Journal of Engineering and Applied Sciences 13 (16): 6844-6849, 2018
ISSN: 1816-949X

Wichmann-Hill PRNG based Design Smart Digital Door Lock Using Android-Arduino

Ahmed Kawther Hussein and Ali Shakir
Department of Computer Science, College of Education, University of Al-Mustansiriyah, Baghdad, Iraq

Abstract: Security is considered as a major issue especially in home security which is necessary as the possibilities of intrusion increasing day by day. Part of home security is the design of a smart door lock system and is very important because it is closely associated to the safety of the home owner. The data transceiver of existing smart door lock system is weak to be forgery and hacking. To improve these security issues, we propose a smart door lock by improving the PIN number generated using Wichmann-Hill PRNG algorithm in Android OS (smartphone) and transmitted to digital door lock controller via. Bluetooth. The proposed design can increase the security of control digital door lock by using the PIN generated by Wichmann-Hill PRNG and show evaluation of attack both PINs, normal and Wichmann-Hill generated by using brute force attack tools which comes with the Wichmann-Hill is harder and takes years to attack where normal PIN takes minutes to attack.

Key words: Smart door lock, PIN, Wichmann-Hill PRNG, Bluetooth, Arduino Android, Brute force attack tool

INTRODUCTION

Recently, there are a lot of studies and researches interested in technologies-based home automation and security. One of these technologies is smart door locks with wireless security system using Bluetooth (Ismail, 2014). A numerous studies from the Alarm Industry Research and Educational Foundation (AIREF) in 2010, home housebreakers take <60 sec to breaking into a house through doors (Anonymous, 2013). For this reasons and others, essential to make a house's doors further secured and harder to be opened that comes by with home security systems and smart digital door locks. The progress of many security systems for housing, commercial applications and smart home take it in consideration during designs and implementations (Ibrahim *et al*., 2015). These systems concentration on the security of smart home technology which developed and enhanced, based on some suitability functionalities such as door access authentication, dependability of controller circuit design and secured data in communication medium during pass the key code via. wire or wireless medium (Suryadevara and Mukhopadhyay, 2015; Park *et al*., 2009). The design of digital door lock is considered as one of the most modern digital devices which take place of conventional types of locks because of the utilize convenience and low-cost. Also, digital door lock works by the entering combination of digital key, security password or number codes sets higher secure protection with reliability over the conventional locking systems. Therefore, it is a good digital device fitting for checking the access information and controlling the door on or off because everyone has to access to the door lock to go inside or outside (Norman, 2011).

Numerous studies that have been available on the subjects of home security and digital door lock are as follows: by Sahani *et al*. (2015) design and the implementation of home security for door lock/unlock using GSM, ZigBee and web-enabled and control systems based on human face recognition technology and remotely monitoring technology, to confirm visitor identity and to control door accessibility. There are many resources used in this research, face recognition, monitoring information and transceiver data from remote device to control device via GSM and ZigBee. These resources consumes various energies and processing during operation. Lee *et al*. (2017) discussed the use of RSA algorithm which depend on public-key in design electronic lock system using gesture password via. Wi-Fi. By Ismail *et al*. (2014), they have designed method in smart home for door lock to serve the disabilities people to lock/unlock digital door lock via. Bluetooth. No security issued has implemented in contrast to our work this approach can be break with short time while our work

Corresponding Author: Ahmed Kawther Hussein, Department of Computer Science, College of Education, University of Al-Mustansiriyah, Baghdad, Iraq

focused on generated 10-digits long. Kader *et al.* (2016) in this study design digital door lock using fingerprint model as method for authentication in contrast to our research, this method need training data (fingerprint samples) and fingerprint model is cost compared to our method which not need any sensor devices and database.

Random number generators: Random numbers considered as an important role in the use of encryption for numerous network security applications. There are three types of Random Number Generators (RNG): the first types are the True Random Number Generators (TRNGs) which their result cannot be repeated. TRNGs are based on physical testing such as coin flipped 80 times and the result detailed as binary bit. So, it is difficult to generate bit similar bit again by using of the similar way.

The second types are Pseudorandom Number Generators (PRNG) generates structures that are calculated from a first seeds and produces a structure of result bits using a deterministic algorithm. Usually, PRNG may have a feedback path. PRNG uses the flowing formula: A, B and m are integer constants:

$$s[i+1] = s[i]*A+B \bmod m;\ i = 0, 1, 2, 3, \ldots, \quad s[i];\ A, B \in 0, 1, 2, 3, \ldots, \tag{1}$$

Third type is Pseudorandom Number Function (PRF) is used to generate a pseudorandom string of bits of around fixed length such as fixed length keys (Elmahi *et al.*, 2007).

One of the public methods of PRNG used for generating the pseudo uniform random numbers is the congruence defined by:

$$X_{i+1} = (aX_i+c)(\bmod m)\ i = 1, 2, 3, \ldots, n, \ldots, \tag{2}$$

where multiplier a, the growth c and modulus m are non-negative integers. It means, if (aX_i+c) is divided by m, then the remainder is i 1 X+. In this equation m is a big number such that m = 2w-1 where w is the word size of the computer in use for producing the (m-1) numbers and (i = 0) is seed value. The seed value means any initial value applied for generating a set of random numbers. Seed value has to be different for different set of random numbers (Ahmed and Rahaman, 2016).

MATERIALS AND METHODS

Proposed design description: The proposed work has two main blocks, remote device and door lock electronic circuit as show in Fig. 1. The procedure of whole proposed work is illustrated in Fig. 2.

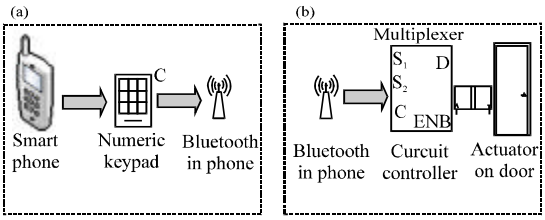

Fig. 1: Conceptual diagram of proposed work: a) Remote device and b) Door lock circut

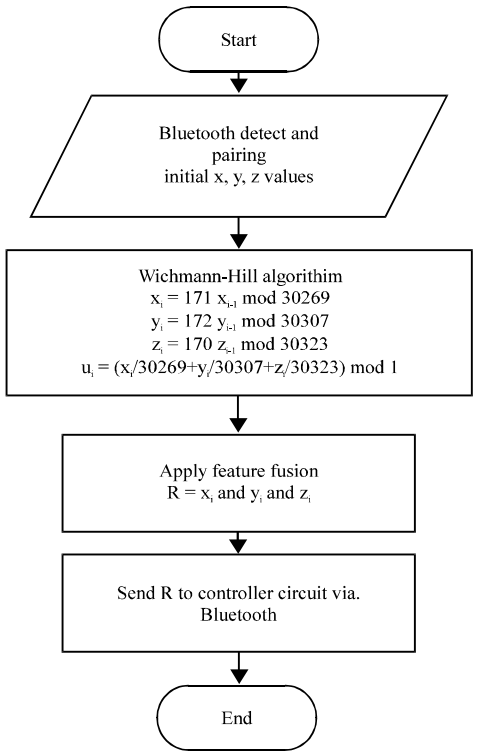

Fig. 2: Main procedure of proposed work

Smartphone remote application: An application of remote device has been designed in Android OS as shown in Fig. 3. The application has consists of list of available compatible Bluetooths in range of detection, three entry fields for Wichmann-Hill algorithm and one field for the algorithm result, two commands to lock and unlock the door.

The smartphone is communicating and integrated frameworks and is involves of several sensors and numerous wireless data communication such as Bluetooth and Wi-Fi (Sahani *et al.*, 2015). In the proposed work, the programming language of application design for remote device is Android OS using MIT App. inventor framework.

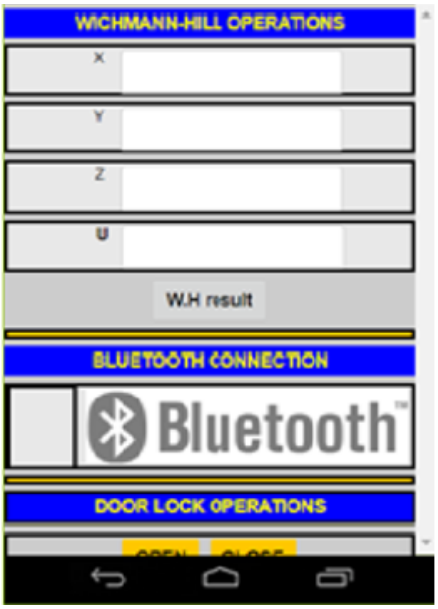

Fig. 3: Android application design

Bluetooth procedure in remote device: The procedure of Bluetooth connection and data transceiver is explain in Fig. 4. The flow block diagram of Bluetooth procedure is showing in Fig. 5.

Implementation of Wichmann-Hill in remote device: The normal length of user code combination used in authentication devices is 4-digits entered by using keypad. The proposed algorithm for authentication has been apply a Wichmann-Hill algorithm which is one of Pseudorandom Number Generator (PRNG) to generate complex code by combined of three congruential generators as in Eq. 3 (Lee *et al*., 2017):

$$\begin{aligned} x_i &= 171x_{i-1} \bmod 30269 \\ y_i &= 172\ y_{i-1} \bmod 30307 \\ z_i &= 170\ z_{i-1} \bmod 30323 \\ u_i &= \left(\frac{x_i}{30269}+\frac{y_i}{30307}+\frac{z_i}{30323}\right) \bmod 1, \ldots, \end{aligned} \quad (3)$$

As noted in above, need to set three seeds (x_0,y_0 and z_0) as an initial values which in our case is the digits of PIN number for example, let the PIN $x_0 = 3$, $y_0 = 5$ and $z_0 = 9$, the u value is #5138601530, we have used feature fusion method. The feature fusion is part of data fusion used to concatenated data/features into new set.

In this phase of proposed research, we have applied feature fusion method for grouping or combining the

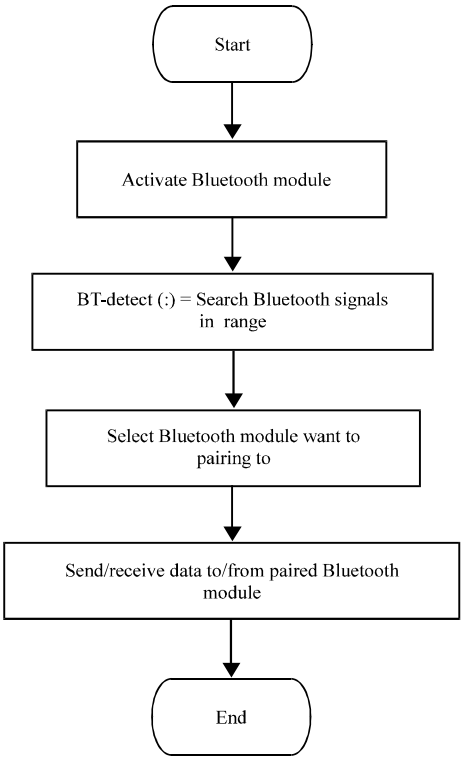

Fig. 4: Bluetooth connection and data transceiver procedure

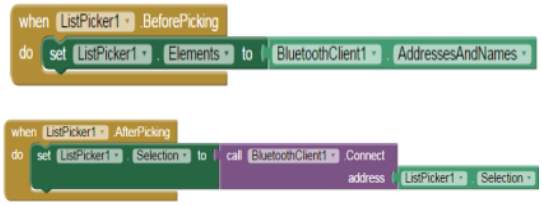

Fig. 5: Bluetooth flow code in MIT App. inventor

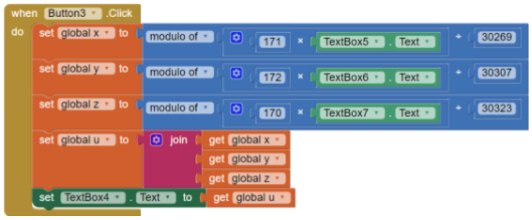

Fig. 6: Wichmann-Hill algorithm in MIT App. inventor

Wichmann-Hill results (513, 860 and 1530) as in example above, together in one new set (5138601530) to be send to lock/unlock door lock. The flow block diagram of Wichmann-Hill algorithm is showing in Fig. 6.

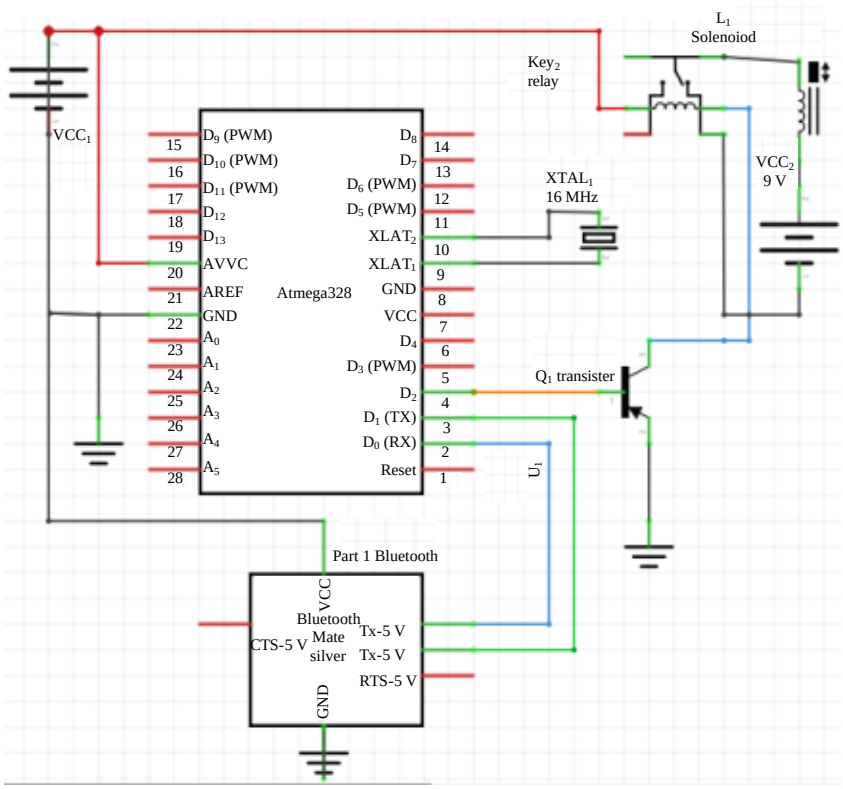

Fig. 7: Schematic of controller circuit design for proposal work

Controller circuit: The controller circuit has been designed based on ATMEGA328 microcontroller and Bluetooth modular used as communication medium in addition, relay (5 V) component used to switching the actuator (door lock driver) on/off. The schematic of controller circuit design is showing in the Fig. 7.

Controller circuit description: The electronic circuit operation has been describe in flow chart in Fig. 8. The Bluetooth device in controller circuit waiting to pairing with another adapter (Bluetooth device) within the range of signal detection. After detected, need to exchange the passkey, default "123" when this verified, the both Bluetooth paired now ready to exchange the information in our research, the PIN number generated by Wichmann-Hill algorithm.

After Bluetooth device received the information, a program in microcontroller will check if the length of the information is matched with saved key such as the length of Wichmann-Hill number generated is 10 digits if the PIN entered by user in his/her smart phone is 3 digits. The next step is checking PIN received with key saved in microcontroller flash memory if both matched or not.

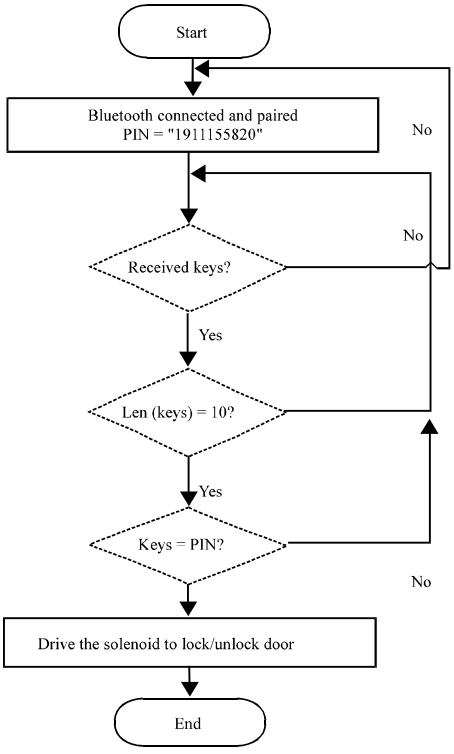

Fig. 8: Controller circuit operation

Finally, if the key and PIN matched, a digital pin (D2) in ATMEGA328 will set HIGH (ON) and send this signal to the base of transistor to switches the load which drive the solenoid to lock/unlock the door.

RESULTS AND DISCUSSION

The main concept of the proposed work is enhancing security of the digital key access in digital door lock. There are two main subjects in the proposed work, the remote controller and the controller circuit.

The remote control, it is an application design based on Android OS for smart phones, used to enter the secured key 3 digits by digital keypad and this key encrypted by Wichmann-Hill PRNG algorithm to generate complex key code. Then, the generated key transmitted via. Bluetooth to the paired one which attached to controller circuit. The application design of remote control shown in Fig. 9. The application of remote control consists of following objects:

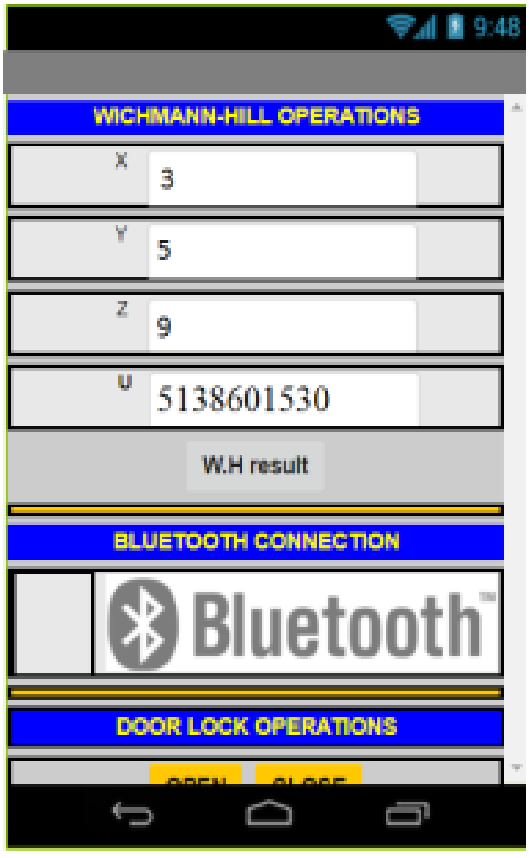

Fig. 9: Remote control application design for Android OS

- PIN field: textbox used to enter the 3-digits combination key and one field for result
- W.H result: textbox used to display the result of generated new key using Wichmann-Hill PRNG algorithm
- List Picker: a push button used to select a Bluetooth to pair and connect
- Lock/Unlock: a push button used to control the digital door lock

The controller circuit has been design to control the door lock by driving relay to switch the solenoid on/off. In addition, Arduino Uno Kit has used to control the Bluetooth for pairing and receiving the key, then comparing this key with stored key in flash memory of microcontroller. When the both of keys matched, a command be send to switch the transistor to drive the relay. The electronic components used in controller circuit design shown in Fig. 10:

- Arduino Uno kit
- HC-06 Bluetooth module
- Relay: used to control the solenoid (on/off)

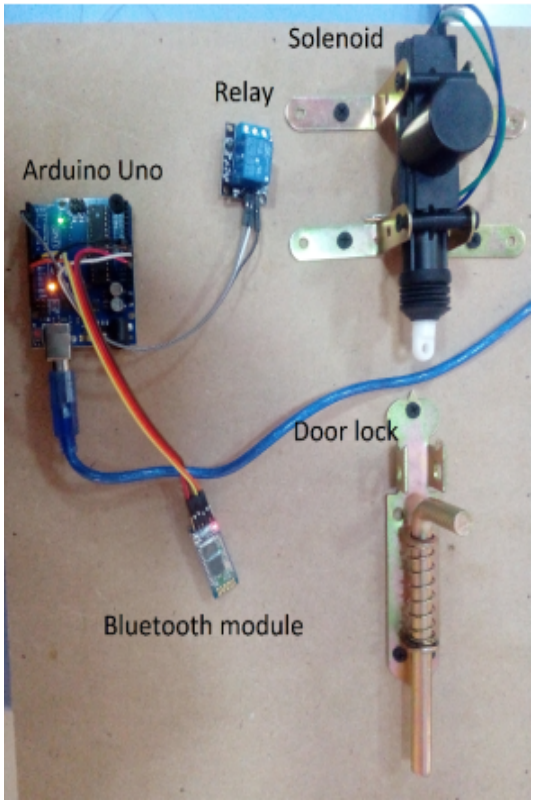

Fig. 10: Circuit design for digital door lock controller

CONCLUSION

This study focuses on the design and implementation of smart digital door lock using Wichmann-Hill as new PIN generator with Bluetooth technique as communication medium for transceiver data. The proposal work has two main parts, remote control (smart phone) and controller circuit.

The remote control has been designed for Android OS by using block programming App. inventor environment. An Arduino UNO kit has used as a controller circuit to control the door lock's motor. We have evaluate the security of PIN code for digital door lock by applying Wichmann-Hill algorithm compared with standard 4-digits. The comparison evaluated by finding spent time to possible attacking PIN using brute force attack online tool. The calculation has done for both length of key 4-digits and key generated by Wichmann-Hill PRNG algorithm. In addition, the setting the delay time or speed of pass password per sec is 0.40 sec considered as a Bluetooth transceiver delay. The implementation of Wichmann-Hill algorithm in this research increased the generated number of digits of PIN then leads to more complexity to break. During experimental research, we have used brute force attack tools and found that the time spent to attack 4-digits is 42 min where the time spent to attack Wichmann-Hill PRNG is about 80 years.

REFERENCES

Ahmed, T. and M.M. Rahman, 2016. The hybrid pseudo random number generator. Intl. J. Hybrid Inf. Technol., 9: 299-312.

Anonymous, 2013. Convicted burglars confirm value of alarms, other deterrents. Alarm Industry Research & Educational Foundation (AIREF), Irving, Texas. http://airef.org/burglars-confirm-value-of-alarms/

Elmahi, M.Y., S. Kosti and M.H. Sayed, 2017. Text steganography using compression and random number generators. Intl. J. Comput. Appl. Technol. Res., 6: 259-263.

Ibrahim, A., A. Paravath, P.K. Aswin, S.M. Iqbal and S.U. Abdulla, 2015. GSM based digital door lock security system. Proceedings of the 2015 International Conference on Power, Instrumentation, Control and Computing (PICC'15), December 9-11, 2015, IEEE, Thrissur, India, ISBN:978-1-4673-8072-0, pp: 1-6.

Ismail, N.H., Z. Tukiran, N.N. Shamsuddin and E.I.S. Saadon, 2014. Android-based home door locks application via. Bluetooth for disabled people. Proceedings of the IEEE International Conference on Control System, Computing and Engineering (ICCSCE'14), November 28-30, 2014, IEEE, Batu Ferringhi, Malaysia, ISBN:978-1-4799-5687-6, pp: 227-231.

Kader, M.A., Y. Haider, R. Karim, S. Islam and M.M. Uddin, 2016. Design and implementation of a digital calling bell with door lock security system using fingerprint. Proceedings of the International Conference on Innovations in Science, Engineering and Technology (ICISET'16), October 28-29, 2016, IEEE, Dhaka, Bangladesh, ISBN:978-1-5090-6123-5, pp: 1-5.

Lee, C.T., Y.C. Chung, T.C. Shen and K.W. Weng, 2017. Development of electronic locks using gesture password of smartphone base on RSA algorithm. Proceedings of the 2017 International Conference on Applied System Innovation (ICASI'17), May 13-17, 2017, IEEE, Sapporo, Japan, ISBN:978-1-5090-4898-4, pp: 449-452.

Norman, T.L., 2011. Electronic Access Control. Elsevier, New York, USA., ISBN:978-0-12-382028-0, Pages: 423.

Park, Y.T., P. Sthapit and J.Y. Pyun, 2009. Smart digital door lock for the home automation. Proceedings of the IEEE Region 10 Conference on TENCON 2009-2009, January 23-26, 2009, IEEE, Singapore, ISBN: 978-1-4244-4546-2, pp: 1-6.

Sahani, M., C., Nanda, A.K. Sahu and B. Pattnaik, 2015. Web-based online embedded door access control and home security system based on face recognition. Proceedings of the 2015 International Conference on Circuit, Power and Computing Technologies (ICCPCT'15), March 19-20, 2015, IEEE, Nagercoil, India, ISBN:978-1-4799-7075-9, pp: 1-6.

Suryadevara, N.K. and S.C. Mukhopadhyay, 2015. Smart Homes: Design, Implementation and Issues. Vol. 14, Springer, Berlin, Germany, ISBN:978-3-319-13556-4, Pages: 176.