged to a mobile or bank account directly.However, the drawback of NFC mobile payment method is the lack of supporting infrastructure, complex ecosystem of stakeholders, and standards [10].

Figure 2: Near Field Communication [11]

2.5 Direct carrier/bank co-operation

This model is also known as direct operator billing, mobile content billing, WAP billing, and carrier billing. It is a mechanism of buying content from WAP Wireless Application Protocol sites that is charged directly to consumer's mobile phone bill. This payment method should be integrated with another party called operator.In this payment model, the consumer can purchase goods, transfer money, cash-out, and cash-in. The front end interface to the consumers is the mobile phone and the phone carrier. A special code can be entered on the mobile phone to open a 'mini wallet' account, by depositing money at a participating local merchant and the mobile phone number. Similarly, other transactions can be accomplished by entering special codes and the phone number of the other party on the consumer's mobile phone.Moreover, consumers can buy mobile content without registering for a service or entering a username or password. Consumers can download content by clicking on a link and agrees to make a purchase[12, 13].

3. THE PROPOSED METHOD

Generally, the proposed method describes three processes for mobile payment system (refer to Figures 1-3). Whereby, the proposed method is based on the integer factorization problem for RSA public-key cryptosystem [14, 15]. Meanwhile, RSA cryptosystem is typically divided into three sub-algorithms; key generation, encryption, and decryption algorithms. However, the proposed methodprocesses are: the authentication process, the member recognition process, and payment process.

3.1 Authentication (Getting Service) Process

This process is the first step in the proposed mobile payment system that prepares the customer to be able to use the mobile for payment. In this phase, the Bank, the Visa Center, and the Mobile Center plays the main role, whereby confirmation can be given to the customer. As illustrated in Figure 3 Step 1, the customer should request the mobile payment service from the bank. Once the customerrequested the service from the bank,the following steps should have been done by the bank. As shown in Figure 3 Steps2 and 3, the bank should contact the visa center depending on the customer's request to give authorization for the mobile. Following these two steps, the bank should notify the mobile center that the service is authorized by sending the customer information as shown in Figure 3 Step 4. The mobile center, in turn, confirms this process by sending a message to the customeras shown in Figure 3 Step 5. Figure 3 step 6 shows that the customer gets the service by receiving the PIN from the bank. Once the customer gets the PIN, the bank will generate a computed RSA public-key and private-key (refer to Figure 3 step 7) and then pass the public-key to the market (refer to Figure 3 step 7). After that the market will generate a computed RSA public-key and private-key (refer to Figure 3 step 9) and then pass the public-key to the bank (refer to Figure 3 step 10). Finally, the customer can go to the market and use the mobile for payment.

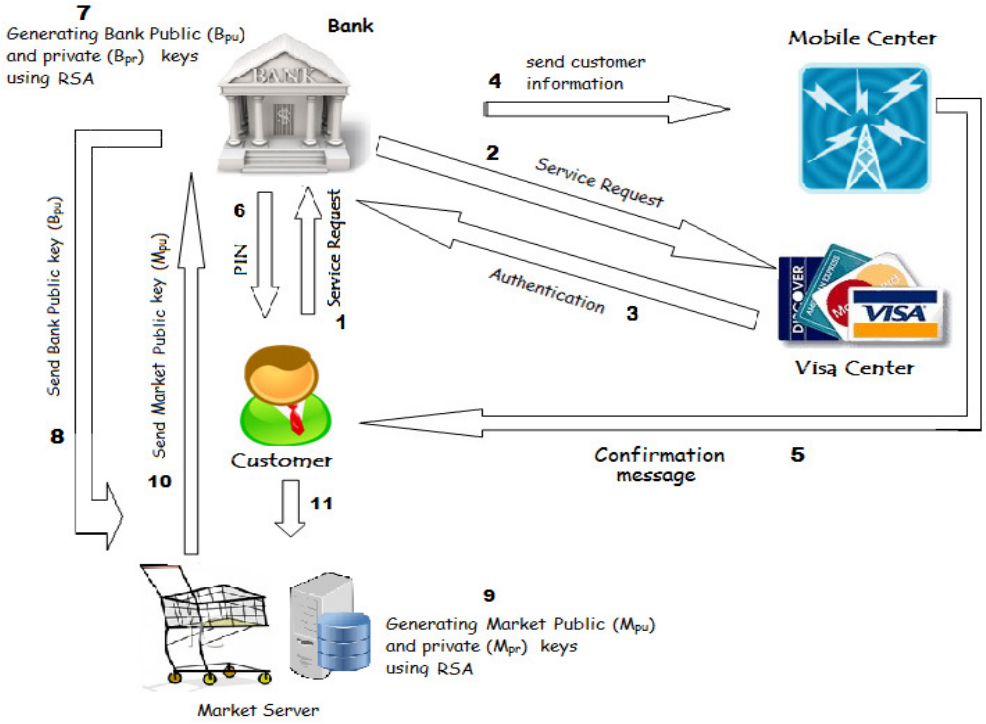

Figure 3: Authentication process

3.2 Member Recognition Process

This processis clarified in Figure 4 from the beginning to the end. When the customer enters the market (Figure 4 Step 1), the market server should test the customer membership as illustrated in

Figure 4 Steps 2 and 3. If the customer was a member, then a welcome message from the market server will be sent to the customer (Figure 4 Step 4). Otherwise, thecustomer will be ignored (Figure 4 Step 5).

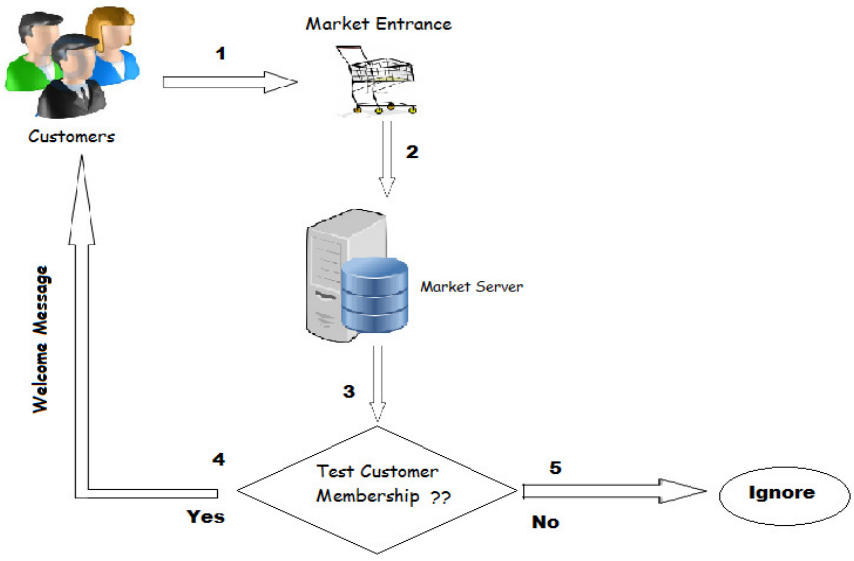

Figure 4: Member Recognition Process

3.3 Payment Process

The third process in the proposed system is the payment process. This step involves payment phase and payment confirmation phase.

3.3.1Payment Phase

The payment phase starts when the customer, who is a member in mobile payment service, reaches the cashier, where the member is given the choice to pay via cash, visa or mobile (Figure 5 Step 1). If the member chooses the mobile payment, the following steps will be implemented securely. First, the market server should ensure the customer membership as illustrated in Figure 5 Steps 2. If the customer was a member, then a number of steps will take place. The market server should contact the visa center to guarantee that the payment amount is available (Figure 5 step 3). Therefore, the RSA encryption algorithm is implemented to encrypt the customer information using the bank public-key (B_{pu})and sendthese information as a ciphertext (encrypted text) to the visa center. When the visa center receives the encrypted text, the RSA algorithm is implemented to decrypt it using the bank private-key (B_{pr})andtests for valid amount as shown in Figure 5 step 4. If the amount is valid or not, then the visa center will send the result (*valid* or *not valid*) to the mobile company as illustrated in Figure 5 step 5. After that, the mobile company sends a message to the member for payment confirmation and the member should respond to the message with the PIN (Figure 5 steps 6 and 7). In Figure 5 step 8 shows the deduction of the amount from mobile company to the visa center.

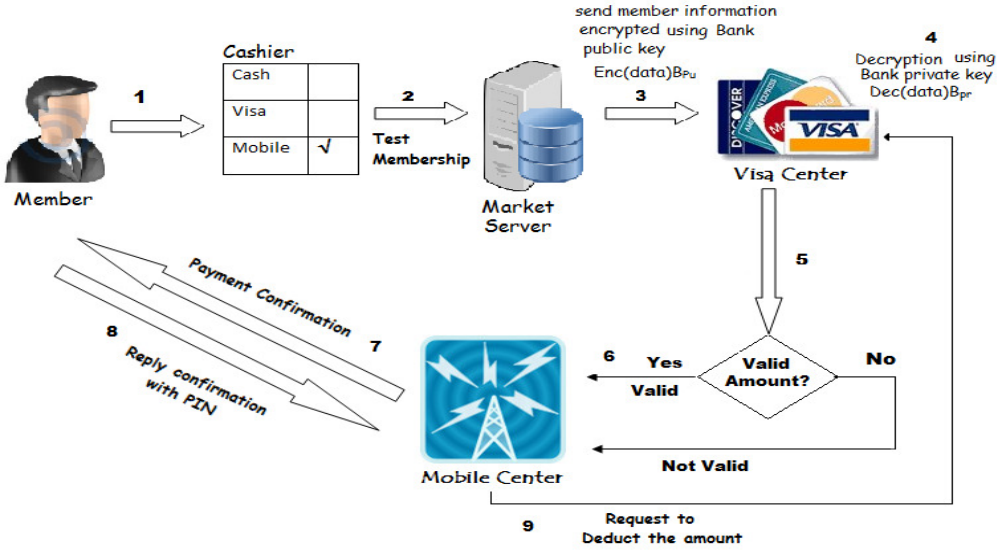

Figure 5: Payment Phase

3.3.2 Payment confirmation phase

This phase follows the payment phase to confirm the payment process as shown in Figure 6. The phase begins by sending a report for the payment process from visa center to the market server as illustrated in Figure 6Step 1. This report is encrypted by implementing the RSA algorithm using the market public-key (M_{pu}). The market server receives the encrypted report and decrypts it by applying the RSA algorithm using the market private-key (M_{pr}) as shown in Figure 6Step 2. Meanwhile, the visa center sends an operation success notification to the mobile company (Figure 6 Step 3). Finally, the mobile company sends an operation success (authentication) message to the member (Figure 6 Step 4).

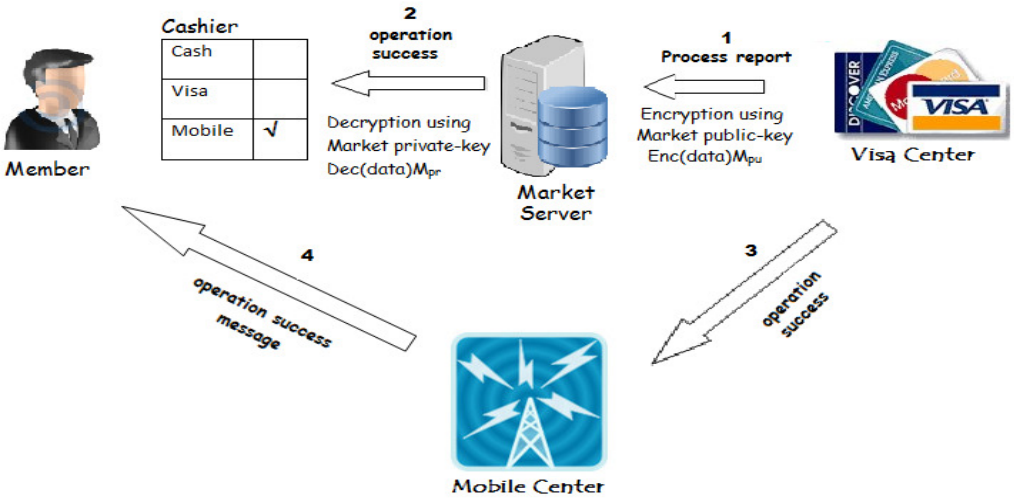

Figure 6: Payment Confirmation Phase

4.PERFORMANCE EVALUATION BASED ON KEY SIZES FOR RSA PUBLIC-KEY PROTOCOL

As mentioned earlier, the proposed method is actually based on the public-key RSA cryptosystem, since the encryption and decryption processes are being performed over the insecure network to apply the confidentiality cryptographic service on the user information (refer to Figure 6). Therefore, we have compared the performance of the three sub-algorithms for RSA public-key protocol. Table1 shows the performance for RSA key generation, RSA encryption, RSA decryption algorithms. These protocols were coded in TurboC with GMP library, and run on a computer with Intel CORE i7 processor. We also used Miller-Rabin algorithm [15, 16] for theprimality test which was coded using C and GMP as well.The implementation for RSA protocolshows that RSA performs high level of security at a much lowcost, this is in terms of key size and execution time (refer to Figures 7, 8, 9, and 10).

Table 1: Performance evaluation for public-key RSA protocols

	RSA	
Description	**Key Size**	Time **(Millisecond)**
Key generation	512 - bits	290
Encryption		3
Decryption		5
Key generation	1024-bits	516
Encryption		14
Decryption		128
Key generation	2048 – bits	1697
Encryption		16
Decryption		315
Key generation	3072 - bits	3490
Encryption		29
Decryption		4800
Key generation	7680-bits	5232
Encryption		39
Decryption		7731
Key generation	15360-bits	18221
Encryption		150
Decryption		54193

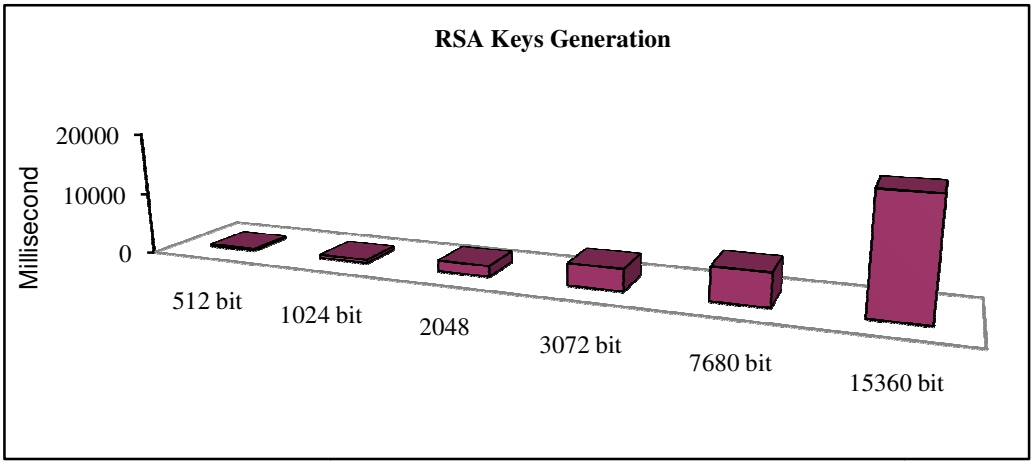

Figure 7: RSA keys generation time.

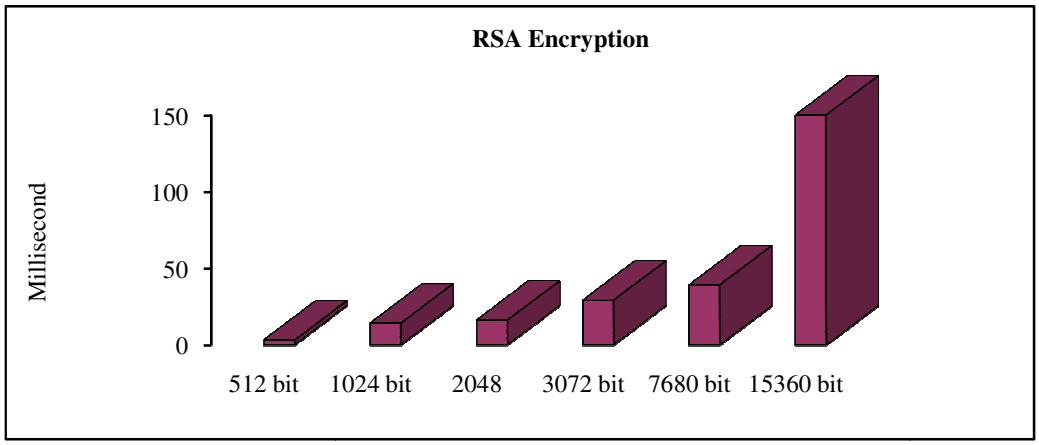

Figure 8: RSA encryption time.

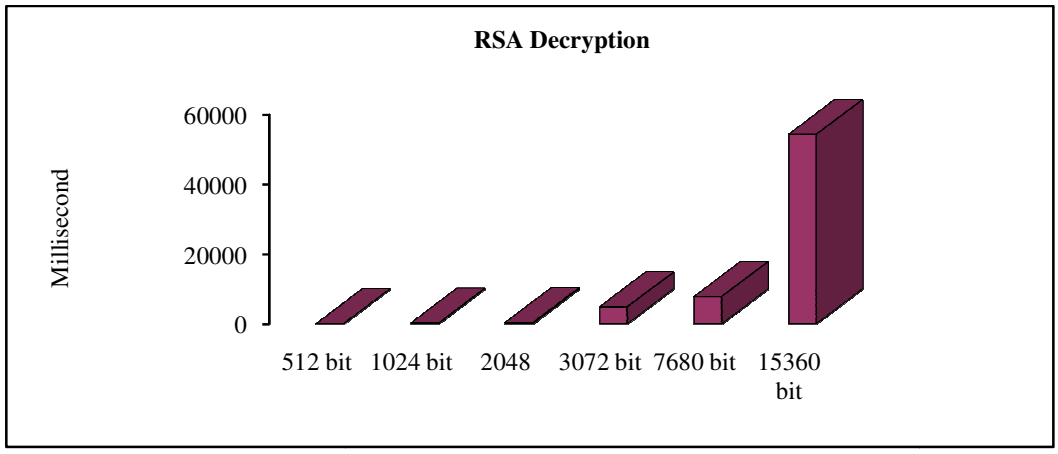

Figure 9: RSA decryption time.

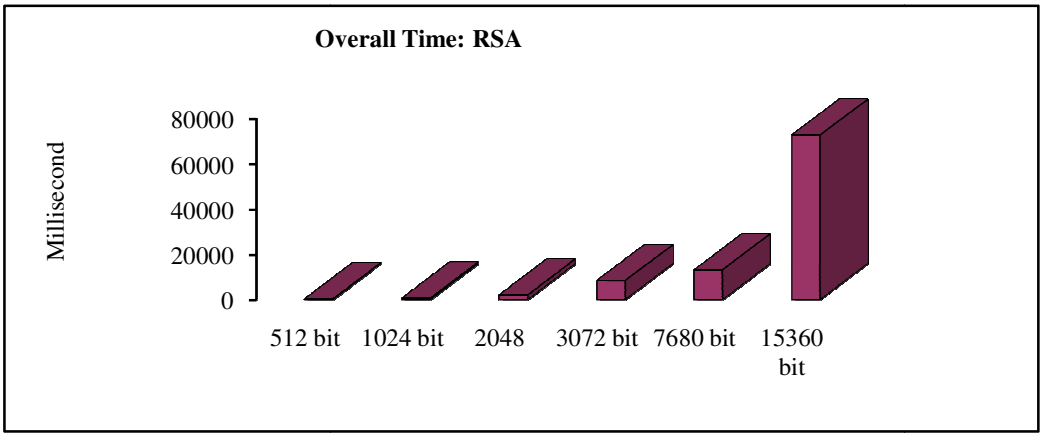

Figure 10: Overall time for RSA public-key algorithm time

5.CONCLUSIONS

Thispaper shows the possibility of establishing mobile payment based on public-key encryption cryptosystem. The security of the proposed mobile payment depends on RSA public key encryption protocol. As the discussion, the proposed method is more efficient than the others methods. It allows the customer to pay from his/her own personal mobile without any extra cost and effort. As new technology for mobile payment method, this method is proposed to replace the unreliable previous paymentmethods, since customers feel justifiably confident that their payment will be accurate. As well as, the proposed method needs only the basic requirements such as; mobile phone, mobile center, market server, and visa center.

6.ACKNOWLEDGMENT

The authors would like to thank Al-Zaytoonah University of Jordan for supporting this study.

REFERENCES

[1] M. J. Arnold, K. E. Reynolds, N. Ponderc, and J. E. Lueg. "Customer delight in a retail context: investigating delightful and terrible shopping experiences". Journal of Business Research, 58 (8): 1132–1145. doi:10.1016/j.jbusres.2004.01.006, 2012.

[2] S. Karnouskos, and F. Fokus. "Mobile Payment: A Journey Through Existing Procedures And Standardization Initiatives", IEEE Communications Surveys & Tutorials, Vol. 6, No. 4, Pp. 44–66, 2004.

[3] Y.A. Au, and R.J. Kauffman. "The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application". Electronic Commerce Research and Applications, doi:10.1016/j.elerap.2006.12.004, 2007.

[4] E. Hardcastle. "Ericsson launches mobile phone banking services". Thomson Reuters, 2012.

[5] Ericsson Money. "Ericsson Money Services brings connected mobile money to Europe". Ericsson.com.2014.

[6] S. Bhawan, and J. L. Nehru Marg. "USSD-based Mobile Banking Services for Financial Inclusion". Telecom Regulatory Authority of India. 2013

[7] G. kamonzo. "Mobile Money Exchange", WordPress.com. The Pilcrow Theme, 2011.

[8] Y.-Y. Chen, J.-K.Jan, and C.-L. Chen. "A fair and secure mobile billing system.Computer Networks", 48(4), pp.517-524, 2005.

[9] Ericsson, "Western Union partner to push mobile financial services". Mobile Payments Today, 2013.

[10] Payment Systems, "VDC: NFC Adoption Will Be Slower Than Expected". RFID Journal. 2008.

[11] D. Murph. "Wave-and-Pay System Headed to Canada". Engadget, 2007.

[12] L. Chaix, and D.Torre. "Four models for mobile payments". University Nice Sophia-Antipolis, JEL Classification: E42, O33, 2011.

[13] R. Englund, and D. Turesson. "Contactless mobile payments in Europe: Stakeholders´ perspective on ecosystem issues and developments". KTH Industrial Engineering and Management. SE-100 44 STOCKHOLM, DiVA, 2012.

[14] R. A. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems".Communications of the ACM, 21(2), pp.120-126, 1978.

[15] Menezes, A., P. Van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography". CRC Press, pp.4-15, 516, 1996.

[16] G. L. Miller. "Riemann's Hypothesis and Tests for Primality".Journal of Computer and System Sciences, 13 (3), pp. 300–317, 1976.

Authors

Dr. Adnan Hnaifis an Assistance professor at the computer networks department, Faculty of Science Computer and information technology, Al Zaytoonah University of Jordan. Dr. Hnaif received his PhD degree in networks security from University Sains Malaysia – National Advanced IPv6 Centre and Excellence (NAV6) in 2010. He received his MSc degree of Computer Science from department of Computer Science- Alneelain University in 2003, and obtained his Bachelor degree of Computer Science from the department of Computer Science, Mu'tah University in 1999/2000. His researches focus on the network security, matching algorithms and parallel processing.

Dr. Mohammad Alia is an Associate professor at the computer information systems department, Faculty of science Computer and information technology, Al Zaytoonah University of Jordan. He received the B.Sc. degree in Science from the Alzaytoonah University, Jordan, in 1999. He obtained his Ph.D. degree in Computer Science from University Science of Malaysia, in 2008. During 2000 until 2004, he worked at Al-Zaytoonah University of Jordan as an instructor of Computer sciences and Information Technology. Then, he worked as a lecturer at Al-Quds University in Saudi Arabia from 2004 - 2005. Currently he is working as a Chair of Computer Information Systems dept. at Al Zaytoonah University of Jordan. His research interests are in the field of Cryptography, and Network security.