Utilization of the RSA Algorim in Business Communication in Making e-Commerce Applications

Fauzi[1], Muhammad Fachry[2]
[1]Department of Business and Accounting, Akademi Akuntasi YPK Medan, Indonesia
[2]Department of Information System, Universitas Muhammadiyah Sumatera Utara, Indonesia

ABSTRACT

Cryptography is a science or art of securing messages and is carried out by cryptographers. Data that is secured includes several aspects such as message security such as confidentiality, data integrity, and authentication. One cryptographic algorithm that is often used in the process of data security is the RSA algorithm. RSA is short for the names of the inventors of this algorithm, namely Ron, Shamir and Adleman. RSA is an algorithm that uses the concept of public key creation (the asymmetry / key used to encrypt is different from that used to decrypt). Where the applications made with Webbase in their security are still often using the MD5 and Sha algorithms so that additional security is needed in securing the existing education in making e-Commerce.

Keyword : RSA, Business, Communication, e-Commerce.

Corresponding Author:
Fauzi,
Department of Business and Acounting,
Akademi Akuntansi YPK Medan,
Jalan Sakti Lubis Gang Pegawai No 8. 20219, Indonesia.
Email: fauzi59@gmail.com

1. INTRODUCTION

The development of telecommunications and computer technology has caused changes in our daily culture. In this era called "information age", electronic media is one of the mainstays for communication and business [1]. Social Media is an extension of commerce by exploiting electronic media [2] [3]. Although the use of electronic media is not yet understood, business insistence causes business people inevitably have to use this electronic media E-commerce or can be called Electronic commerce or e-commerce is the dissemination, purchase, sale, marketing of goods and services through electronic systems such as the internet or television, www, or other computer networks. e-commerce can involve electronic funds transfer, electronic data exchanges, automated inventory management systems, and automated data collection systems [4] [5] [6] [7].

The advantage of e-commerce is to provide convenience for consumers in the transaction because consumers do not have to meet physically. Customers can trade in various types of stores (online store) 24 hours a day and seven days a week, with very fast access making it easier for buyers (consumers) to compare prices and make purchases, without having to leave home or office. Within seconds, consumers can quickly get the goods or services they want, such as e-books, music, or computer software [8] [9].

Reference [10] on his research entitled mapping various problems in e-commerce security explains that although the internet has been proven to provide various facilities for business people, especially for consumers, but in practice it is not free from adverse risks so that if a system is created that can later be created used to protect the parties in the transaction, the system should be able to provide protection Changes, additions or damage by parties who are not responsible for data and information, both during storage and during the transmission process by the sender to the recipient so that irresponsible actions are strive to obtain confidential information, whether obtained directly from its storage or when transmitted by the sender to the recipient (eavesdropping efforts).

This encourages thinking to build a system that can secure e-commerce transactions. One of them is by using cryptographic technology (cryptography). Cryptography is the science / art of encoding messages into a form that is not understood by others. Public-key cryptography uses a key pair, one key for encryption and one key for decryption. The key for encryption is public (not secret) so it is called a public key, while the decryption key is confidential so that it is called a secret key (private key or secret key) [11] [12] [13].

RSA Algorithm Is one of the best-known key-asymmetric (public-key) cryptographic algorithms. This algorithm was made by Ron Rivest, Adi Shamir and Leonardo Adleman. The security of the RSA algorithm lies in the difficulty of factoring large numbers into prime factors. Factoring is done to obtain a secret key. As long as factoring large numbers into prime factors has not been determined, so long as the security of the RSA algorithm is guaranteed [14] [15].

2. RESEARCH AND METHODOLOGY

A. Current State of the System

Every important member data, good communication in terms of business that is stored on the database is not all that is encrypted. Indeed, to retrieve the contents of the database from the system, the one taking the data must enter the system. At present there is still a lot of data stored in the database for important pieces of data that have not been encrypted. If the data has been taken by an unauthorized person, if the data is encrypted it is not easy to read it. It takes time to change the encrypted data to decryption. The algorithm used for is RSA which is implemented on social media to encrypt business-related communications contained in tables in the database.

B. Structure Diagram

Data Flow Diagrams (DFD) are tools commonly used to document processes in a system or a technical graphic that illustrates the flow of information and transformations that are applied when data moves from input to output. Figure 1 illustrates the data flow diagram of the system to be created.

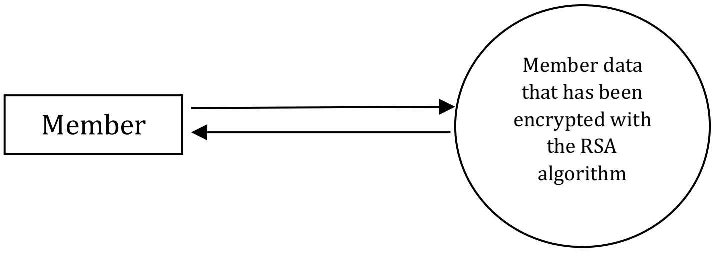

Figure 1. Member Data Encryption Structure Diagram

In the picture above, consumers who register must enter data that has been determined by the system. Member data that has been entered into social media previously encrypted first so that data that enters the system is data that has been encrypted using RSA.

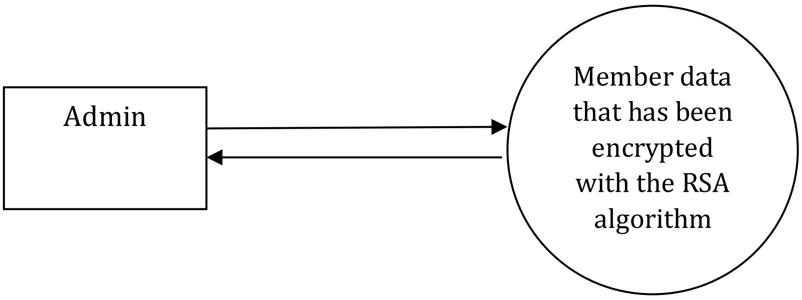

Figure 2. Diagram of Member Data Encryption Structure

In Figure 2, social media users who communicate into the system were previously encrypted so that the data entering the system is data that has been encrypted using RSA.

C. Data Dictionary

Data Dictionary is a catalog of facts about data and information needs of an information system. The data dictionary serves to explain the composition of data packets that move through the data stream. The data dictionary of the program created are:

admin = { email+ pass }
body_content = { content }
bukutamu = { id + nama + email + komentar }
category = { cat_id + cat_name + cat_meta_desc + cat_meta_keywords +
cat_image + delete_tab }
order_details = { sno + order_id + product_id + product_name + price + qty + weight + price_unit + weight_unit + bank }
order_tbl = { order_id + user_id + order_date + order_address + order_zip + order_country + session_id + amount }
product = { product_id + cat_id + sub_cat + product_name + product_price + product_weight + product_weight_unit + product_image + product_in_stock + delete_tab }
shopcart = { product_id + product_name + cat_id + sub_cat + product_price + product_price_unit + product_image + qty + session_id + user_id }
subcategory = { cat_id + subcat_id + subcat_name + delete_tab }
userinfo = { userid + email + pass + user_name + address + dob + tel + status }
zone = { zone + ship_rate }

3. RESULTS AND DISCUSSION

A. User Interface Design

The front screen design before a web page is produced, the interface design will first be used as a guide to the final results of a web page. The following are some of the user interface designs produced in this paper. Next is the initial display screen design.

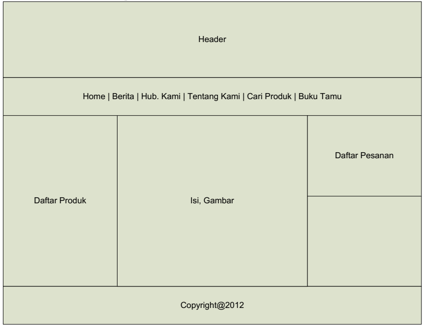
Header
Home | Berita | Hub. Kami | Tentang Kami | Cari Produk | Buku Tamu
Daftar Pesanan
Daftar Produk
Isi, Gambar
Copyright@2012

Figure 3. Initial Display

The picture above is the initial appearance of the application which is the first appearance when the website is opened. On this initial screen you can see the home menu, news, hub. We, about us, find products, guest books. If the news menu is selected, a news page will appear that contains information about product sales.

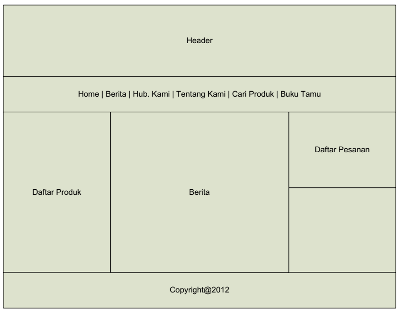
Header
Home | Berita | Hub. Kami | Tentang Kami | Cari Produk | Buku Tamu
Daftar Pesanan
Daftar Produk
Berita
Copyright@2012

Figure 4. News Display

News that are displayed are news that is filled in by the website administrator.

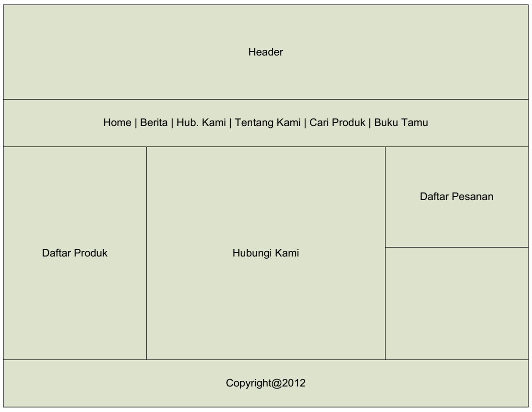
Header
Home | Berita | Hub. Kami | Tentang Kami | Cari Produk | Buku Tamu
Daftar Produk
Hubungi Kami
Daftar Pesanan
Copyright@2012

Figure 5. Contact Us Page Display

The picture above is a display of contact information for companies that have this website. Visitors can make direct contact with the numbers that appear on web pages.

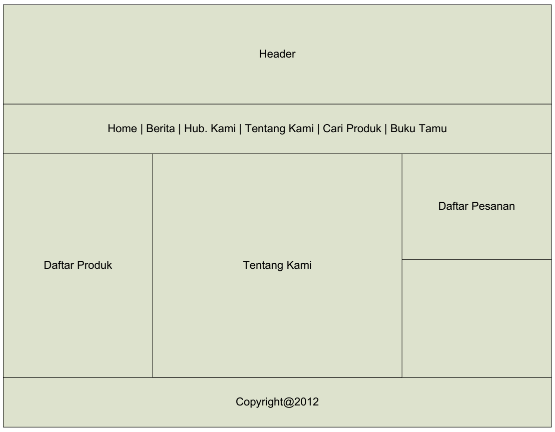
Header
Home | Berita | Hub. Kami | Tentang Kami | Cari Produk | Buku Tamu
Daftar Produk
Tentang Kami
Daftar Pesanan
Copyright@2012

Figure 6. Display Page About Us

On the page above, the page display about us, which contains information on the profile of the company such as company history, clients.

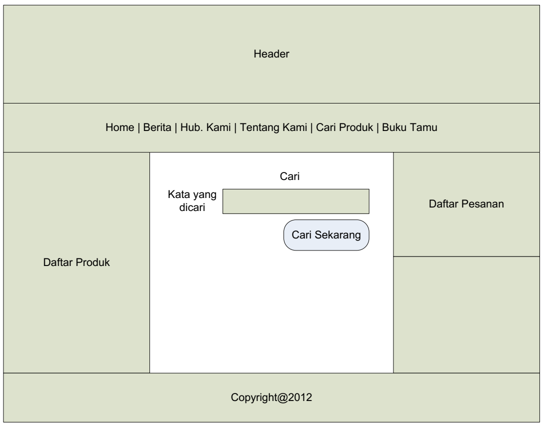

Figure 7. Display Product Search Page

The picture above is a page view for finding products. Website visitors who want to do a search by entering the data to be searched in the fields provided then click the search button.

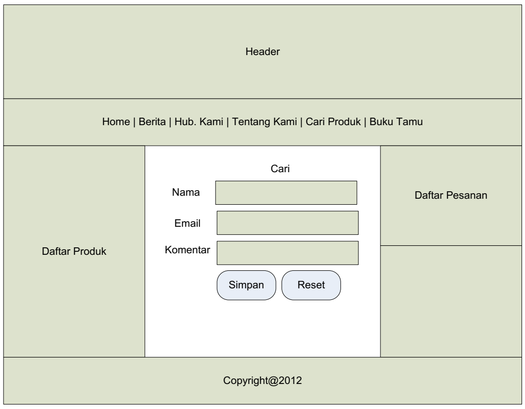

Figure 8. Guestbook Page Display

The picture above is a page view for finding products. Website visitors who want to do a search by entering the data to be searched in the fields provided then click the search button.

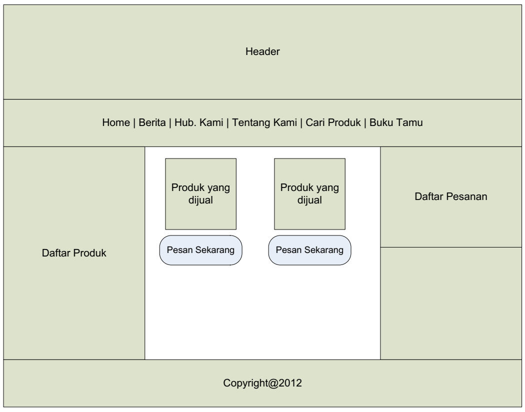

Figure 9. Display page of the product being sold

The picture above is a page display of products sold on this website. Website visitors can see a list of product categories on the left side of the page. There are several categories provided. After selecting a product category, a product will appear according to the selected category. At the bottom of the product that appears there is a message button now. To place an order for a product, click the order button now. After the message button is now clicked the order list will appear on the right side of the page.

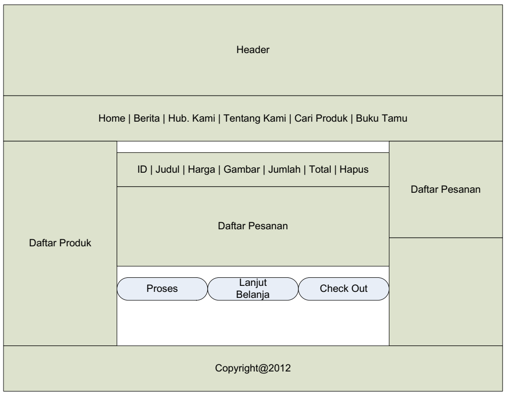
Header
Home | Berita | Hub. Kami | Tentang Kami | Cari Produk | Buku Tamu
ID | Judul | Harga | Gambar | Jumlah | Total | Hapus
Daftar Pesanan
Proses
Lanjut Belanja
Check Out
Daftar Produk
Daftar Pesanan
Copyright@2012

Figure 10. Display the Entire Order List Page

The picture above is a display page of the overall product order list. At the bottom of the order list there is a process button that functions to change the purchase data such as adding, reducing or deleting products that have been ordered. Continue shopping button functions to search for products again. Check Out button functions to end product purchase. Next is the administrator login screen on this website.

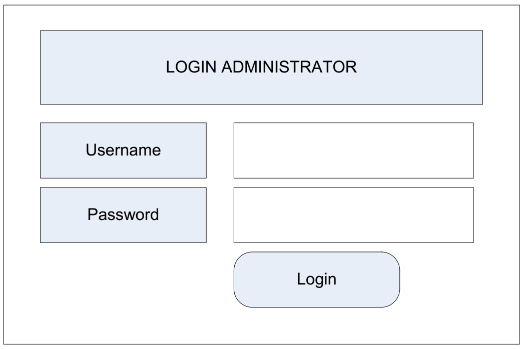

Figure 11. Display Administrator Login

In the display above is a display for administrator login. Admins must enter the correct username and password to enter the administrator page. Next, the administrator page that will be designed.

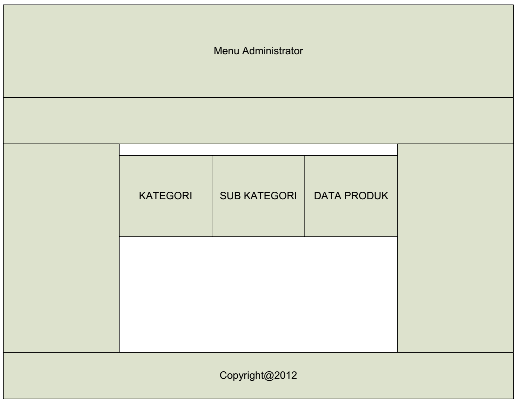

Figure 12. Display Administrator Menu

On the administrator page there is a category menu which is about product categories. Sub category contains product sub categories and product data is product data that will be sold on the website. In each there are facilities to add, change and delete data. There are also buttons for printing data.

B. Encrypt Process

Prime 1 (p) value :47
Prima 2 (q) value :71
public (e) key :79
N (p x q) value :3337
phi (N) --> (p-1) x (q-1) :3220
Private Key (d) : (1+k*3220)/79; k=1,2,3,....
find d with rounded results by trying k values
obtained private key value (d) :1019
So :
Public Key : (79,3220)
Private Key: (1019,3220)
Message (M) = HARI INI
===============
ENCRYPTION PROCESS
===============
Convert Message to Decimal Format
H = 72

A = 65
R = 82
I = 73
_ = 32
I = 73
N = 78
I = 73

For this encryption process, I break m into smaller blocks, for example m is broken into six blocks that require 3 digits

M0=726
M1=582
M2=733
M3=273
M4=787
M5=003

CipherText (C) = Plaintext (M) ^ e mod N

C0 = 726 ^ 79 mod 3337 = 215
C1 = 582 ^ 79 mod 3337 = 776
C2 = 733 ^ 79 mod 3337 = 1743
C3 = 273 ^ 79 mod 3337 = 933
C4 = 787 ^ 79 mod 3337 = 1731
C5 = 3 ^ 79 mod 3337 = 158

CipherText: 215.776.1743.933.1731.158

Plaintext (M) =Ciphertext (C) ^ d mod N

P0 = 215 ^ 1019 mod 3337 = 726
P1 = 776 ^ 1019 mod 3337 = 582
P2 = 1743 ^ 1019 mod 3337 = 733
P3 = 933 ^ 1019 mod 3337 = 273
P4 = 1731 ^ 1019 mod 3337 = 787
P5 = 158 ^ 1019 mod 3337 = 3

Convert Decimal to Ascii
Return Decryption
72=H
65=A
82=R
73=I
32=
73=I
78=N
73=I

4. CONCLUSION

The results of the discussion carried out in the previous chapter, the authors can conclude that every application related to e-commerce must have a good level of security, because the purpose of e-commerce websites is to offer products that are then related to money. In the security level of this website, I think it is good enough. There is a login facility to enter the system and encryption for each user data, it is sufficient even though it does not guarantee data will be stolen.

REFERENCES

[1] Fauzi, F., Al-Khowarizmi, A. K., & Muhathir, M. (2020). The e-Business Community Model is Used to Improve Communication Between Businesses by Utilizing Union Principles. *JITE (JOURNAL OF INFORMATICS AND TELECOMMUNICATION ENGINEERING)*, *3*(2), 252-257.

[2] Ramadhani, F., Ramadhani, U., & Basit, L. (2020). Combination of Hybrid Cryptography In One Time Pad (OTP) Algorithm And Keyed-Hash Message Authentication Code (HMAC) In Securing The Whatsapp Communication Application. *Journal of Computer Science, Information Technology and Telecommunication Engineering*, *1*(1), 31-36.

[3] Lubis, A. R., Lubis, M., & Azhar, C. D. (2019). The Effect of Social Media to the Sustainability of Short Message Service (SMS) and Phone Call. *Procedia Computer Science*, *161*, 687-695.

[4] Al-Khowarizmi, A. K., Nasution, I. R., Lubis, M., & Lubis, A. R. (2020). The effect of a SECoS in crude palm oil forecasting to improve business intelligence. *Bulletin of Electrical Engineering and Informatics*, *9*(4).

[5] Lubis, A. R., Lubis, M., Al-Khowarimi, & Listriani, D. (2019, August). Big Data Forecasting Applied Nearest Neighbor Method. In *2019 International Conference on Sustainable Engineering and Creative Computing (ICSECC)* (pp. 116-120). IEEE.

[6] Stiawan, D. (2013). E-commerce.

[7] Hidayat, R. A. (2012). Web E-Comerce Pada Tripio Komputer Menggunakan Pendekatan Business To Custemer (B2c). *Telematika*, *5*(2).

[8] Gultom, E. (2018). PERLINDUNGAN TRANSAKSI ELECTRONIC COMMERCE MELALUI LEMBAGA ASURANSI. *Jurnal Legislasi Indonesia*, *5*(4), 53-73.

[9] Shopiah, S. (2019). *PENGARUH E-COMMERCE TERHADAP PERILAKU KONSUMEN MAHASISWA FKIP UNIVERSITAS PASUNDAN (Studi Kasus Mahasiswa Program Studi Pendidikan Bahasa, Sastra Indonesia dan Daerah FKIP Unpas Angkatan 2016)* (Doctoral dissertation, FKIP UNPAS).

[10] Karay, J. B., Sembiring, I., & Purnomo, H. D. (2017). Pemetaan Berbagai Permasalahan dalam Security E-Commerce.

[11] Arrijal, I. M. A., Efendi, R., & Susilo, B. (2016). Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks. *Pseudocode*, *3*(1), 69-82.

[12] Ariyus, D. (2008). *Pengantar ilmu kriptografi: teori analisis & implementasi*. Penerbit Andi.

[13] Handoko, L. B., & Umam, C. (2019). PENYEMBUNYIAN PESAN MENGGUNAKAN STEGANOGRAFI DENGAN METODE LSB DAN ENKRIPSI KRITOGRAFI.

[14] Wahyadyatmika, A. P., Isnanto, R. R., & Somantri, M. (2014). Implementasi Algoritma Kriptografi RSA pada Surat Elektronik (E-Mail). *TRANSIENT*, *3*(4), 442-450.

[15] Putra, S. S., Sasongko, P. S., & Bahtiar, N. (2011). Verifikasi Kepemilikan Citra Medis dengan Kriptografi RSA dan LSB Watermarking. *JURNAL SAINS DAN MATEMATIKA*, *19*(3), 75-81.