Extended 16x16 Play-Fair Algorithm for Secure Key Exchange Using RSA Algorithm

Sanjay Kumar Mathur[1]* Sandeep Srivastava[2]

[1]PG Scholar

[2]Assistant Professor, Sobhasaria Group of Institutions, Sikar

Abstract – With the world entering in the 21st century rigorous efforts are being made to secure data and flow of information among the users. Though with the advancements are fast and efficient the third party intervention and security threats has also increased many folds. The algorithms being used to encrypt and decrypt data needs to be strong enough to secure the data but also simple enough for a user to handle the process. With this article a novel, practical approach is presented which not only makes the information more secured but also being based on RSA algorithm is easy enough for users to understand and implement into the systems.

Key Words: Play Fair Cipher, RSA Algorithm.

--------------------------♦----------------------------

1. INTRODUCTION

In the time of digital world, security of "information" has become critical to both organization and individuals. At the purpose once info is place away or transmitted by a message or bundles of messages by some channel there ought to be some mechanism or technique to defend that info from interruption and hacking.

The interrupted data flow and hacking may lead to unwanted avalanche of events that can hinder with a security of nation and/or privacy of an individual(s). Thus there's a needs of certain mechanism which can protect the information all through the channel from any outside intervention and provide robust against the changing environmental conditions which may lead to wrong interpretation of the data at the receiver.

Consequently, Cryptography assumes an imperative part in data communication in today's digital world or in internet. Current cryptography is a piece of mathematics and innovation of software engineering. Applications of cryptography incorporate all PC passwords, ATM cards, and electronic trade.

The present research concentrates on the attempting to being improve the existing Play-fair technique (5x5 matrix) to 16x16 size of rectangular matrix with the assistance of RSA algorithm (asymmetric key cryptography), to provide information security and handle them with right sorts of counter measures. The security of key will lead us to secure data from being hacked and make data more robust against noise.

2. CRYPTOGRAPHY

Cryptography can be defined as a practice and study of science which leads to hiding of user data from any external intervention (like noise, security hacks, etc.) and provide a safer way to commute between the transmitting and receiving party. Cryptography leads to various aspects of information security such as data confidentiality, data integrity, authentication and non-repudiation. Cryptography in its most primitive definition is the process of encryption and decryption. Encryption is the process of converting the user's message (plaintext) to a certain unreadable nonsense text (ciphertext). This will allow the system to become robust against the possible data security threats. On the other hand, Decryption is the process of reconverting the cipher text back to original plaintext of the user. Here the important point is the data should not get changed during the process which will lead to different conclusions. During recent decades the cryptography has been extended further to include message integrity checking, sender/receiver identity authentication, digital signatures and interactive proofs and secure computation, among others.

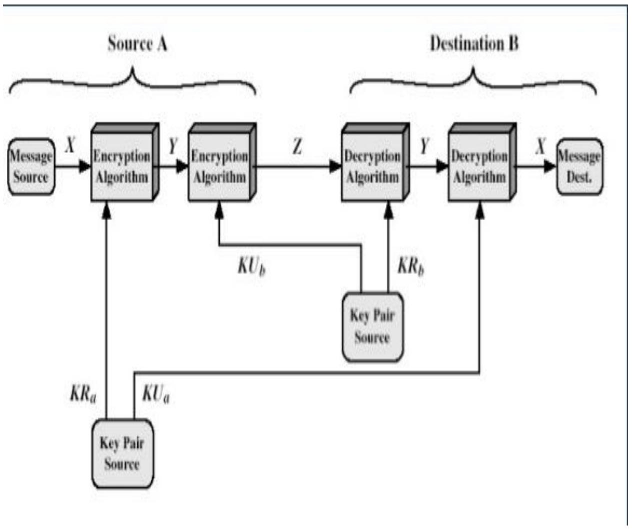

Fig.2.1 Public Key Encryption Algorithm

2.1 Types of Cryptography

In the modern computer era, Cryptography is basically divided into two types:

1. Symmetric-key cryptography

2. Asymmetric or Public-key cryptography.

In Symmetric Key cryptography includes type of encryption methods in which both the sender and receiver share the same key whereas Asymmetric or private key cryptography comprises of two different but mathematically connected keys named public and private keys in this public-private key system, the public key is known to everyone but private key is kept secured and unknown to anyone other than the user. Public key will encrypt the data in such a way that only the private key can decipher it. The main advantage of using public-key algorithm is the security of the key. The Symmetric key algorithms as mentioned above have to secure the key so as to make communication more secured. But to keep it secured one needs to make the private key as complex as possible so as to prevent eavesdropping and third party intervention. But to make key secured it needs to be complex which will make the system complex as well and increase the number of mathematical calculations. Due to such technical difficulties idea of Asymmetric keys was proposed in June 1976. With the new concept coined the first success was made in 1978 with introduction of RSA algorithm.

3. RSA ALGORITHM

RSA Algorithm named after the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1978. RSA algorithm is based on the idea that the factorization product of two large prime numbers is very hard to calculate. The user of RSA algorithm generates and publically issues a public key along with one auxiliary value that is used during calculations. The prime numbers must be kept private. The receiver with the public key and with its own private key decrypts the plaintext back from ciphertext.

4. PLAY FAIR ALGORITHM

The Play-fair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher. To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting "Q" to reduce the alphabet to fit; other versions put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for filling in the 5 by 5 table constitutes the cipher key. To encrypt a message, one would break the message into bigrams (groups of 2 letters) such that, for example, "Hello World" becomes "HE LL OW OR LD", and map them out on the key table. If needed, append an uncommon monogram to complete the final bigram. The two letters of the bigram are considered as the opposite corners of a rectangle in the key table. Note the relative position of the corners of this rectangle. Then apply the following 4 rules, in order, to each pair of letters in the plaintext:

1. If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Play-fair use "Q" instead of "X", but any letter, itself uncommon as a repeated pair, will do.

2. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).

3. If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).

4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first

letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.

5. PROPOSED ALGORITHM

5.1 At the Sender ends:

Step one: Construct a modified table of Play-fair cipher technique of size 16X16, that contain each one of the alphabets frame begin to end capitalized and a to z in lower-case letter, all the special characters that are on the keyboard and each numeric esteem (from zero to 9).

The PF encryption technique is separation into 2 stages:

a) First stage is creation and population of Matrix (by mistreatment the key).

b) The second stage is encryption process of the plain text message with the assistance of the Matrix. Make the Cipher text (CT1) of the plain text.

Step Two: Utilize the key of Playfair technique as a Plain Text in RSA algorithm to make the Cipher text (CT2) of the key and send to the receiver.

5.2 At the Receiver ends.

Step Three: decrypt the Cipher Text (CT2) into Plain Text (Playfair matrix key).

Step Four: construct a modified table of Playfair cipher technique of size 16X16, which contain all the alphabets from A to Z upper case and a to z in lower case, all the special characters which are on the keyboard and every one numeric values (from zero to 9). The PF decryption technique is split into 2 phases:

c) First part is creation and population of Matrix (by using the key).

d) The second section is decryption method of the cipher text (CT1) message with the help of the matrix and makes the plain text.

5.4 Experiment Analysis

The proposed work is dividing in two phases:

- The principal stage for Matrix construction utilizes every one of the standards of customary Play fair matrix with these changes:

- The 2 I and J letters in upper case and lower-case letter are considered as 2 unique letters (I and J are different and that i and j are distinctive).

- It enables more than 26(up to 256 characters with no duplicate) characters as key.

- It is case sensitive; it utilizes the upper case as well as lower case characters.

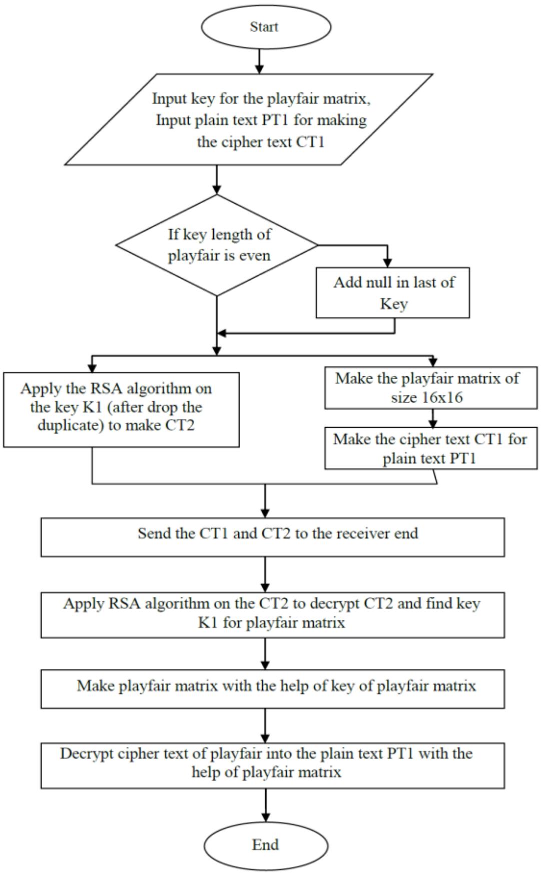
Start
Input key for the playfair matrix, Input plain text PT1 for making the cipher text CT1
If key length of playfair is even
Add null in last of Key
Apply the RSA algorithm on the key K1 (after drop the duplicate) to make CT2
Make the playfair matrix of size 16x16
Make the cipher text CT1 for plain text PT1
Send the CT1 and CT2 to the receiver end
Apply RSA algorithm on the CT2 to decrypt CT2 and find key K1 for playfair matrix
Make playfair matrix with the help of key of playfair matrix
Decrypt cipher text of playfair into the plain text PT1 with the help of playfair matrix
End

Fig.5.1 Algorithm for Proposed Methodology

6. RESULTS AND DISCUSSION

6.1 Performance Analysis

This chapter delineates the techniques connected in keeping the content secret through character upheld, frequency analysis, and required matrix for brute force attack.

6.1.1 Character Supported

From the over 9 illustration, we can see that there is no any two consequences of cipher text 1 and cipher text 2 are same. So we can state that this algorithm is sufficient safe from the attacks.

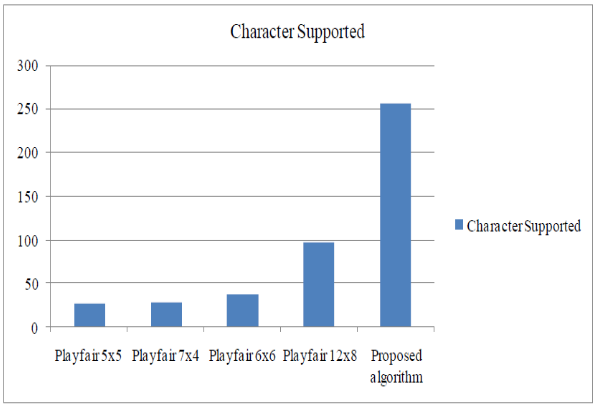

Fig. 6.1 Graph number of character supported by different algorithm.

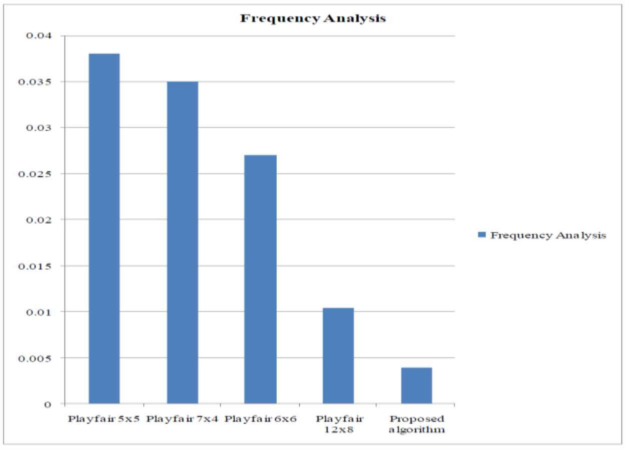

Fig. 6.2 Graph of frequency analysis attack by different algorithm.

With the comparison with existence algorithm this proposes algorithm takes the preferred standpoint on them in number of character upheld. Fig 6.1 shows this comparison.

6.1.2 Frequency Analysis

Now, with the comparison with existence algorithm this proposes algorithm takes the advantage on them in frequency analysis attack. Fig 6.2 shows this comparison.

6.1.3 Brute Force Attack

In the last comparison with existence algorithm this proposes algorithm takes the advantage on them in Brute Force Attack. Fig 6.3 shows this comparison.

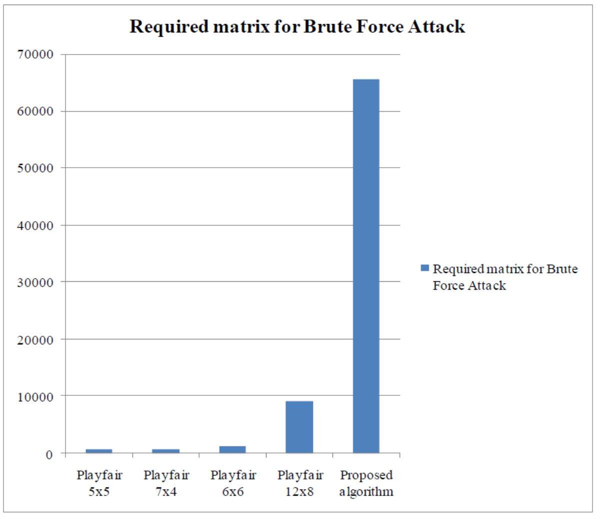

Fig. 6.3 Graph of required matrix for Brute Force Attack on different algorithm.

6.2 Advantage of Algorithm

- In this algorithm 256character are utilized therefore it exploits on 5x5 matrix that utilized the 26 characters.

- The planned 16×16 Play fair cipher may be said to be protected against Brute Force Attack, because the attacker must find in a 256×256 = 65536 digraphs.

- Increasing the key size likewise reduces the probabilities to interrupt the cipher by the Frequency Analysis. The chance of occurrence of a part within the original Playfair(PF) matrix table of size 5×5 was 1/26 = 0.0384, though within the extended16×16Playfair matrix the likelihood is that 1/256 = 0.00390625,which is way less when compared and it makes the frequency analysis a more durable employment.

- The "I" and "J" character are in various cell house between 2 words within the Plain Text is considered together character. Special characters are utilized as a vicinity of this formula.

- The uppercase and graphic symbol alphabets are during this formula.

- An extra letter NULL is included once the word consists of weird number of character within the decryption method this NULL is disregarded.

- The arrangement ought to be completely secure. The key dispersion issue must be settled by this arrangement.

- There are some ASCII values which can't printable on the screen so it is hard to retrieve the message by the hacker.

7. CONCLUSION AND FUTURE WORK

7.1 Conclusion

Keeping in mind the end goal to beat demerits, we've got proposed an extension to customary PF cipher algorithm; which may be utilized all the additional with efficiency notwithstanding for the Plain Text containing alphanumeric esteems and special characters and utilize the flip factor for the high avalanche result. Then a public key encryption system has been designed that provides the authentication and confidentiality but there are a couple of limitations. Complete mathematical reasoning is given to demonstrate the exact outcome at each sender and receiver sides the previous encryption technique is likewise a chunk of this technique. Once completion of program the strength of the technique has been checked and this encryption technique will likewise be utilized for alternative networks. During this algorithm play-fair matrix is employed for making the cipher text and also the RSA algorithm is used for providing the secure channel.

7.2 Future work

1. Later on when new technology of cryptanalysis will come in the market, to prevent the data frame that kind of attack, enhance this work in such sort that it will be spare our data from that kind of attack on data. There are a few proposals for the future work.

2. Work on the algorithm for encryption and decryption of the picture, sound, video.

3. Try to create the algorithm which provides more security than this algorithm, because security of key is relies on upon the RSA algorithm so take the vast prime number as the estimation of P and Q.

4. Make simple key dispersion, if there is more than on receiver.

5. Decrease the decryption time of the RSA algorithm.

REFERENCES

A. Aftab Alam, B. Shah Khalid, and C. Muhammad Salam (2013). "A Modified Version of Playfair Cipher Using 7×4 Matrix". International Journal of Computer Theory and Engineering, vol.-5, no. 4, August 2013.

Ali Mir Arif Mir Asif, and Shaikh Abdul Hannan (2014). "A Review on Classical and Modern Encryption Techniques", International Journal of Engineering Trends and Technology (IJETT) – Volume 12.

Arvind Kumar, Pawan Singh Mehra, Gagan Gupta, and Manika Sharma (2013). "Enhanced Block Playfair Cipher", International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. QShine: Quality, Reliability, Security and Robustness in Heterogeneous Networks, pp. 689-695.

Atul Kahate (2010). "Cryptography and Network Security", 2nd edition, McGraw-Hill.

Ayushi Kansal, Shruti Sneha, and Manish Kumar Patel (2016). "Modifying Playfair Cipher by Using DNA and Amino Acids", International Journal of Education and Science Research Review , E-ISSN 2348-6457, Volume-3, Issue-2, www.ijesrr.org.

Behrouz A. Forouzan (2007). Cryptography and Network Security. Special Indian Edition, Tata McGraw- Hill Publishing Company Limited, New Delhi.s

Bhagyashree Bodkhe, and D. C. Jain (2012). "An Enhanced Play-fair Cipher Cryptographic Substitution Algorithm with 6X6 Matrix", Journal of Current Engineering Research, 2 (3), PP. 1-4.

Chandan Kumar, Sandip Dutta, and Soubhik Chakraborty (2015). "A Hybrid Polybius-Playfair Music Cipher", International Journal of Multimedia and Ubiquitous Engineering Vol.10, No.8, pp.187-198 http://dx.doi.org/10.14257/ijmue.2015.10.8.19.

Charles Edge (2007). William Barker & Zack Smith A brief history of cryptography, Foundation of Mac OS X Security.

David Terr History of cryptography, http://www.davidterr.com/science-articles/cryptography.html

Fauzan Saeed and Mustafa Rashid (2010). "Integrating Classical Encryption with Modern Technique", IJCSNS International Journal of Computer 280 Science and Network Security, Vol.10, No.5, Page 280-285.

Gaurav Agrawal, Saurabh Singh, Manu Agarwal (2011). "An Enhanced and Secure Playfair Cipher by Introducing the Frequency of Letters in any Plain text", Journal of Current Computer Science and Technology Vol. 1 Issue 3, pp. 10-16.

Hadab Khalid Obayes (2013). "Suggested Approach to Embedded Playfair Cipher Message in Digital Image", Hadab Khalid Obayes . Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 3, Issue 5, pp. 710-714.

Harinandan Tunga, Soumen Mukherjee (2012). "A New Modified Playfair Algorithm Based On Frequency Analysis", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 1.

Lt. Ravindra Babu Kallam, Dr. S. Udaya Kumar, Dr. A. Vinaya Babu and Dr. M. Thirupathi Reddy (2010). "A Block Cipher Generation Using Color Substitution", ©2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 28.

Mona Sabry, Mohamed Hashem, Taymoor Nazmy, Mohamed Essam Khalifa (2010). "A DNA and Amino Acids-Based Implementation of Playfair Cipher" , (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 3.

Monika Arora, Anish Sandiliya, and Jawad Ahmad Dar (2015). "Modified Encryption Technique by Triple Substitution on Playfair Square Cipher Using 6 By 6 Matrix with Five Iteration Steps" International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 5, Issue 4.

Muhammad Salam, Nasir Rashid, Shah Khalid, and Muhammad Raees Khan (2011). "A NXM Version of 5X5 Playfair Cipher for any Natural Language (Urdu as Special Case)", World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:5, No:1.

Nisarga Chand, and Subhajit Bhattacharyya (2014). "A Novel Approach for Encryption of Text Messages Using PLAY-FAIR Cipher 6 by 6 Matrix with Four Iteration Steps", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 1.

Packirisamy Murali and Gandhidoss Senthil kumar (2009). "Modified Version of Playfair Cipher using Linear Feedback Shift Register", 2009 International Conference on Information Management and Engineering, Page 488-490.

Packirisamy Murali and Gandhidoss Senthilkumar (2008). "Modified Version of Playfair Cipher using Linear Feedback Shift Register", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12.

Priyanka Goyal, Gaurav Sharma and Shivpratap Singh Kushwah (2015). "Network Security: A Survey Paper on Playfair Cipher and its Variants", International Journal of Urban Design for Ubiquitous Computing Vol. 3, No. 1, pp.1-8 ttp://dx.doi.org/10.21742/ijuduc.2015.3.1.01

Ravindra babu, Udaya Kumar, Vinaya babu (2011). "An Extension to Traditional Play Fair Cipher Cryptographic Substitution Method", IJCA, 0975-8887, vol.-17, No. 5.

Robbi Rahim, and Ali Ikhwan (2016). "Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher", © IJSRST | Volume 2 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X Themed Section: Science and Technology.

S. S. Dhenakaran, and M. Ilayaraja (2012). "Extension of Playfair Cipher using 16X16 Matrix", International Journal of Computer Applications (0975 – 888) Volume 48– No.7.

Sagar Gurnani, Nitish Mhalgi, Samyukta Iyer, and Deepika Dixit (2013). "Modified 3-D Playfair Stream Cipher", International Journal of Computer Applications (0975 – 8887) Volume 84 – No 15.

Sanjay Basu, and Utpal Kumar Ray (2012). "Modified Playfair Cipher using Rectangular Matrix", International Journal of Computer Applications (0975 – 8887) Volume 46– No. 9.

Shiv Shakti Srivastava, Nitin Gupta (2011). "A Novel Approach to Security using Extended Playfair Cipher", International Journal of Computer Applications (0975 – 8887) Volume 20– No. 6.

Sriram Ramanujam and Marimuthu Karuppiaj (2011). "Designing an algorithm with High Avalanche Effect", IJCSNS International Journal of Computer Science and Network Security, Vol. 11, No. 1, Page 106-111.

Subhajit Bhattacharyya, Nisarga Chand & Subham Chakraborty (2014). "A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps" International Journal of Advanced Research in Computer Engineering & Technology vol.-3, Issue 2.

Surendra Singh Chauhan, Hawa Singh, and Ram Niwas Gurjar (2014). "Secure Key Exchange using RSA in Extended Playfair Cipher Technique", International Journal of Computer Applications (0975 – 8887).

V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani (2009). "A Modified Playfair Cipher Involving Interweaving and Iteration", International Journal of Computer Theory and Engineering, Vol. 1, No. 5, pp. 1793-8201.

William Stallings (2006). "Cryptography and Network Security: Principles and Practice", 4th edition, Prentice Hall.

Corresponding Author

Sanjay Kumar Mathur*

PG Scholar

E-Mail – **sameer.sanjaymath0@gmail.com**