ЭЛЕКТРОНИКА МК-85С ANCRYPT АЗИМУТ (AZIMUTH)

MOSCOW - Museum Of Soviet Calculator On the Web

Written by Andrew Davie

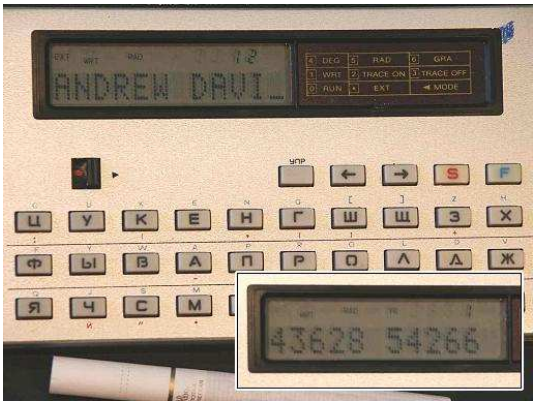
The content of Museum of Soviet Calculators is copyright © 1997-2001 Andrew Davie & contributors. Unless indicated to the contrary, permission is granted for private non-commercial use of images and text.

The ELEKTRONIKA MK-85C was a top-secret cryptographic device used mainly by the Russian military. Recently I was able to find a source for photographs of one of these machines, and here is the first tantalising glimpse of the machine alongside it's code-disk and cryptographic key. As the sender of the photos wrote to me... 'I am sure there is no "ANCRYPT" at the museums of US Army, FBI and CIA. You had a chance to possess it.'

I think he's possibly right - but the last thing I want is the CIA, FBI and the US Army on my tail! Not to mention the Russian secret services. It is interesting to read the early tentative reports of the machine (below) for a comparison between the real thing and what was surmised. I have some more photographs which I'll put online soon. But for now, enjoy the first pictures of this device to be seen in the West!

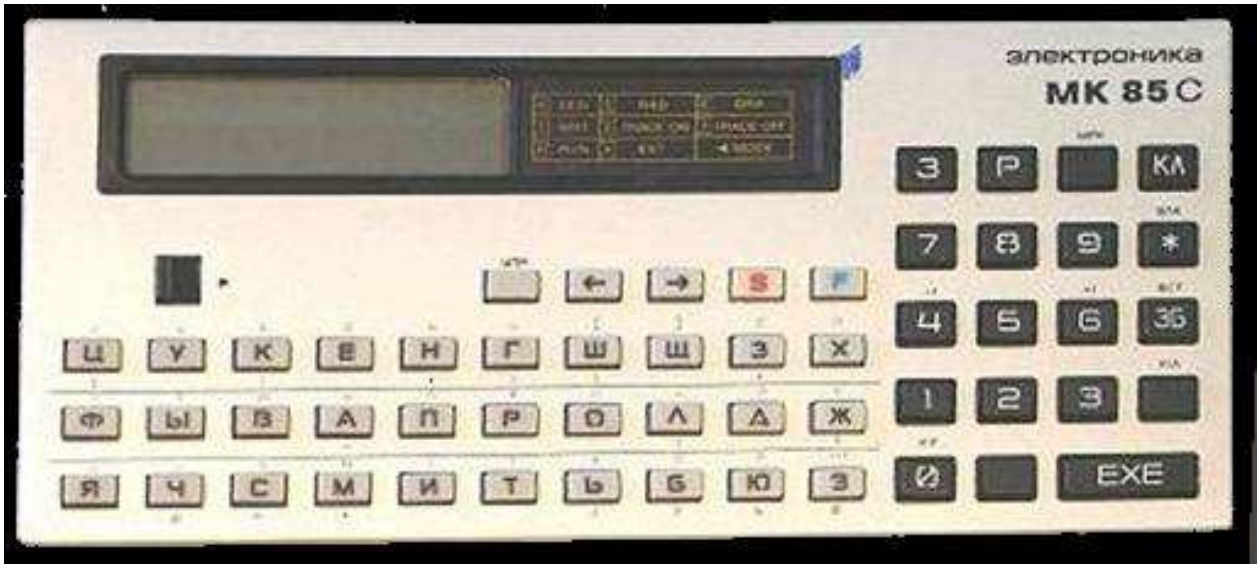
In case the secret services are reading - no, I do not have one of these machines - the photos were sent to me anonymously. All I know about it is the information you see on this page.

At last I've been encoded on a Russian military cypher calculator. Does it get any better than this?!



MK-85

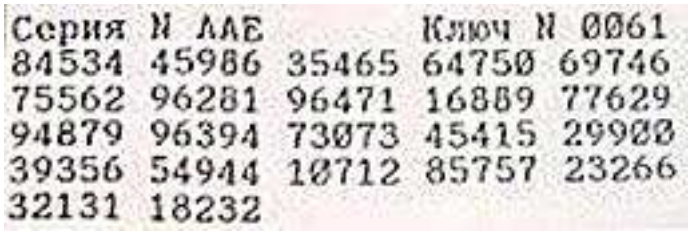
The MK-85 was used as the basis for this machine, as the picture below shows. Note the differences in the keyboards; the MK-85C has a custom keyboard and face replacement, along with in built cryptographic software.



Floodgates of Information Open!

It's interesting after the initial 'discovery' of a new machine how sometimes a flood of new information comes in. The pictures you see here of the MK-85C come after an approach I made to the Ancort company asking for a sample. At about the same time, I received pointers to a few pages from the Ancort company which gave some details and a small image of the machine. Thanks to those people (who wish to remain anonymous) who pointed me in the right direction!

This appears to be the cryptographic key:


Серия N ЛАЕ Ключ N 0061
84534 45986 35465 64750 69746
75562 96281 96471 16889 77629
94879 96394 73073 45415 29900
39356 54944 10712 85757 23266
32131 18232

ANCRYPT

(source: Ancort company website http://www.ancort.ru/English/fea_ancript.htm)

"ANCRYPT" is a first-rate miniature encipherer. It is an embodiment of up-to-date achievements of Russian cryptography, having centuries-old traditions. "ANCRYPT" offers outstanding ease of use. Compact hardware and high enciphering speed will meet your business needs both in the office and in a travel. It would take hundreds years to decrypt the information encrypted by "ANCRYPT" if someone doesn't know the cipher key.

The number of key variations (10 in 100th power) to be tested to attack the encrypted data exceeds the number of Galaxy atoms! The newest electronic technologies of "ANCRYPT" protect the information against intercepting devices situated nearby. The international business confirms the high efficiency of individual systems for a secret communication.

Operation mode

The user inputs a plaintext from alphanumeric keyboard. This text can be further edited. The entire text enciphering is made by simultaneous keystroke of two control keys. To decipher the information you have to input the ciphertext (a cryptogram) from the keyboard and select a proper control command.

A limit length of one-time enciphered text is 750 alphanumeric characters (a half of a standard typewriter page). The enciphered text can be further read out from the display to transmit it via communication facilities. A large data volume can be enciphered using the tandem "ANCRYPT".

Keeping enciphering secret

1. A cryptographic strength of cipher keys is provided.
2. During encipherer operation with a stand-alone power supply, data recovery made impossible for any special devices.
3. The hardware is password-protected against its illegal use by intruders.
4. Built-in facility is provided for immediate erasing of data and secret keys in emergency (attempt of the unit capture).
5. Disguising design of the unit makes it alike to an ordinary hand-held calculator.

Delivery set

1. "ANCRYPT" Encipherer 1
2. AC adapter 1
3. Protective Case; 1
4. User Guide 1
5. Minimum Set of Encipherment Keys 10

Options

1. Encipherment Key Generation Program (PC/AT) - 1 diskette
2. PC/ANCRYPT Compatibility Program - 1 diskette

Warranties

1. 12 months-limited warranty.
2. Maintenance support by ANCORT company as subscriber service or on requests.

Sales provisions

1. Advance payment in dollars by written order.
2. Delivery time limit - one week since the day of advance payment.

Specifications

Keyboard:	33 cyrillic characters; 26 roman characters; 10 digits; 14 control keys; 16 punctuation marks keys;
Display:	1 matrix LCD; 9 auxiliary symbols in a command line
Main functions:	• text enciphering/deciphering • text editing; • cryptogram error correction;
Encipherment mode:	• alphanumeric; • numeric;
Plaintext size:	750 alphanumeric characters or 1.500 digits
Plaintext input:	from a keyboard
Cryptogram output:	to LCD
Encipherment key input:	from a keyboard
One-time key:	generated by "ANCRYPT"
Data volume for encryption with the same encipherment key:	3.000.000 characters max.
Encipherment key variations:	10^{100}
One-time key variations:	10^{10}
Encipherment algorithm:	sophisticated non-linear
Dimensions:	70 x 162 x 17 mm
Net weight:	150 g
Operating environment:	• Working temperature range +5C to +50C; • Power source: 4 0.18 cells (battery life - 120 hours) AC adapter: 220V • Power consumption - 0.02W

It's a pity that Schtirlitz* and Kate* did not have it.

A. Nicolaev at Ancort website (source: http://www.ancort.ru/English/newspaper_002.htm)

In the course of tactical exercises of the 45th Special Regiment of Paratroopers, some 12 reconnaissance groups had been sent into the enemy's rear for the information support of the operation.

The coded messages were flowing incessantly and the cipher-clerks have been overwhelmed with work. Three urgent telegrams came with new orders of deployment for 3 reconnaissance groups. To encrypt them in traditional (manual) way would require much precious time and the orders would have lost their sense, so under the circumstances the top commander ordered to use the machine encryption (device called "Azimuth").

Thanks to efficiency and higher speed of machine encryption the operation had been successfully accomplished. The role of microcomputers "Elektronika MK-85C-Azimuth", supplied to the regiment several years ago as a backup or reserve equipment for coded communication is indisputable. For the first time I acquainted myself with this device in December of 1994 in Mozdok, before the hostilities in Chechenya. In half an hour time I acquired the necessary skills to operate the "Azimuth" and later the coded line Grozny-Mozdok-Moscow functioned without failures, in different environment and under various temperature conditions.

In spring and summer of 1995 the operation control of reconnaissance groups acting in the rear of Chechen bands was handled only with "Azimuths" portable encryptors. They proved to be not only efficient and convenient, but from the point of view of security of the stored information the risks of losing it or impossibility to destroy the secret papers in crucial situations as before the Portable encryptors are really priceless and safe. The key data used in message encryption/decryption can be erased in 2 seconds by pressing a special button, the previous encrypted messages disappear from the microschemes after the device is switched off.

Other advantages of the "Azimuth":

- complete keyboard both for Russian and Latin alphabet, digits and symbols;
- password for access to keyboard;
- automatic breaking of the coded message into three/-four/-five digital groups as required by user;
- possibility of quick correction of the coded text, also in decryption process;
- operational speed 4-5 times higher than in manual encryption;
- message can hold 750 numbers or 150 groups of 5 digits;
- weight of the minicomputer is only 150 grams, length 17 cm.

The time required for the user to obtain the operational skills is about 2 hours or less. The "Azimuth" had been duly tested and certified by FAGCI

This equipment for coded communications is manufactured by ANCORT Company, founded in 1990 (now JS ANCORT Co Ltd President Mr. Anatoly Klepov). More than 150 staff and contract specialists pursue the same goal to produce the equipment corresponding to the world standards and they succeeded in diversification and serial manufacture of various devices, thanks to a unique amalgam of high intellectual potential and professionalism of designers and developers. Along with "Azimuth" already known, its modernized analogue "Electronica MK-95C", compatible with any type of communication channels, is available, also the cryptophone AT-2400 and Fax-Crypto device for facsimile messages encryption.

However, the priority of ANCORT development work is concentrated today on data protection in computerized networks. The "Cryptocentre" system is absolutely secure one for the transmission and storage of confidential information.

The products developed by ANCORT offer the encryption of "guaranteed reliability" it means the third, highest level of resistibility to code breaking. First two levels of temporary (coded message can be broken almost immediately after interception) and of limited resistibility (codes can be broken in less than 3 months' time) are not secure. That is why the products created by ANCORT on the basis of original cryptographic systems, have been certified in Russia and in several foreign countries (South Africa, Sweden ea.). The production of reliable

cryptographic equipment is an expensive business, bringing dividends not quickly. Abroad such an activity cannot be handled by a usual solid company.

The products of ANCORT have the impact of the rich experience of special services of our country and the demand for them in many foreign countries is stable. Presently some government agencies in the CIS countries took a considerable interest in our devices, and this is positively considered by the management of the Company. Copyright © 1998 ANCORT. All rights reserved. Last updates: July 15, 1998

Citations

"The book "Podgotovka razvedchika" - Training of the Scout - (ISBN 985-433-190-3, published in Minsk, Belarus by "Harvest" publisher in 1998) describes on page 513 a portable encryption device "Azimuth", that is available in two versions, "Elektronika MK-85s" and "MK-95s" ("s" probably stands for "secret"). The latter is claimed to have the capability of "connection to any communication lines". I doubt more information will ever be available..." - Sergey Svischev

"I read in one paper, that on using the MK-85 as a base, the creation of special devices is possible. But, I think that idea of making cryptographic devices is unlikely. This calculator does not have peripheral units, the loading operation through the keyboard is extremely hampered. When I used the MK-85, I had problems with an oxydation of contacts, as a result of which the information was cleared from memory. I have not previously heard of the calculator MK-95. The "C" character, most likely meant "Special" - Sergei Frolov

"One of modern hardware solutions for an encryption of the information offered by the multi-experimental Russian developers, is the portable encipherer "Elektronika MK-85C". It is similar on average sizes the microcalculator (sizes 70x160x20, weight about 150 g). The text, which is necessary for ciphering, is entered from the alphanumeric keyboard of the instrument and can expose to the procedure of editing. And the manufacturers state that the instrument can be exploited in the locations, unprotected from listening. For an encryption of the e-mail there is a program solution - cryptography system PostCrypt. At obtaining the ciphered message automatically there is "acquittance" to the remailer, which obtaining is a warranty that the message has passed. There is a program of encoding of separate files intended for novice users.". - Garant-Service Samara LLC information technology (source: http://www.gss.ru/press/so/1998/so041/17-1.htm)