ISSN: 1231-4005
e-ISSN: 2354-0133
DOI: 10.2478/kones-2019-0045

USE OF CRYPTOGRAPHY PRINCIPLES IN DIGITAL REGISTRATION DEVICES

Agnieszka Aleksandra Szokało

*Lublin University of Technology, Mechanical Engineering Faculty
Institute of Transport, Combustion Engines and Ecology
Nadbystrzycka Street 36, 20-618 Lublin, Poland
e-mail: aszokalo@interia.pl*

Marcin Rychter

*State Higher Vocational School in Ciechanów, Faculties of Engineering and Economics
Department of Mechanics and Machine Building
Narutowicza Street 9, 06-400 Ciechanów, Poland
e-mail: rychter@poczta.fm*

Abstract

Cryptography is a field of science necessary to solve problems with encryption of classified messages. The security of electronic information is an integral part of the digital tachography system. From year to year, there is a noticeable increase in electronic data logging systems in many aspects of life. The control measures created for the purpose of performing roadside checks are not sufficient to detect all violations in the recording equipment. Many violations that have occurred during the use of the vehicle are stored in the device's memory. The article describes the basic mathematical rules illuminating cryptography. The hazards to which the motion sensor installed in the vehicle may be exposed are described. Breaking safety in transport systems may lead to incorrect results of inspections carried out while the vehicle is stopped by authorized services. The article also provides information on the authorities responsible for issuing cards for digital tachographs. Nowadays, documents are increasingly issued with the use of a digital signature. The digital signature of its origin is based on the principles of cryptography. The security key seems to be complicated for the average user. The article discusses the topic of tachograph construction, in particular the schematic responsible for information encryption.

Keywords: *tachograph cards, cryptography, digital tachograph system, recording equipment, road transport*

1. Introduction

Cryptography is a science that aims at writing non-public messages to a casual reader. The message itself is concealed, but the existence of this message is available and public. The origin of the pictographic script comes from ancient Egypt, where the drawings were not only confidential symbols, but above all, they existed to beautify and decorate the interior of the tombs. The most famous encryption method was Cezar's cipher (Juliusz Caesar was the creator of this cipher), which based on substituting for a public letter, a letter placed three places further in the alphabet (see Tab. 1).

During the time of the Second World War, the most famous cryptographic machine was the Enigma machine. The impeller machine created by ArturScherbius was used by the German military to encrypt messages. It consisted of two typewriters combined together.

By rotating the impeller, the letter was changed to another letter, it was important that the public letter could not be a secret letter at the same time. The advantage of Scherbius machine was the ability to decode messages at the same time.

Launching of computerization has contributed to significant modernization of the encryption process. It has become much faster and it could contain many more characters resulting in more complex algorithms. These algorithms have so far contained only letters, but using computers in the encryption process, they became possible to use numbers in binary system.

Tab. 1. Caesar's cipher

A → D	H → K	N → R	U → X
B → F	I → L	O → S	V → Y
C → G	J → M	P → T	W → Z
D → H	K → N	R → U	X → A
F → I	L → O	S → V	Y → B
G → J	M → P	T → W	Z → C

2. Introduction to cryptographic

One of the first cryptographic systems is DES (the name comes from the word Demonstration). A block cipher with length of data blocks already set did not use single bits (or bytes), but entire blocks of data. The most popular key was the 128-bit key, which was characterized by above-average resistance to full review method attacks. However, it was limited to 56 bits, what led to reduction of the cipher security.

Another cryptographic system is RSA, which is based on asymmetric encryption algorithm. The assumptions of this system are based on the distribution of large numbers to the first factor and the secure exchange of encryption keys. This article will demonstrate the encryption process of the RSA crypto-system. In the early stages of using this system, the simplest algorithm could be calculated with the aid of a pocket calculator. Now, with the passage of time, security ciphers are based on ever-increasing keys, which make breaking them very difficult. The digital tachograph system is based on the RSA crypto-system. The need to go through the European level, the level of the Member State, or the level of the equipment increases the workload required to break the cipher and change the algorithm.

The RSA cipher uses a private key and a public key. The second one is given as a message, but its true meaning is public only when we use the private key for decryption. The data from the private code is passed on only to specific people who are supposed to decrypt the text of the forwarded message.

In the mathematical terms, encryption system is called the finite and non-empty set of M relation, which we define by the equation (1) [1]:

$$M = \{X_0, X_1, X, ..., X_{\theta-1}\}, \tag{1}$$

where:
θ – number of all relations in M set.

A single relation describes the pattern (2), the use of which in each following relationship is the next step of encryption [1]:

$$X_i : V^{(ni)} \rightarrow W^{(mi)}. \tag{2}$$

By adopting a specific algorithm in RSA cryptosystems encryption of the message, we use modulo arithmetic and prime numbers qualities.

Suppose that a system user chooses two relatively large prime numbers p and q. For simplifying the example, we will use numbers 13 and 19. Then the user calculates the number n, which is the product of the two numbers ($n = 247$). Now we select the number e, which together with the product n will be the encryption key. The numbers e and $(p - 1) \times (q - 1)$ should be relatively prime. Suppose that $e = 5$. Both the number n and number e are made public to those who are interested in encrypting the message. To do this, the message has to be converted into number under the ASCII standard. Assume that passed character will be a letter. In ASCII standard, this letter equals 01000001 combination. After conversion to denary, it is 65, which means that the plaintext is $J = 65$. A person who possesses only public keys will not be able to reverse the operation of the de-scribed cryptographic function.

Value of the secret text is calculated according to formula (3) [1]:

$$S = J^e (mod n), \tag{3}$$

We now use the exponentiation properties:

$$a^{n+m} = a^n \times a^m, \tag{4}$$

And modulo arithmetic properties:

$$(a \times b) mod n = ((a\, mod n) \times (b\, mod n)) mod n, \tag{5}$$

So:

$$S = 65^5 (mod 247) = [65^2 (mod 247) \times 65^2 (mod 247) \times 65 (mod 247)]\, mod 247,$$

where:

$$mod 247 - (26 \times 26 \times 65)\, mod 247 = [1690 (mod 247) \times 26 (mod 247)]\, mod 247 = 208 \times 26 (mod 247) = 221.$$

Our encrypted message has a form of $S = 221$.

The multifaceted nature of the road transport has forced the authorities responsible for carrying out checks to bring out a digital device that will record data using tachograph cards. It was necessary to use complex keys and certificates to prevent the abuse that often occurred during the recording data on traditional record devices (using an analogue tachograph). These encodings are used for both tachograph cards as well as digital tachograph devices (STCs). In order to enable cooperation between them, the digital tachograph system uses the same key system in particular country for effective collaboration. This cooperation is based on specific links such as drivers, transport companies, authorities conducting checks and digital recording equipment manufacturers.

Each member state of the European Union is required to create appropriate structures within its territory to manage the digital tachograph system. However, there are general requirements that each country can implement in its territory in a manner that suits it best. The proper structure for managing the digital tachograph system should include [3]:

- accepting applications and issuing tachograph cards to individual users,
- accepting applications and issuing certificates to digital recording devices manufacturers,
- creating a user database,
- exchange of information between Member States to monitor abidance of regulations,
- authorization and supervision of a network of installation and verification workshops.

Irregularities and errors that can be encountered during the operation of digital recording equipment may block the correct issuance of tachograph cards, including workshop cards. The workshop card is important because it is possible to carry out the activation and calibration procedure of the digital recording equipment with its use. In Poland, the responsibility for issuing these cards has Polish Securities Works Authority S.A. The digital tachograph is supervised by the minister responsible for transport.

Data read from digital recording equipment must include all information showing driver's behaviour and vehicle exploitation. These data must be reliable as they are the basis for the inspection performed by authorized services. The most important is the security, or counteracting malicious at the same time adverse impacts on system by interfering in the communication mechanisms between its elements. The consequence of such an attack may be undesirable modification of the content of the data stream between the motion sensor and the tachograph, in order to falsify information about the vehicle speed and distance. Basic security mechanism used in the system of digital tachographs is encryption. Encryption scheme of data exchange between the card, the tachograph and motion sensor is presented in Fig. 1 [6].

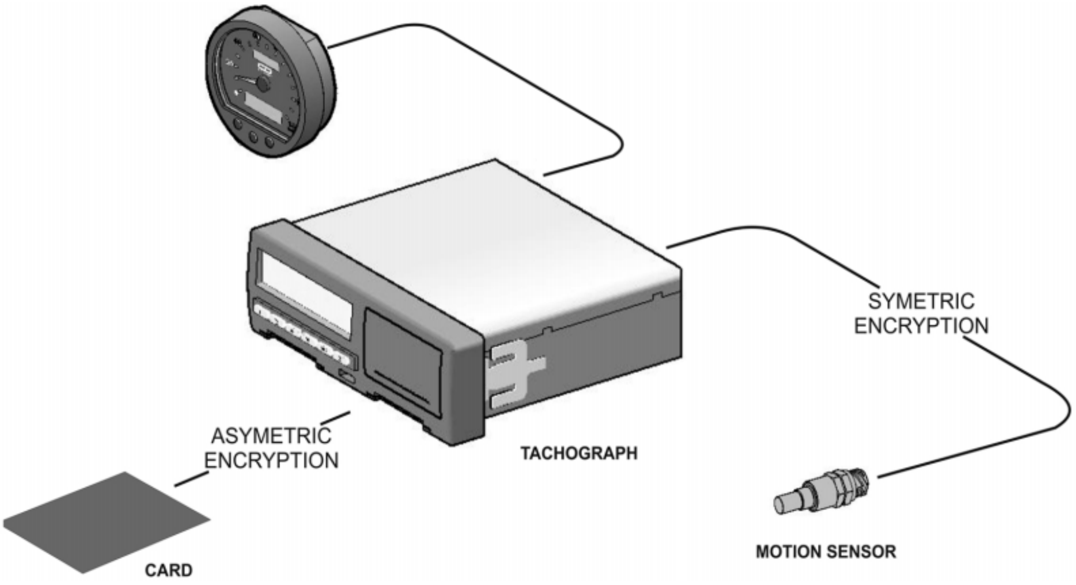

Fig. 1. The scheme of a tachograph encrypted data exchange [6]

3. Digital Tachograph System

One of the elements securing the digital recording equipment is the electronics and IT protection consisted of [4]:

- certificates and keys system,
- tachograph card identifier that allows unambiguous identification of the user,
- security system, equipped in digital signature mechanism with Hash algorithm that protects the data red from the tachograph card,
- a classic RSA algorithm that generates private and public keys,
- symmetric keys, produced by the TDES algorithm, used to protect the initialization process and vaporization of sensor with the on-board unit.

Any message between the on-board unit and the motion sensor is transmitted via the cipher.

The motion sensor is used in vehicles used in road transport. The motion sensor is a part of the recording equipment providing a signal representing the vehicle's speed and/or made distance [2]. The basic function of this sensor is to record the speed of the vehicle and the distance travelled by it as well as transmission of this information to the recording device (VU). The motion sensor is mounted on the vehicle in places where these parameters can be recorded. These may be wheels, gearbox, or other vehicle parts, specified by the manufacturer. A typical motion sensor diagram is shown in Fig. 2.

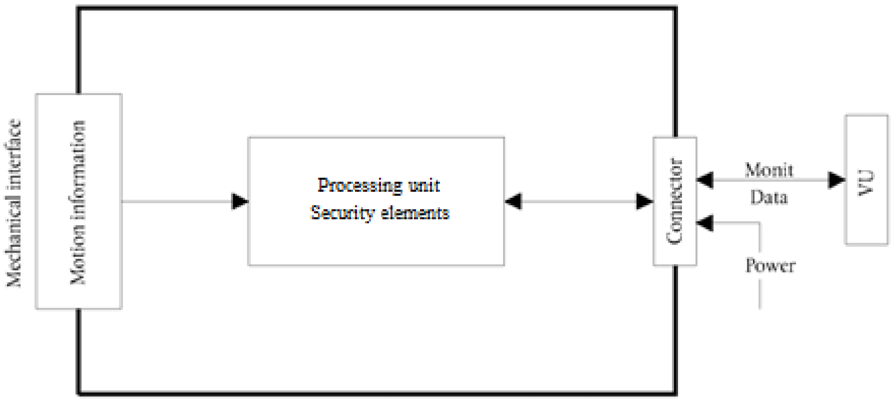

Fig. 2. Typical motion sensor [2]

Among the risks on which a motion sensor may be exposed can be distinguished [2]:

- trying to access the features,
- trying to change the recorded and saved data using the sensor,
- structural faults,
- environmental attacks such as for example: thermal, electromagnetic, chemical, mechanical attacks,
- use of non-invalidated testing modes,
- modification of sensor hardware and software,
- manipulation with sensor's input for movement, e.g. by unscrewing the sensor from the gearbox,
- power supply manipulation.

Exceeding the maximum average speed over the limit value may be the use of additional devices designed to terminate the vehicle speed limiter. It is worth remembering that if the tachograph records are suspected of deliberate action during the inspection, the vehicle can be returned to the nearest workshop for accurate vehicle verification.

Breaking these protections may result in incorrect results of tested parameters checked by the appropriate authorities. The recording equipment collects data on drivers' working hours, distance travelled and vehicle speed, which can be used to provide information on driving styles and respect for eco-driving principles. Recording equipment is also used to display, print and output driver's activity data [2]. The typical life cycle of the recording device is shown in Fig. 3.

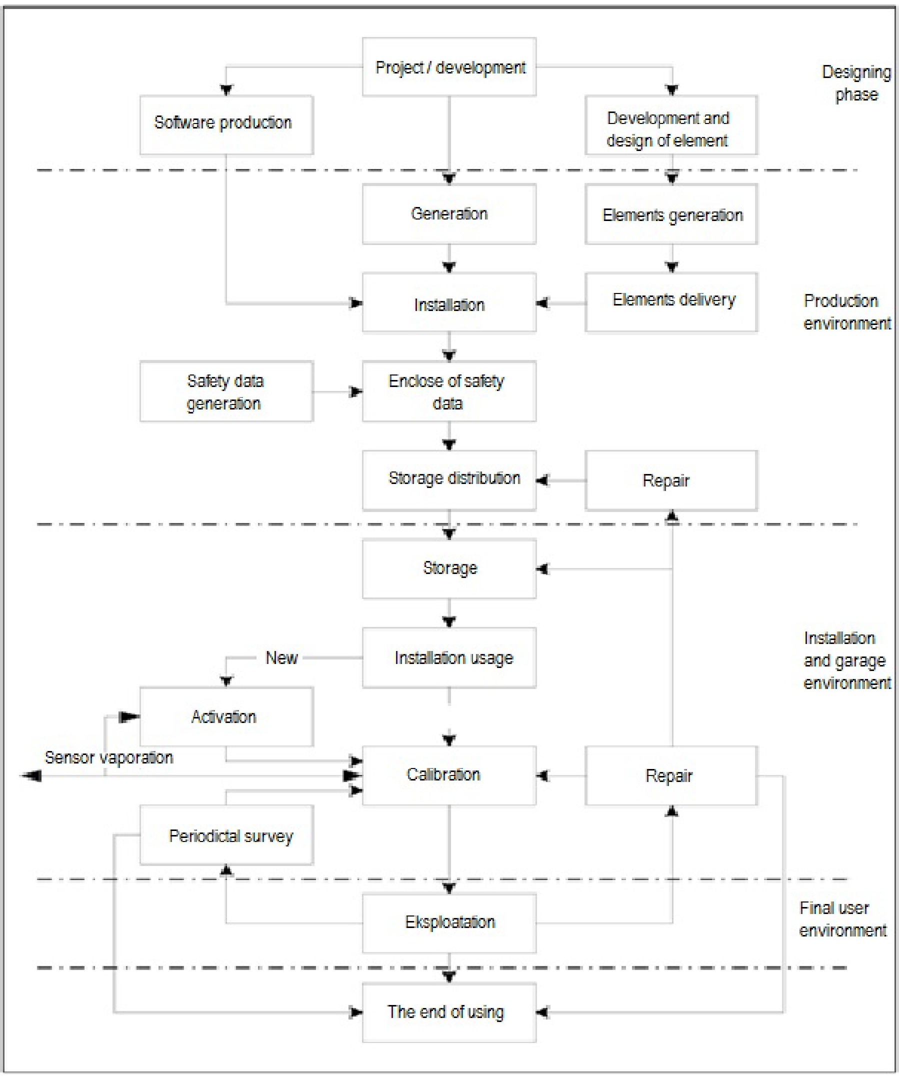

Fig. 3. Typical recording device life cycle [2]

Among the most important elements of the construction of the digital recording device are the following:

- tachograph card readers,
- display,
- diode signalizing alarm,
- printer,
- function and navigation keys,
- calibration and diagnostic connector.

Operation of the digital recording device facilitates 4 modes of operation: exploitative, control, calibration and company. The appropriate mode of operation is turned on after the inserting tachograph card corresponding to specific mode into the card reader.

Tachograph cards integrate participants using the digital tachograph system. They are used in identification of the cardholder and to record information about work conditions and parameters of the driver and car's drive. As with the modes of operation of the recording device, there are four types of tachograph cards:

- the driver's card – white colour, is personalized, i.e. refers to only one person. Its validity is no longer than 5 years or until the end of the validity period of the cardholder's driving license. It records the course of the driver's work in the last 28 days,
- enterprise's card – yellow colour, is issued to the specific company. The validity period of the card is 5 years. The card can be used by many people authorized by this company. It allows printing data recorded in the last 28 days,
- control card – blue colour. Issued to a specific authority authorized to carry out inspections and it may be also issued to a specific person (controller, inspector). It is issued for a period of 5 years. Use of it is possible only in the territory of Poland,
- workshop card – red colour. The holder is a person who has the power to perform checks of digital recording devices and is employed in the company which has been authorized to install, activate, calibrate, technical control and repair in compliance with the requirements of Commission Regulation (EC) No 1360/2002 of 13 June 2002, adapting for the seventh time to technical progress Council Regulation (EEC) No 3821/85 on recording equipment in road transport, Urz. EU L No. 207 of 5.8.2002, p.1. Its memory allows storing the cryptographic keys needed during evaporation of the motion sensor with on-board unit, as well as the identification number (PIN) in which it has been equipped as a security element [4]. It is issued for 12 months.

We will lead further considerations on the base of workshop card (Fig. 4).

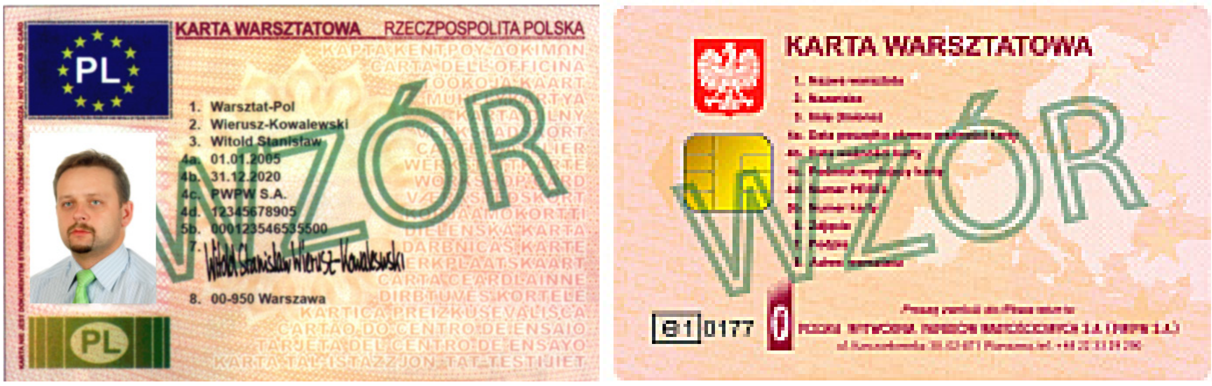

Fig. 4. Model of workshop card valid in the territory of the Republic of Poland (obverse and reverse card)

In Poland, the responsibility for issuing workshop cards has Polish Securities Works Authority S.A. The digital tachograph is supervised by the minister responsible for transport. The Polish Securities Office S.A. issues tachograph cards identical to those issued in the European Union.

Thanks to the unification of issued tachograph cards, participants of the European Union member states can easily move between countries. Each card has its own identification of the card, which means a specific set of data about the type of card, the RMS code of the issuing Member State, the sequence number of the card and the number in case of replacing and refreshing the card.

In order to prevent falsification of cards, the following safeguards have been implemented:

- an appropriate background design,
- the background pattern and identifying photo overlap in the area of the security photo,
- a line made by micro-printing in at least two colours,
- possible identification marks and state symbols.

Thanks to the introduced security, the authenticity of the card is credible. This protection also allows the recording of data concerning the work of a professional driver, and thus the prevention of manipulation of data stored in tachograph cards. Data from tachograph cards can be read using other devices, for example computers.

The Act introducing the digital tachograph system in Poland, including the introduction of tachograph cards as security, also introduced digital certificates and electronic signatures. The electronic signature unambiguously facilitates the daily functioning of transport companies and units cooperating with them. It confirms the authenticity of the document, verification of the signatory and prohibits making changes to the documents already signed. The world's digital signature was created in 1978 thanks to the introduction of a cryptographic public key system. Asymmetric cryptographic algorithms allowed for the submission of a digital signature and its verification. However, it was only in 1999 that the European Parliament and the Council adopted a legal framework allowing the electronic signature to be recognized as an equivalent handwritten signature. In Poland, the resolution on the signature was taken in 2001. An electronic signature is made using a private key and checked using a public key. Thanks to this, only one particular person can sign, but many people who do not own the signature can read it.

To use an electronic signature, you must obtain the appropriate certificate that uses the private key. We can obtain the certificate on one of many websites where we make a purchase. Next, a message containing the activation code and a link to the page where it should be entered is sent to the e-mail address indicated by us. Verification takes place, during which we enter the password protecting the key. If the password is sent to outsiders, the owner of the electronic signature loses credibility and its signature ceases to be authentic.

4. Summary

The way information is encrypted has been known since the time of Caesar. However, the ciphers used, however, bring a lot of trouble in decoding them. The system of repetitive codes is complicated but can be deciphered for outstanding minds.Encryption of transport information plays a very important role. This information provides us with information about the style and profile of the truck driver. Building a digital recorder is complicated, although at first glance it would seem that this is not the case. Motion sensors that are increasingly interfered with are important. The increase in violations is noticeable in the interruption of the registration of selected data. Among them is the speed by which we measure the speed of the vehicle. With these two parameters, we are able to give an indicative fuel consumption of the vehicle.

References

[1] Karbowski, M., *Podstawy kryptografii*, pp. 50, 63-64, Helion, Gliwice 2015.

[2] Rozporządzenie Komisji (WE) nr 1360/2002, z dnia 13 czerwca 2002 r., dostosowujące po raz siódmy do postępu technicznego Rozporządzenie Rady (EWG) nr 3821/85 w sprawie urządzeń rejestrujących stosowanych w transporcie drogowym, pp. 287-288, 483-485, 492, 494, 2002.

[3] Rozporządzenie Rady (WE) Nr 2135/98 z dnia 24 września 1998 r. zmieniające rozporządzenie (EWG) Nr 3821/85 w sprawie urządzeń rejestrujących stosowanych w transporcie drogowym oraz dyrektywę 88/599/EWG dotyczącą stosowania rozporządzeń (EWG) nr 3820/85 i (EWG) Nr 3821/85.

[4] Rychter, M., *Budowa i zastosowanie system tachografii cyfrowej*, Wydawnictwo Instytutu Transportu Samochodowego, pp. 21, 175-177, 197, 247-249, Warszawa 2011.

[5] Rychter, M., *Forming recommendations of digital recording devices*, Journal of Polish CIMAC, Vol. 7, No. 2, Diagnosis, Reliability and Safety, pp. 187, Gdansk 2012.

[6] Śmieja, M., Rychter, M., Sułek, P., *Data exchange in a tachograph system as the element of the cybersecurity of the modern car*, Journal of KONES Powertrain and Transport, Vol. 23, No. 4, pp. 536-537, Jastrzębia Góra 2016.

Manuscript received 26 Febryary 2019; approved for printing 27 June 2019