SECTION 2. Applied mathematics. Mathematical modeling.

Alexandr N. Shevtsov
candidate of Technical Sciences,
President, Theoretical & Applied Science, LLP
associate Professor of the Department «Applied mathematics»,
Taraz State University named after M.H. Dulati, Kazakhstan

Yunona R. Krakhmaleva
candidate of Technical Sciences,
associate Professor of the Department «Applied mathematics»,
Taraz State University named after M.H. Dulati, Kazakhstan

SOME REGULARITIES OF DISTRIBUTIONS $\tilde{T}_k$.

The purpose of the article is to identify and build some distributions based on Prime numbers.

Keywords: prime numbers, pattern, distribution.

Many methods of coding and encryption based on the use of primes, and in particular them multiply. This is based cipher El-Gamal (DSA, ECDSA), cipher Rivest-Shamir-Aldeman (RSA), and stream encryption (A3, A5, A8, MUGI, PIKE, RC4, SEAL), cipher El-Gamal (ECDSA) one of the most advanced and modern directions of development of cryptosystems, analyzed many of the leading mathematicians [1-6]. The complexity of hacking these algorithms is precisely the work of Prime numbers, selection, search expansions and others. In this work received and considered separate laws, capable to improve algorithms of coding.

Consider the number of primes from 1 to 10,000. Let us denote it as follows:

$$N_j = 1, 2, 3, 5, 7, 11, \ \dots \ , 9941, 9949, 9967, 9973.$$

Deuce included in the series - not to violate the integrity of reasoning.

Build a new number $\tilde{N}_i$ of elements N_j according to the following algorithm

$$\tilde{N}_i = N_{j+1} - N_j, \ j = \overline{1, 1230}.$$

Table 1

Elements of a number of $\tilde{N}_i$, $i = \overline{1, 1229}$

1	1	2	2	4	2	4	2	4	6	2	6	4	2	4	6	6	2	6	4		
2	6	4	6	8	4	2	4	2	4	14	4	6	2	10	2	6	6	4	6		
6	2	10	2	4	2	12	12	4	2	4	6	2	10	6	6	6	2	6	4		

2 10 14 4 2 4 14 6 10 2 4 6 8 6 6 4 6 8 4 8
10 2 10 2 6 4 6 8 4 2 4 12 8 4 8 4 6 12 2 18
6 10 6 6 2 6 10 6 6 2 6 6 4 2 12 10 2 4 6 6
2 12 4 6 8 10 8 10 8 6 6 4 8 6 4 8 4 14 10 12
2 10 2 4 2 10 14 4 2 4 14 4 2 4 20 4 8 10 8 4
6 6 14 4 6 6 8 6 12 4 6 2 10 2 6 10 2 10 2 6
18 4 2 4 6 6 8 6 6 22 2 10 8 10 6 6 8 12 4 6
6 2 6 12 10 18 2 4 6 2 6 4 2 4 12 2 6 34 6 6
8 18 10 14 4 2 4 6 8 4 2 6 12 10 2 4 2 4 6 12
12 8 12 6 4 6 8 4 8 4 14 4 6 2 4 6 2 6 10 20
6 4 2 24 4 2 10 12 2 10 8 6 6 6 18 6 4 2 12 10
12 8 16 14 6 4 2 4 2 10 12 6 6 18 2 16 2 22 6 8
6 4 2 4 8 6 10 2 10 14 10 6 12 2 4 2 10 12 2 16
2 6 4 2 10 8 18 24 4 6 8 16 2 4 8 16 2 4 8 6
6 4 12 2 22 6 2 6 4 6 14 6 4 2 6 4 6 12 6 6
14 4 6 12 8 6 4 26 18 10 8 4 6 2 6 22 12 2 16 8
4 12 14 10 2 4 8 6 6 4 2 4 6 8 4 2 6 10 2 10
8 4 14 10 12 2 6 4 2 16 14 4 6 8 6 4 18 8 10 6
6 8 10 12 14 4 6 6 2 28 2 10 8 4 14 4 8 12 6 12
4 6 20 10 2 16 26 4 2 12 6 4 12 6 8 4 8 22 2 4
2 12 28 2 6 6 6 4 6 2 12 4 12 2 10 2 16 2 16 6
20 16 8 4 2 4 2 22 8 12 6 10 2 4 6 2 6 10 2 12
10 2 10 14 6 4 6 8 6 6 16 12 2 4 14 6 4 8 10 8
6 6 22 6 2 10 14 4 6 18 2 10 14 4 2 10 14 4 8 18
4 6 2 4 6 2 12 4 20 22 12 2 4 6 6 2 6 22 2 6
16 6 12 2 6 12 16 2 4 6 14 4 2 18 24 10 6 2 10 2
10 2 10 6 2 10 2 10 6 8 30 10 2 10 8 6 10 18 6 12
12 2 18 6 4 6 6 18 2 10 14 6 4 2 4 24 2 12 6 16
8 6 6 18 16 2 4 6 2 6 6 10 6 12 12 18 2 6 4 18
8 24 4 2 4 6 2 12 4 14 30 10 6 12 14 6 10 12 2 4
6 8 6 10 2 4 14 6 6 4 6 2 10 2 16 12 8 18 4 6
12 2 6 6 6 28 6 14 4 8 10 8 12 18 4 2 4 24 12 6
2 16 6 6 14 10 14 4 30 6 6 6 8 6 4 2 12 6 4 2
6 22 6 2 4 18 2 4 12 2 6 4 26 6 6 4 8 10 32 16
2 6 4 2 4 2 10 14 6 4 8 10 6 20 4 2 6 30 4 8
10 6 6 8 6 12 4 6 2 6 4 6 2 10 2 16 6 20 4 12
14 28 6 20 4 18 8 6 4 6 14 6 6 10 2 10 12 8 10 2
10 8 12 10 24 2 4 8 6 4 8 18 10 6 6 2 6 10 12 2
10 6 6 6 8 6 10 6 2 6 6 6 10 8 24 6 22 2 18 4
8 10 30 8 18 4 2 10 6 2 6 4 18 8 12 18 16 6 2 12
6 10 2 10 2 6 10 14 4 24 2 16 2 10 2 10 20 4 2 4
8 16 6 6 2 12 16 8 4 6 30 2 10 2 6 4 6 6 8 6
4 12 6 8 12 4 14 12 10 24 6 12 6 2 22 8 18 10 6 14

4 2 6 10 8 6 4 6 30 14 10 2 12 10 2 16 2 18 24 18
6 16 18 6 2 18 4 6 2 10 8 10 6 6 8 4 6 2 10 2
12 4 6 6 2 12 4 14 18 4 6 20 4 8 6 4 8 4 14 6
4 14 12 4 2 30 4 24 6 6 12 12 14 6 4 2 4 18 6 12
8 6 4 12 2 12 30 16 2 6 22 14 6 10 12 6 2 4 8 10
6 6 24 14 6 4 8 12 18 10 2 10 2 4 6 20 6 4 14 4
2 4 14 6 12 24 10 6 8 10 2 30 4 6 2 12 4 14 6 34
12 8 6 10 2 4 20 10 8 16 2 10 14 4 2 12 6 16 6 8
4 8 4 6 8 6 6 12 6 4 6 6 8 18 4 20 4 12 2 10
6 2 10 12 2 4 20 6 30 6 4 8 10 12 6 2 28 2 6 4
2 16 12 2 6 10 8 24 12 6 18 6 4 14 6 4 12 8 6 12
4 6 12 6 12 2 16 20 4 2 10 18 8 4 14 4 2 6 22 6
14 6 6 10 6 2 10 2 4 2 22 2 4 6 6 12 6 14 10 12
6 8 4 36 14 12 6 4 6 2 12 6 12 16 2 10 8 22 2 12
6 4 6 18 2 12 6 4 12 8 6 12 4 6 12 6 2 12 12 4
14 6 16 6 2 10 8 18 6

Obtain the distribution of the number of separate elements of a number of values, Fig.1.

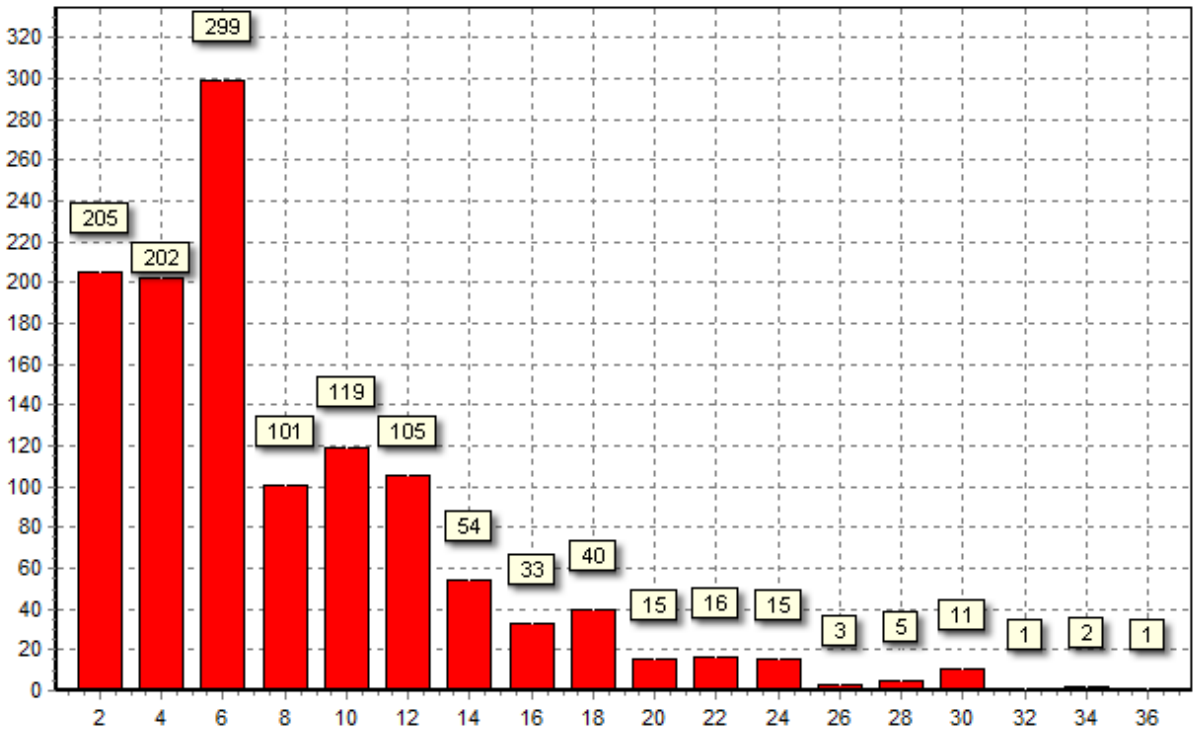

Figure 1 - Distribution of the number of individual elements of a number of values.

Get the periods between the indices of each element of a number of $\tilde{N}_i$, Tab.2. We introduce the designation of the obtained series via $\tilde{T}_k$. Try to find

patterns in data series, for we construct graphs of their distribution by value and by number, Fig.2- Fig.8.

Table 2

Periods of appearance of certain elements.

notation	$\tilde{N}_i$	**Periods**
$\tilde{T}_2$	**2**	1 2 2 3 3 4 3 6 2 5 2 6 2 2 4 3 5 3 4 5 12 2 6 9 6 5 4 3 4 20 2 2 4 4 19 2 3 2 4 8 11 5 3 3 3 10 5 4 2 17 3 6 3 3 9 9 2 6 2 6 5 6 2 3 2 3 9 4 7 3 7 20 4 7 6 5 3 7 3 20 2 14 4 10 2 3 6 4 2 2 7 2 6 3 3 3 11 12 6 4 8 3 6 4 3 5 4 5 5 2 2 3 2 6 9 7 5 3 9 3 8 7 3 12 6 7 2 8 14 5 15 4 4 3 3 11 3 2 10 13 4 2 20 5 6 10 4 9 9 9 3 9 4 2 6 2 2 4 6 7 2 20 8 10 3 2 8 4 9 2 5 20 11 9 4 8 14 2 8 10 4 10 6 4 24 3 3 11 2 3 3 22 4 7 9 2 2 2 18 5 4 6 12 8
$\tilde{T}_4$	**4**	2 2 4 2 5 3 3 2 2 2 7 6 4 2 9 4 2 5 5 3 7 3 2 3 2 17 5 5 9 3 2 7 4 2 2 2 2 4 4 6 12 2 15 9 4 2 11 2 3 6 2 7 3 2 2 3 7 3 12 9 2 14 2 11 8 6 5 4 4 7 4 3 6 5 5 9 5 4 2 3 7 6 4 4 10 8 2 5 7 4 4 4 8 4 12 2 8 12 8 3 11 6 4 3 3 4 5 16 3 33 8 2 12 12 4 2 4 11 6 4 9 10 6 2 11 7 4 6 3 4 4 7 2 5 5 4 8 4 8 6 4 18 3 30 6 6 17 9 2 9 7 5 5 15 6 20 9 6 5 3 3 3 2 3 3 3 8 2 6 15 8 8 4 2 2 11 4 9 8 7 2 7 5 2 9 5 9 13 3 5 8 5 2 13 4 10 5 14 6 5 7
$\tilde{T}_6$	**6**	2 4 1 2 3 2 9 4 1 2 1 11 3 1 1 2 9 4 2 1 2 8 2 10 4 2 1 2 2 1 2 1 7 1 4 6 1 3 27 1 3 1 2 3 4 5 5 1 2 1 6 1 4 1 2 6 2 6 2 1 8 4 7 5 2 7 3 2 3 11 1 1 2 9 7 1 6 2 5 6 10 8 10 1 5 2 2 2 3 2 2 1 3 3 7 2 13 1 4 4 10 6 2 5 1 6 1 11 3 9 3 11 1 1 2 11 11 4 2 8 2 2 1 6 5 1 2 5 13 3 9 1 2 3 2 3 5 7 7 5 7 3 5 2 1 5 7 3 1 5 2 1 2 5 8 7 3 5 2 5 1 2 9 3 1 1 2 13 3 1 6 1 1 2 4 3 2 8 3 1 7 7 4 4 5 1 2 3 2 2 5 6 5 2 2 1 16 5 1 2 5 1 1 2 2 2 1 1 4 13 2 7 3 5 17 1 6 5 2 1 2 3 8 2 6 4 3 2 13 3 4 5 1 3 6 1 7 4 5 9 1 4 5 3 8 3 3 5 1 3 10 2 7 4 6 5 4 14 2 5 2 1 2 2 1 9 7 2 5 4 6 5 2 3 4 3 2 14 2 2 1 2 9 1 2 4 6 2 3 9 2 4 4 3 2 6 2 5
$\tilde{T}_8$	**8**	48 5 2 8 5 2 30 2 2 4 3 21 2 8 20 6 4 24 8 13 5 2 22 11 18 5 21 5 4 4 26 6 9 7 7 7 13 4 4 11 4 18 2 26 6 19 10 2 19 51 5 26 20 21 15 13 2 21 24 14 9 4 23 11 4 6 3 14 9 7 3 10 27 7 11 5 12 9 26 4 19 3 24 18 8 22 13 7 11 2 3 8 19 15 11 15 29 15

		13 17
$\tilde{T}_{10}$	**10**	8 11 8 7 12 2 19 5 9 10 2 11 3 4 12 15 3 2 14 2 11 18 11 25 8 3 10 10 17 2 2 6 8 45 14 14 2 4 15 4 9 12 31 17 6 3 2 16 7 6 4 40 3 2 2 3 2 4 2 3 13 22 20 5 7 9 18 15 32 9 5 9 13 20 2 3 2 3 9 5 3 6 6 9 6 14 2 3 7 2 17 16 9 6 7 3 16 2 7 55 6 10 2 15 3 14 4 4 28 3 10 13 25 13 3 12 17 30
$\tilde{T}_{12}$	**12**	1 44 6 17 7 18 29 29 6 11 18 7 1 2 25 11 2 10 22 5 25 15 6 13 5 23 19 14 2 10 3 9 9 2 17 10 12 35 4 12 3 34 1 17 16 1 13 6 4 18 5 12 6 18 12 37 14 17 6 16 36 5 26 16 3 3 4 21 28 5 17 8 1 8 4 2 9 13 17 11 5 15 12 10 6 10 9 6 8 3 3 2 31 4 6 5 2 7 6 3 3 3 3 1
$\tilde{T}_{14}$	**14**	32 4 71 9 4 12 61 27 33 26 41 10 22 20 8 14 10 69 11 12 6 4 34 40 39 5 12 21 17 2 41 33 10 77 39 13 10 38 11 3 11 19 12 15 4 15 15 61 21 6 17 7 36
$\tilde{T}_{16}$	**16**	13 24 12 4 43 31 36 31 2 3 29 50 6 53 5 50 27 38 36 81 15 10 5 49 6 66 62 8 44 25 47 29
$\tilde{T}_{18}$	**18**	81 25 16 53 19 33 42 48 113 10 34 24 5 5 16 12 4 38 16 32 60 26 27 6 8 3 61 21 2 3 3 23 29 31 65 37 21 52 24
$\tilde{T}_{20}$	**20**	105 183 38 68 205 24 6 93 95 64 31 29 11 41
$\tilde{T}_{22}$	**22**	108 47 31 82 30 35 27 8 164 115 78 96 148 12 27
$\tilde{T}_{24}$	**24**	64 247 41 26 56 107 30 35 40 29 49 35 23 82
$\tilde{T}_{26}$	**26**	79 286
$\tilde{T}_{28}$	**28**	33 223 96 335
$\tilde{T}_{30}$	**30**	60 58 49 85 48 38 57 21 45 57
$\tilde{T}_{32}$	**32**	-
$\tilde{T}_{34}$	**34**	842
$\tilde{T}_{36}$	**36**	-

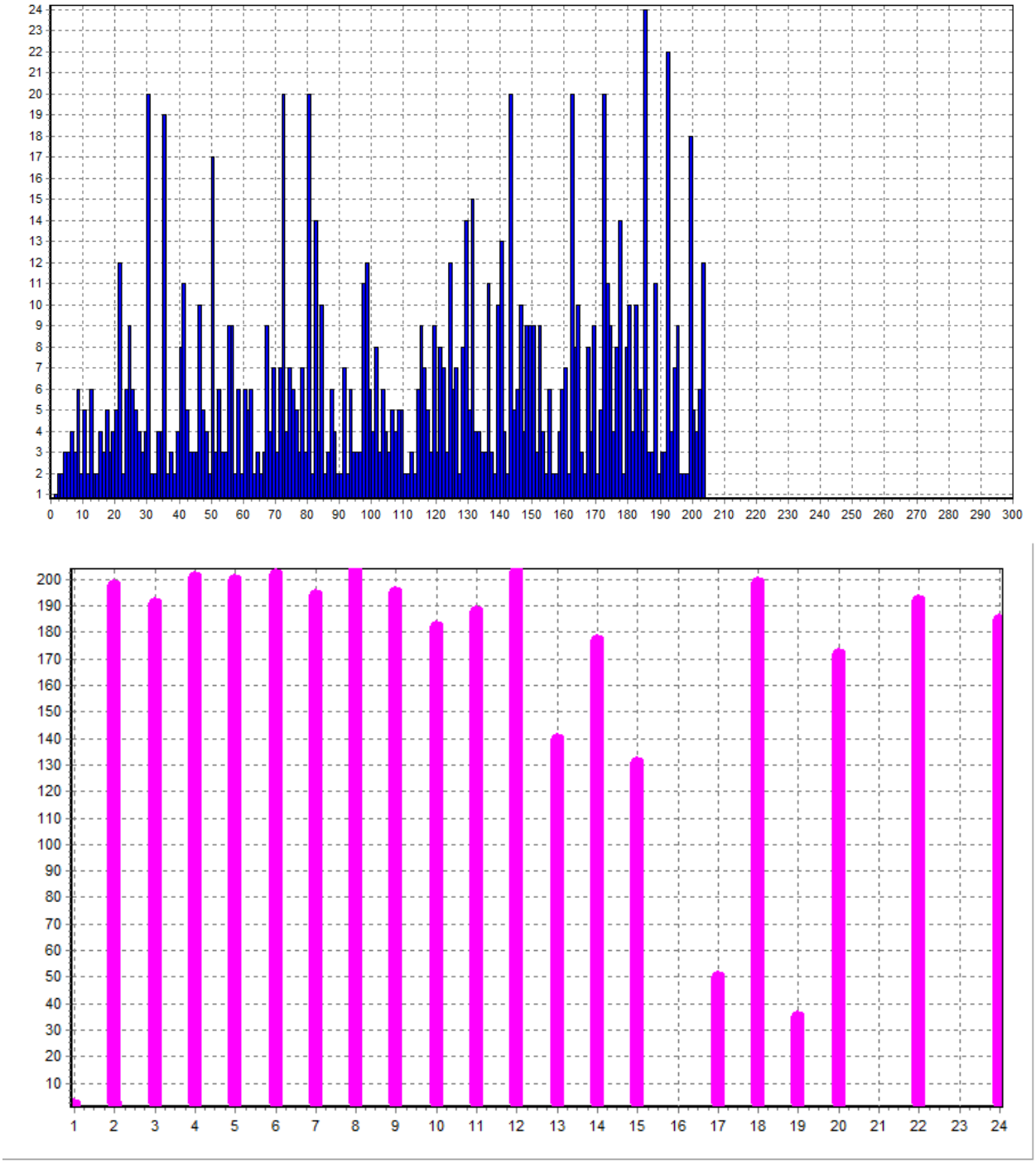

Figure 2 - Distribution of $\tilde{T}_2$.

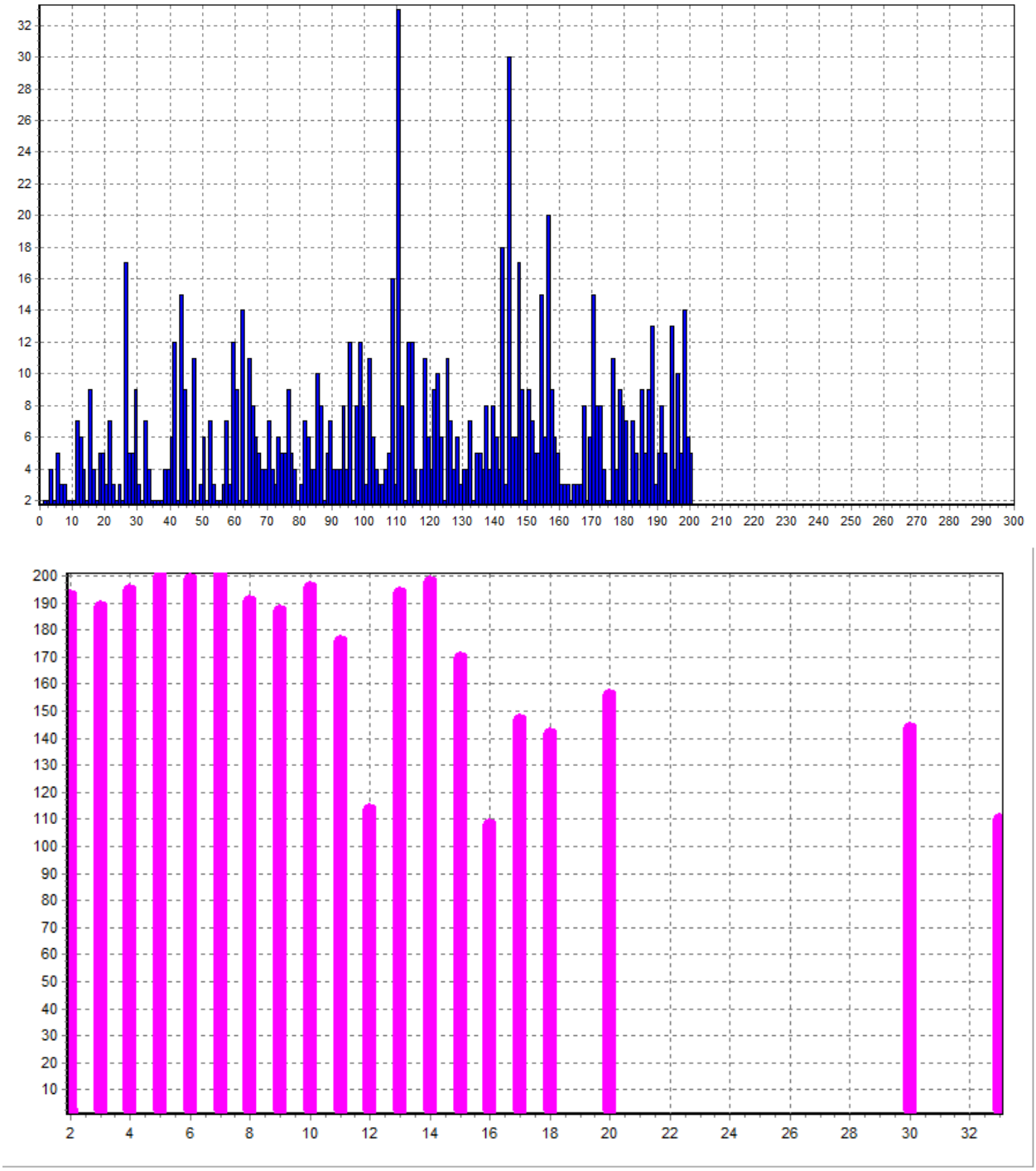

Figure 3 - Distribution of $\widetilde{T}_4$.

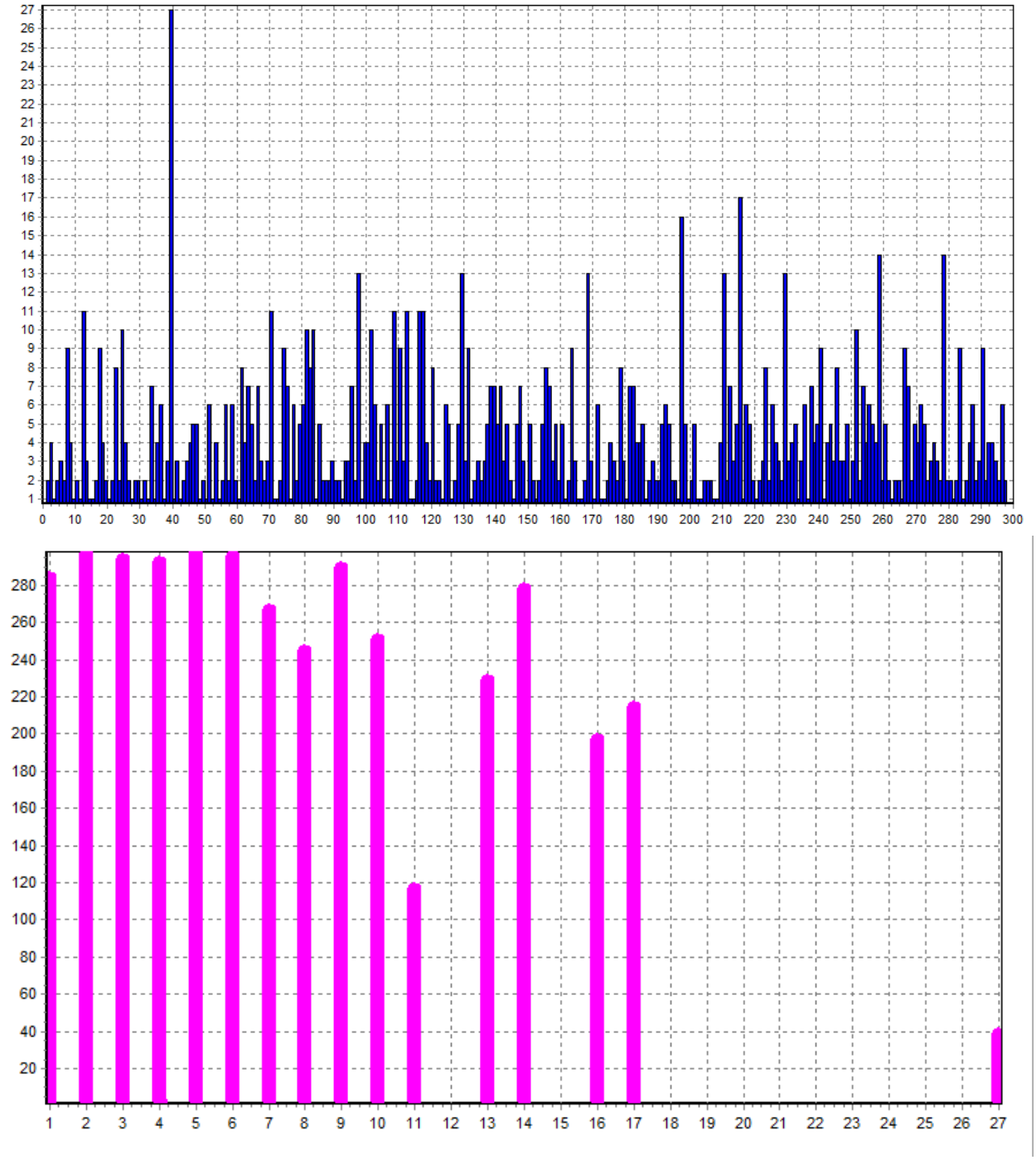

Figure 4 - Distribution of $\tilde{T}_6$.

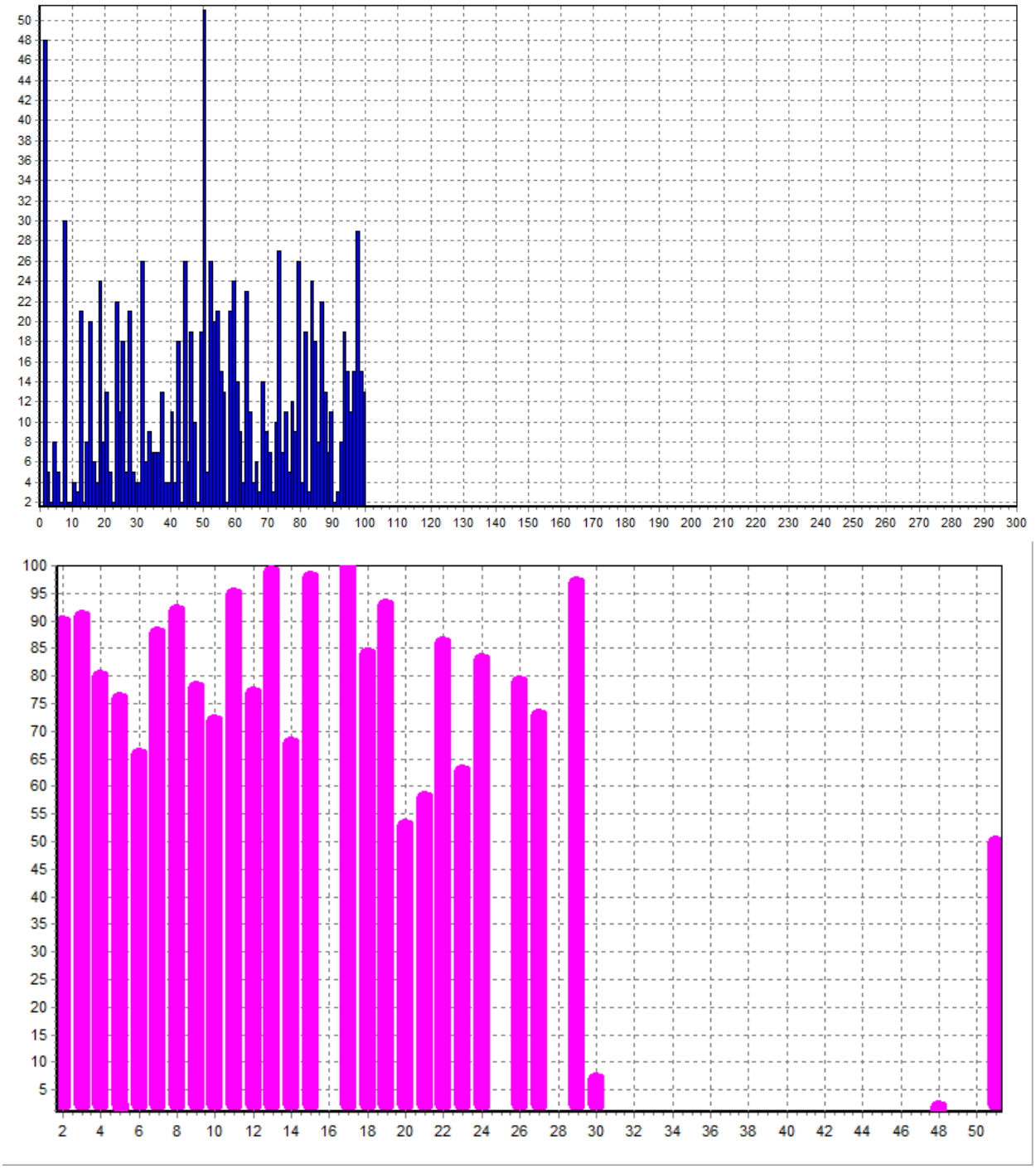

Figure 5 - Distribution of $\tilde{T}_8$.

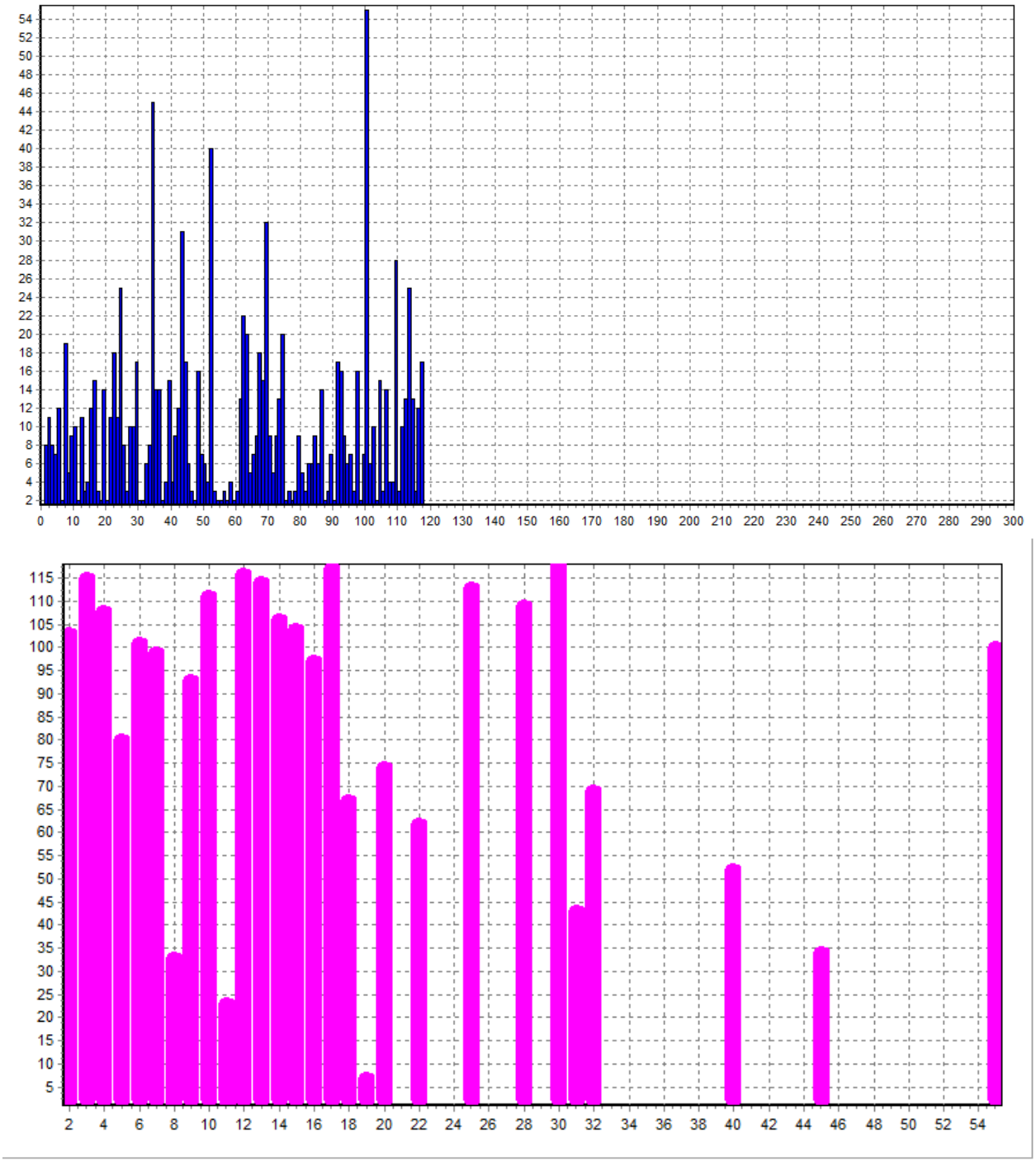

Figure 6 - Distribution of $\widetilde{T}_{10}$.

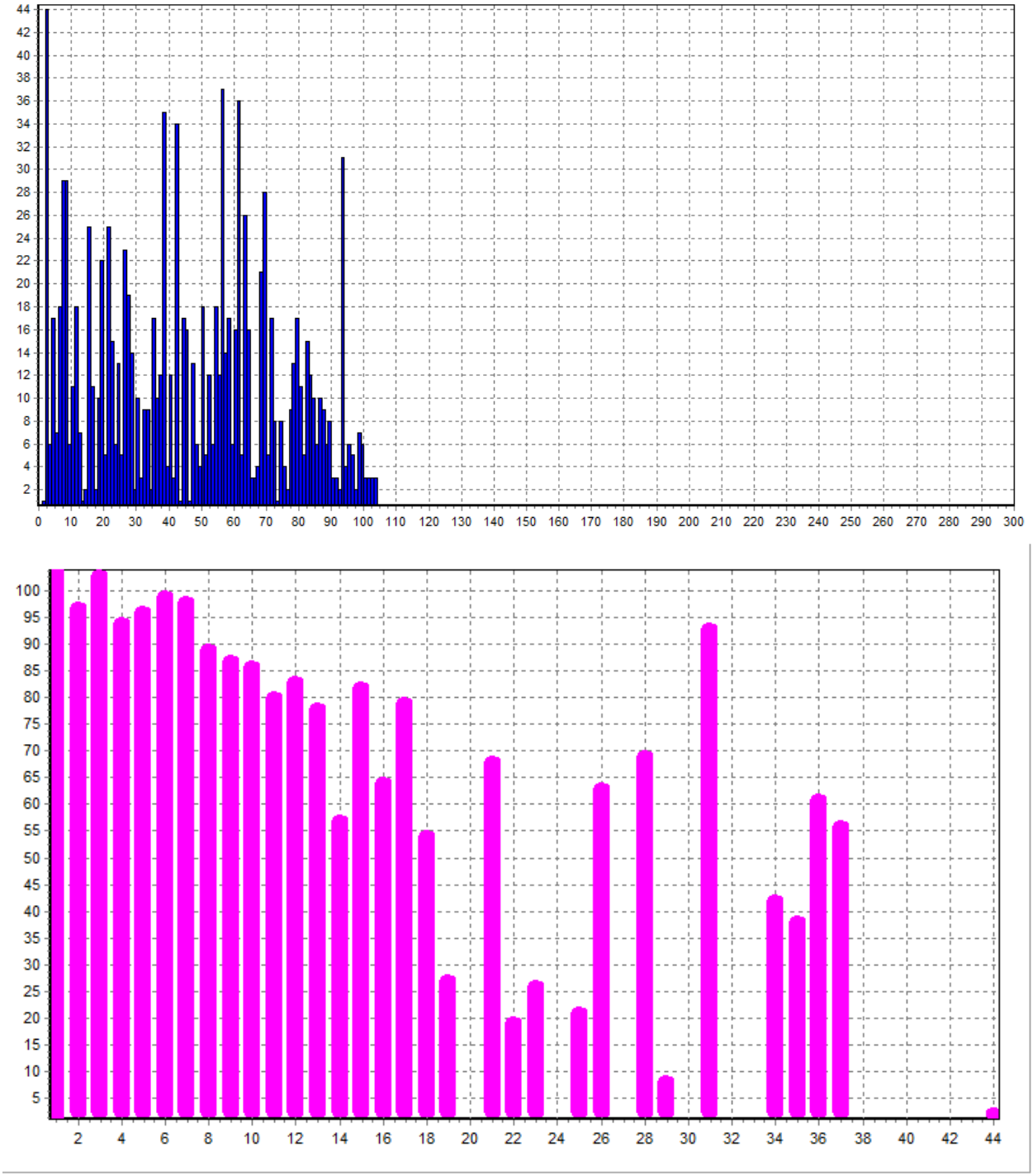

Figure 7 - Distribution of $\tilde{T}_{12}$.

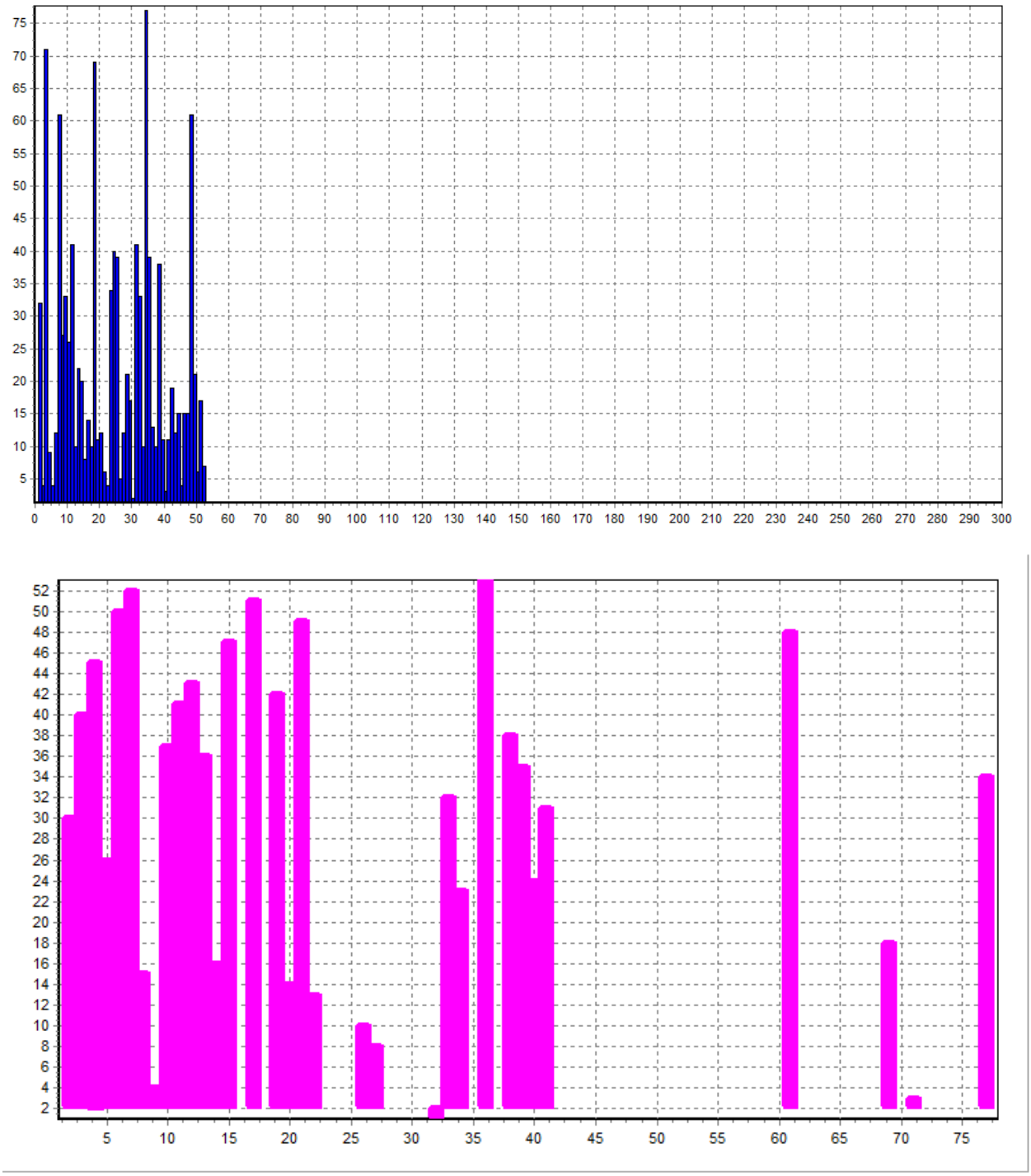

Figure 8 - Distribution of $\widetilde{T}_{14}$.

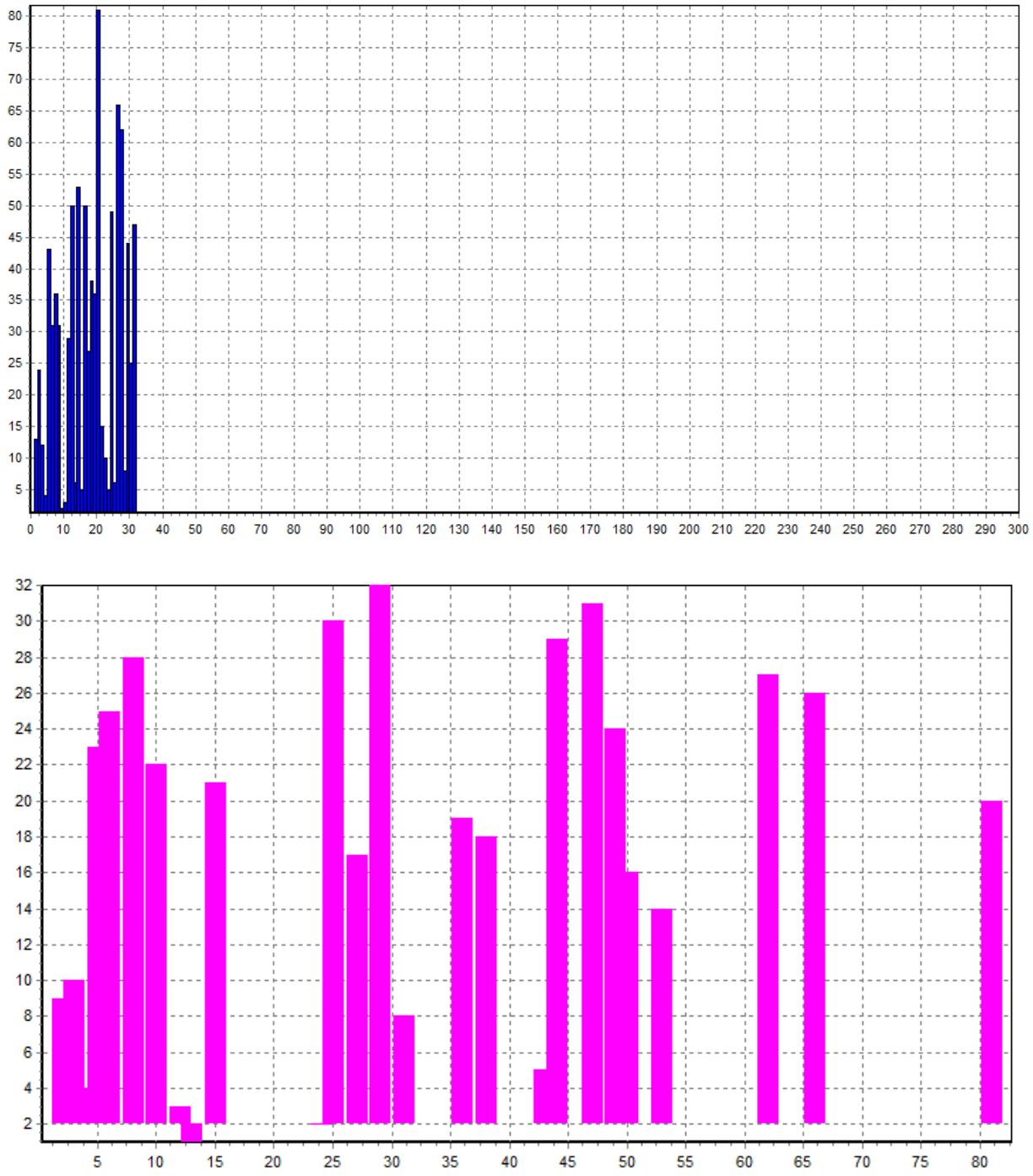

Figure 9 - Distribution of $\tilde{T}_{16}$.

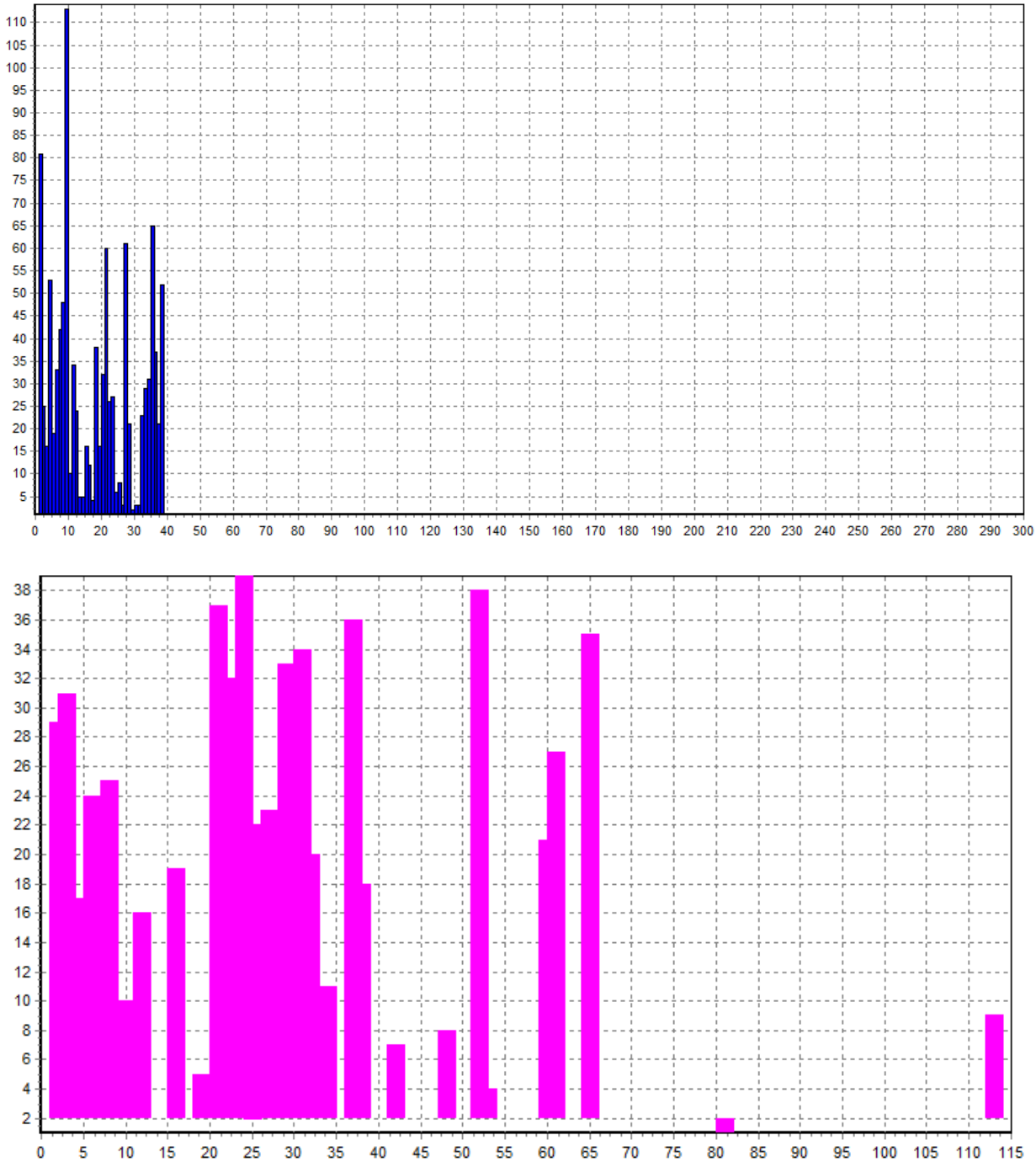

Figure 10 - Distribution of $\widetilde{T}_{18}$.

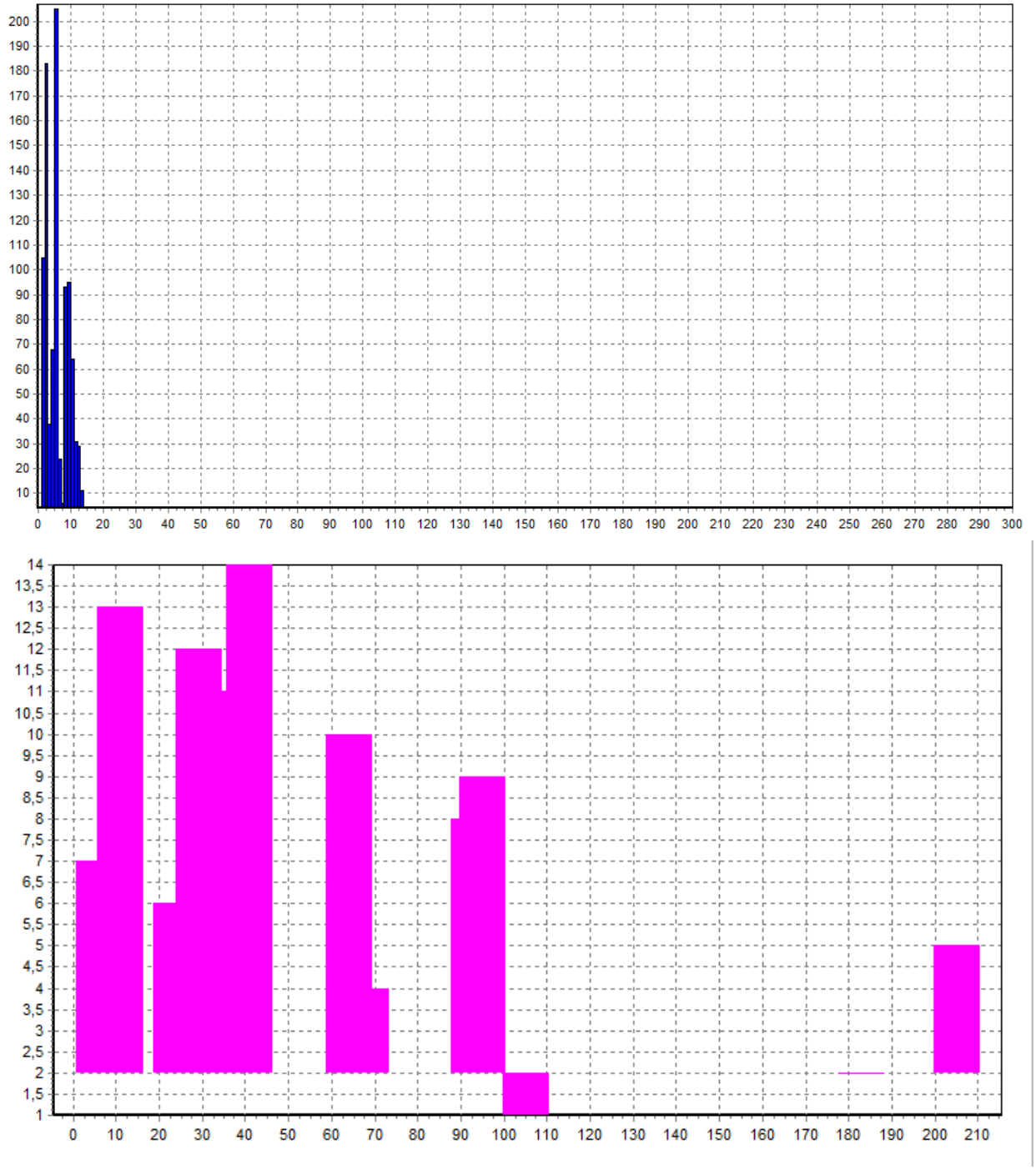

Figure 11 - Distribution of $\tilde{T}_{20}$.

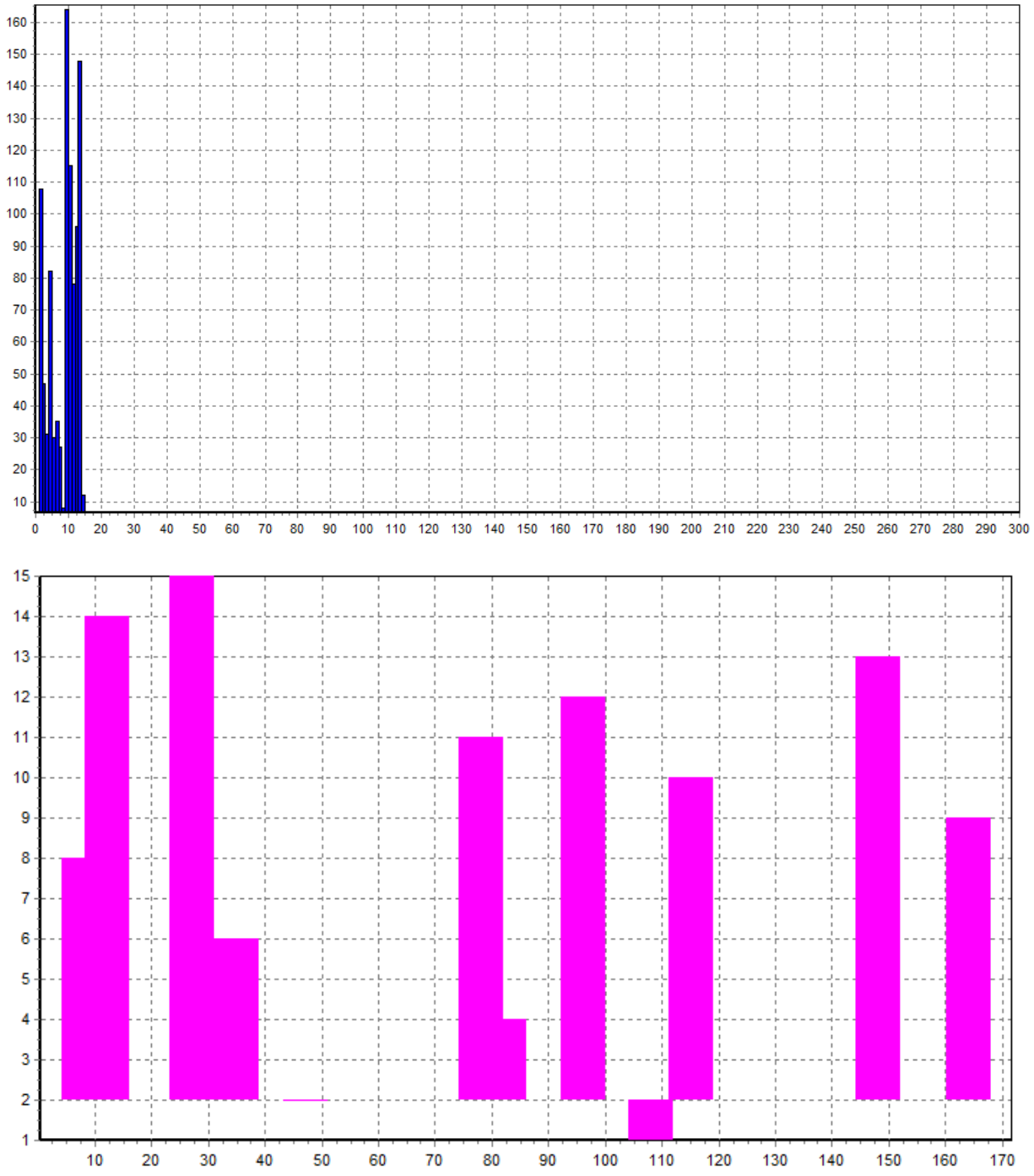

Figure 12 - Distribution of $\tilde{T}_{22}$.

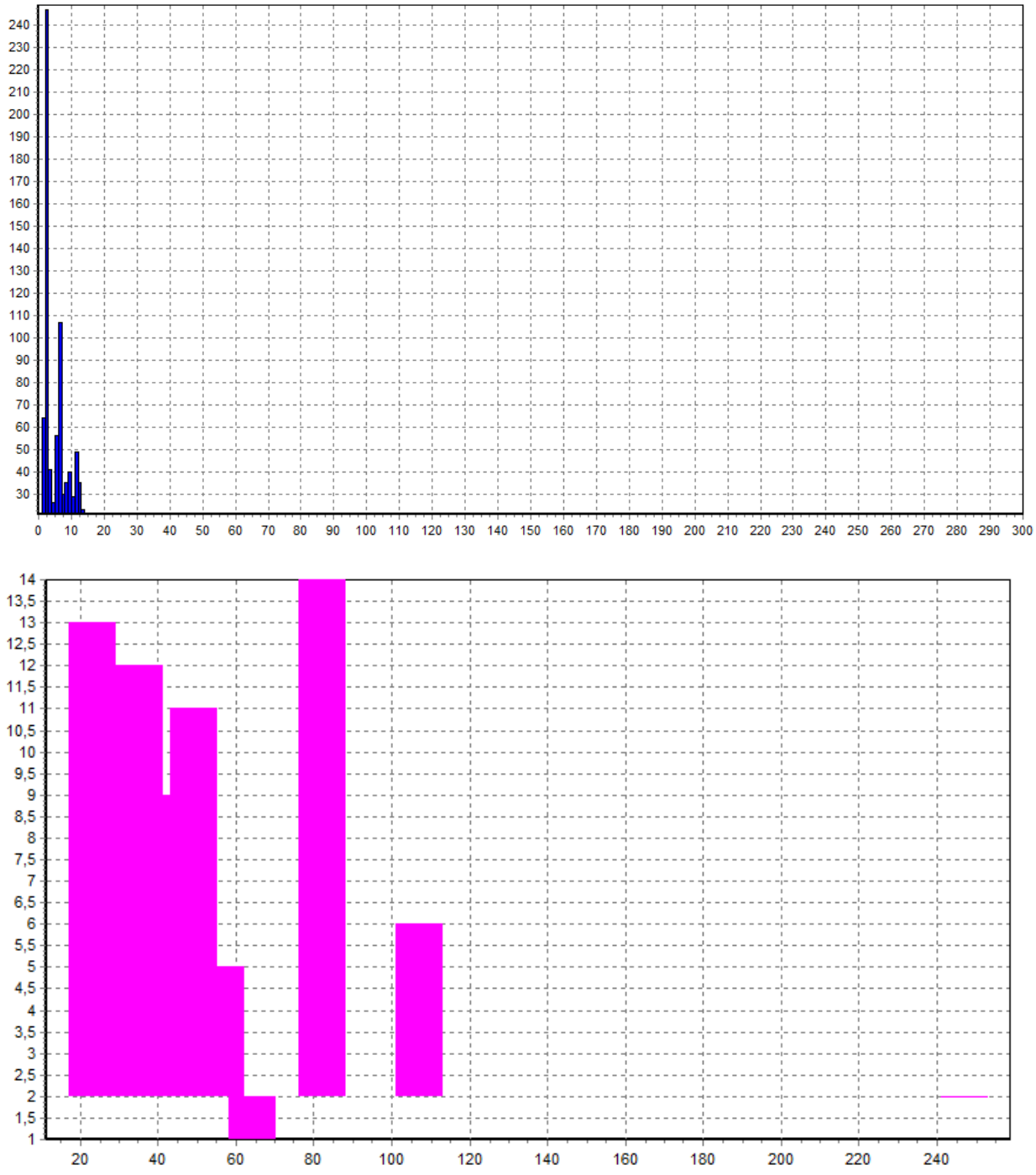

Figure 13 - Distribution of $\tilde{T}_{24}$.

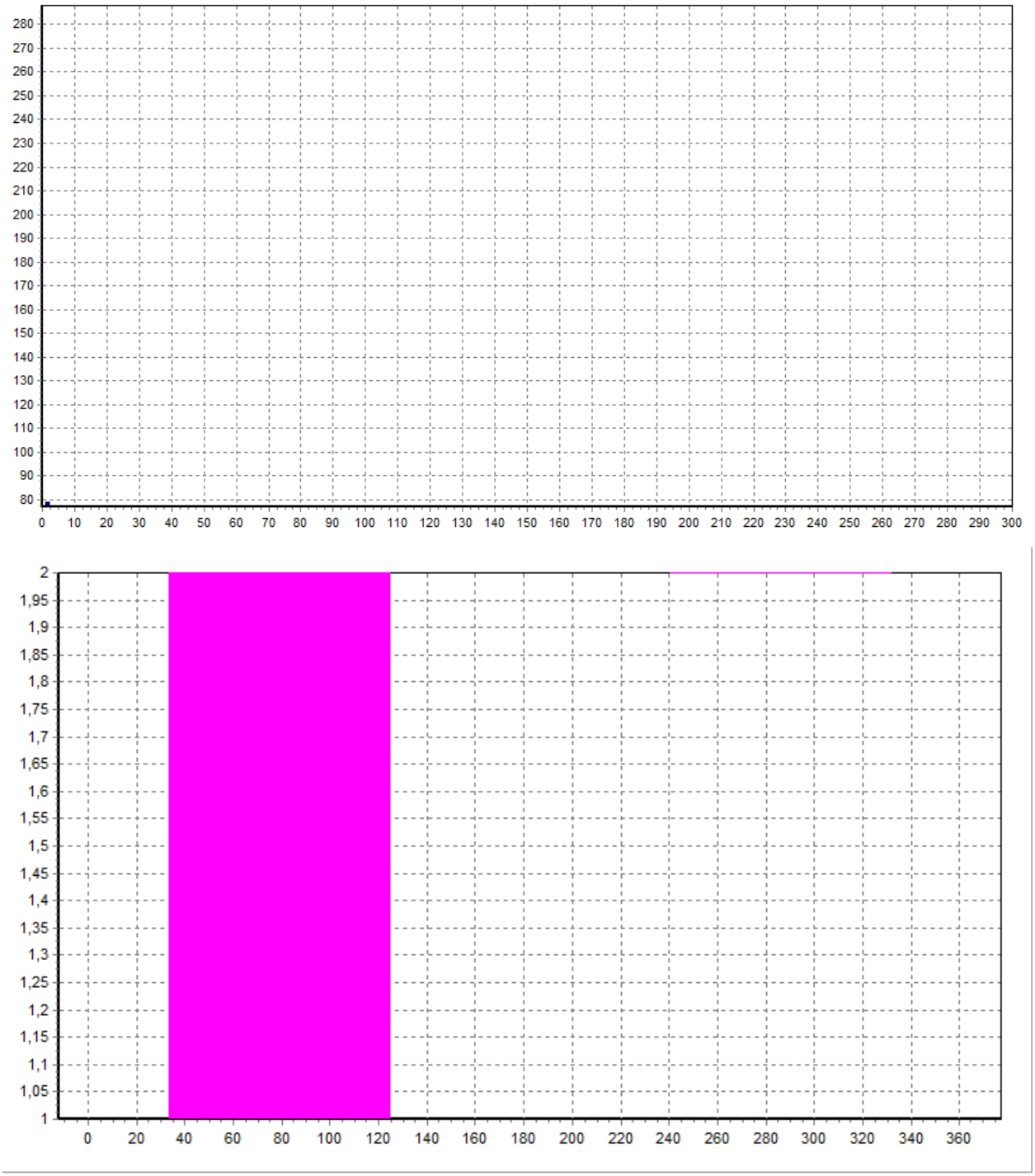

Figure 14 - Distribution of $\tilde{T}_{26}$.

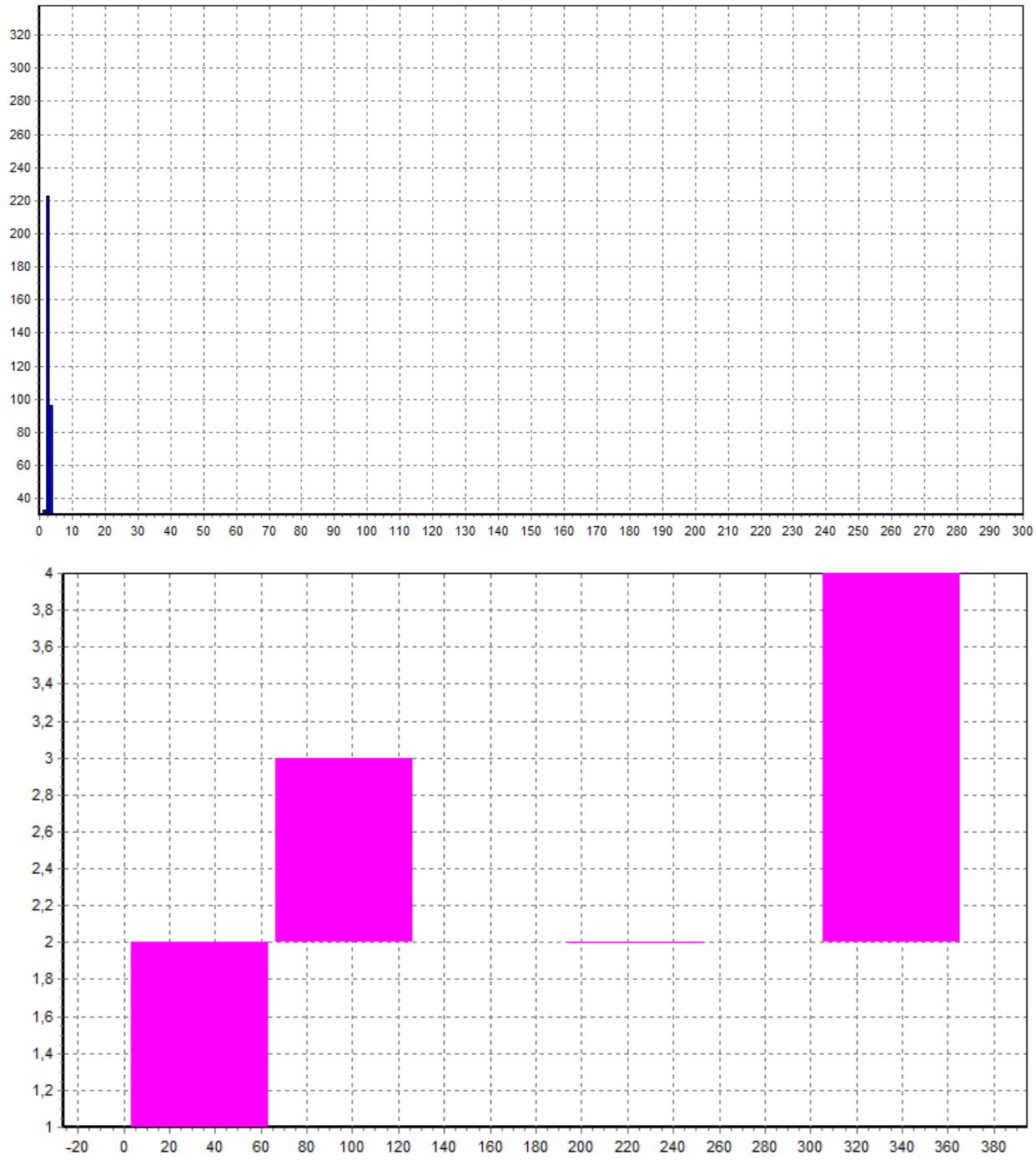

Figure 15 - Distribution of $\tilde{T}_{28}$.

A preliminary analysis of the obtained periods and distributions revealed no explicit dependency, and not allowed to obtain the analytical formula for the n-th member of a number.

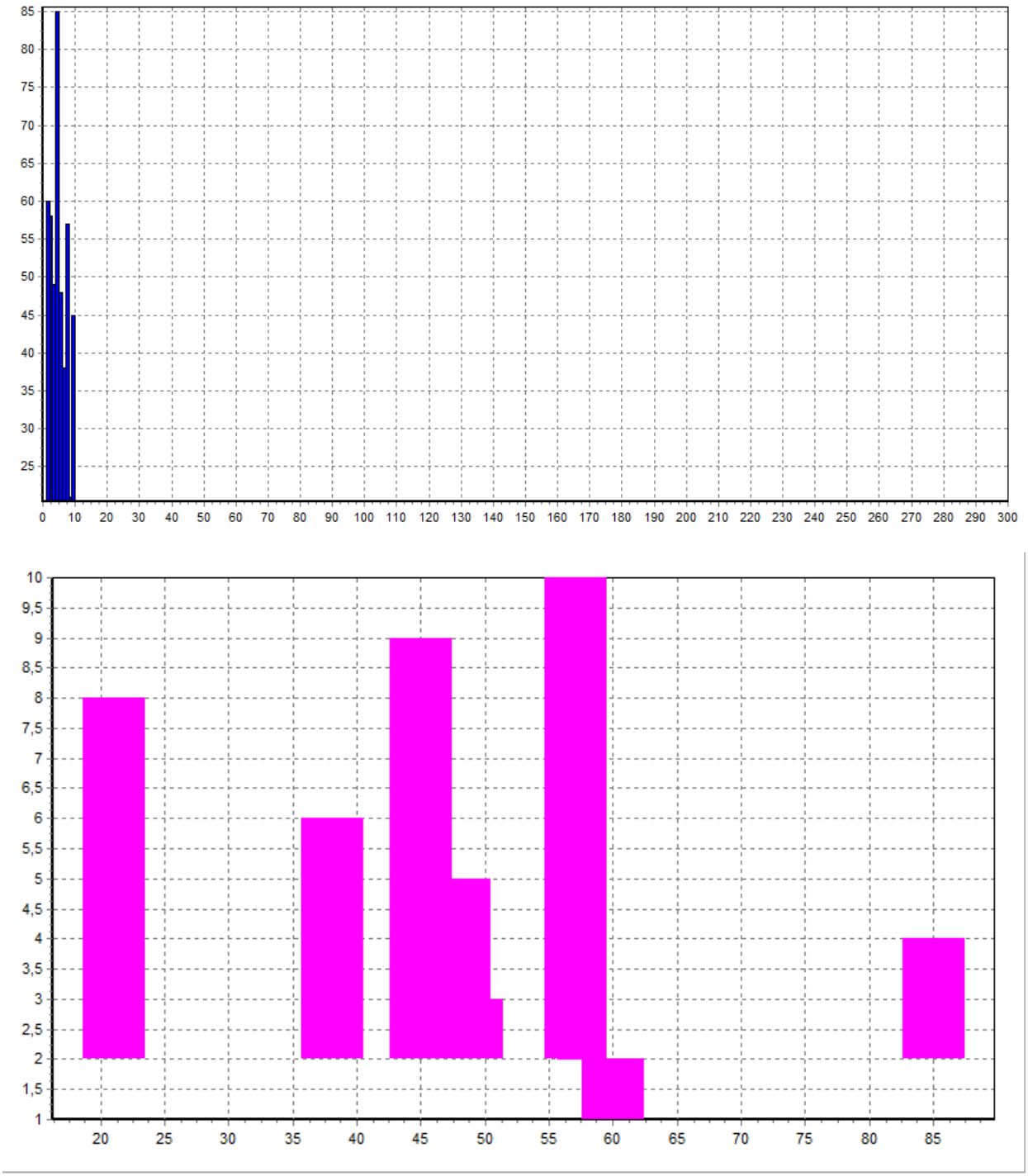

Figure 16 - Distribution of $\tilde{T}_{30}$.

Conclusions:

The obtained distributions can be used in the encoding in connection with the lack of obvious patterns, respectively imposition of any text on the distribution data can increase the cryptographic strength.

Reference

1. Схема Эль-Гамаля. Материал из Википедии — свободной энциклопедии.

[Электронный ресурс]. URL : http://ru.wikipedia.org/wiki/%D1%F5%E5%EC%E0%DD%EB%FC-%C3%E0%EC%E0%EB%FF (дата обращения: 16.08.2013).
2. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В Основы криптографии. –Гелиос АРВ, 2002г., 402с.
3. Фороузан Б.А. Криптография и безопасность сетей. Интернет-университет информационных технологий – ИНТУИТ.ру, Эком, БИНОМ. Лаборатория знаний, Серия: Основы информационных технологий-2010. 784с. [Электронный ресурс]. URL : http://www.intuit.ru/department/security/mathcryptet/15/2.html (дата обращения: 16.08.2013).
4. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. – М.: Изд-во «Интернет-университет информационных технологий – ИНТУИТ.ру», 2005. – 608 с.
5. Системы с открытым ключом. XServer.ru. On-Line библиотека. [Электронный ресурс]. URL : http://www.xserver.ru/computer/raznoe/bezopasn/7/ (дата обращения: 16.08.2013).
6. Шевцов А.Н., Туймебаева А.Е., Шенгелбаева У.К. Разработка кодировщика на Delphi для алгоритма Эль-Гамаля. – МНПК «Теоретические и практические научные инновации», г.Краков, Польша. 29- 31 янв. 2013г.