Summary

Functional Characteristics:

- Key tape perforation
- Key tape duplication
- Key tape back up on discette
- Key tapes compatible with key discettes
- Discette formatting and testing
- Key recording on discettes
- Key duplication from/to discette
- Printing literal keys in any format
- Printing numerical keys in any format
- Statistical testing of key distribution perforated on tapes or recorded on discettes
- Built-in self-diagnostic program

System Components:

- EPROM programming unit
- Discette drive
- Feed winder for two separate rolls of tape
- Perforator
- Reading unit
- Device for printing insertion markings
- Take up winder for two separate rolls of tape
- Complete electronic unit
- CRT terminal for command input, performance control and data display
- Printer for printing out ONE TIME KEY-pads or tables and results of statistical tests

Key Medium: Punched paper tape or discette 5¼"(3½" on request)

Storage Capacity: Key tape about 130000 characters
Key discette about 650000 characters

Operator Training Time: One day

Mechanical Dimensions: ME 600 Random Key Generator
1100 mm high, 520 mm wide, 450 mm deep
50 kg

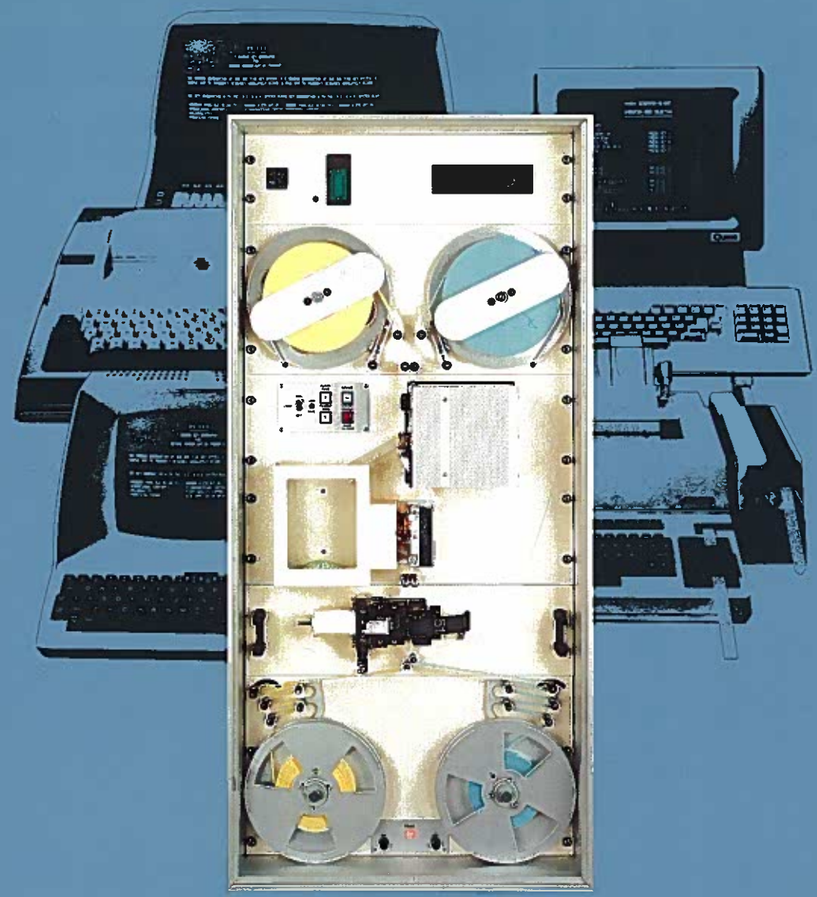
CRT Terminal
400 mm high, 400 mm wide, 350 mm deep
12 kg

Printer
100 mm high, 450 mm wide, 350 mm deep
8 kg

Courtesy comment: The development of the equipment "ME 600" has been supported considerable by the Austrian Industrial Research Promotion Fund.

MILS ELEKTRONIK A-6060 HALL / AUSTRIA POB 26
PHONE (52 23) 77 10-0, 24 77-0 FAX (52 23) 24 77 18 TELEX 533009 mils a

MILS ELEKTRONIK GES. M. B. H. + Co. KG.



ME 600

Random Key Generator

The second generation of our one time key of absolutely

Key produced with the

Universal Application:

The ME 600 features all functions needed in connection with the
keys on punched tape, the ME 600 even makes it possible to burn
which are only changed at long intervals (e.g.
Whereas hitherto separate equipment was required to burn this key
with our new
Existing EPROMs can, of course, be copied via this operating function.
each copy also corresponds 100 %

Extendible Production Capacity:

Should the production capacity of one machine not be adequate in a very
connection. The first machine thus automatically becomes
machines; during this operating function the noise sources
The entire random sequence stored in the master unit is
and can then be
It is for several reasons sensible not to connect machines in parallel, i.e.
considerably improves the degree of use of such machines since
can be changed at that time) can be in operation, the non-operation of
of all other

Optimum Security:

Character sequences from a noise source are absolutely unique and
usually proceed on the assumption that keys obtained in this way are
that random sequences actually unsuitable for ciphering information
come into use, all keys produced at random must be tested and evaluated
covers all important statistical regularities of a key punched tape,

Easy To Handle:

As in all new-generation equipment, all functions in the ME 600 are
makes it possible to integrate a Go/No Go-test as well as the actual
switched on. If the unit is operating without error, the operator receives
intelligible message is issued in the operator's language. This points to the
conclusion of the autotest the machine "questions" the operator via the
"answers" via the keyboard with the relevant command. This dialogue
or extensive periods of training: even operating errors are recognized as
the ME 600 can be operated

equipment offers the user the production secure cipher.

ME 600 system means:

All Important Functions In One Unit

production of random keys. As well as producing classic random
EPROMs. The latter are being used more and more to store keys
basic keys, long-term keys, permutations).
data, this procedure can now be carried out directly and most simply
ME 600 key generator.
Special programs monitor this copying process, it being ensured that
to the mother EPROM content.

Several Units Can Work In Parallel

few cases, further ME 600s can be connected with each other via a plug
the master unit, centrally controlling all attached slave
are, of course, switched off in the slave machines.
transferred to the connected slave machines within seconds
perforated independently.
with each other direct, but via a bus system. The elimination of down time
all machines apart from one (where perhaps the punched tape rolls
one single machine no longer automatically impeding the operation
units.

100 % Test Methods

are thus not reproducible. This fact notwithstanding, one does not
automatically suitable for ciphering. It is in the nature of a noise source
do occur, too. In order to be certain that only suitable key punched tapes
before being used. When suitable test methods are applied, our ME 600
preparing them in a clearly arranged manner for detailed evaluation.

Microprocessor-Controlled

controlled by microprocessors. The use of this modern technology
operating functions. This runs automatically when the machine is
a brief indication of this. In the case of a failure, however, a clearly
faulty module so that this can be exchanged even by a non-expert. After
connected terminal as to the required operating function. The operator
with the system obviates a time-consuming study of operating manuals
such and are automatically suppressed. After only one day's instruction
completely without error by anyone.

ME 600

Application and particulars

Application

Random punched tapes and random discettes can both be produced with the ME 600 unit. They may be compatible with one another or not, as required.

The ME 600 random key generator is the successor to the previous random key generator, the A6723, and it also replaces all other appliances in the ME A67 product family.

Our new ME 600 unit provides numerous advantages in comparison with its forerunner, the A6723. These advantages are due to the additional functions and the high standard of operating comfort provided by modern units today.

The most outstanding innovation in our ME 600 is, however, without doubt the perforating speed – up to 4 times as high, this cuts down the time required to produce a complete pair of punched tapes to well under 30 minutes – in conjunction with the built-in statistical test possibilities for the random sequence generated. The use of the latest electronics and fast test routines enables the entire random sequence (approx. 130000 characters) to be produced, stored and statistically checked almost without delay before it is punched into the tape. This ensures that random punched tape of no use for cryptological application on account of the insufficient statistical distribution of various characters can no longer be produced. This saves time and minimizes the mechanical wear on the puncher-head which would otherwise punch some 450000 holes in vain.

Dialogue-supported operating guidance and the automation of the major functioning phases enable easy, simple operation of the unit: after about one days' training, errorless operation is guaranteed.

Particulars

The ME 600 will without doubt appeal to all those users who already operate its forerunner, the A6723.

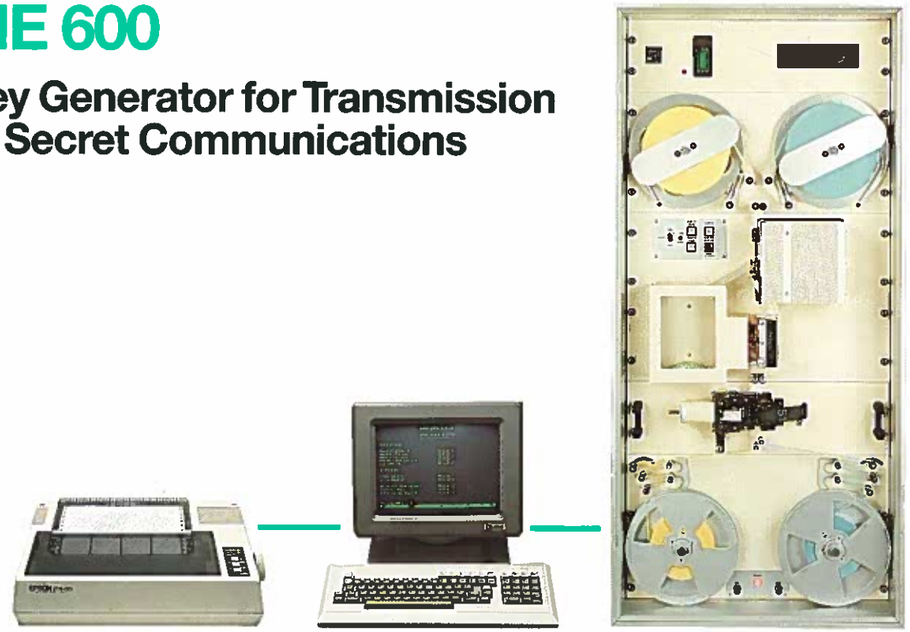
In order to introduce a new group of users to the random key tape system we have completely revised the functions of the preceding model. Here, we were able to use to advantage our more than 25 years' experience in the random key production sector, using the most up-to-date technology to produce a new unit, geared to the future.

We have not altered the random key concept, however – that just cannot be bettered, as international experts confirm (we shall be pleased to provide bibliographical references on this subject). Compared with its predecessor, the A6723, the new ME 600 unit features several decisive advantages. Essentially, these are:

- a considerably higher punching speed (75 characters/sec.)
- hence, a marked decrease in the production time for random punched tape (under 30 minutes for a complete pair with 130000 characters)
- production of compatible random punched tape and random discettes
- dialogue-controlled input guaranteeing errorless operation
- low maintenance
- different tests for the qualitative assessment of the statistical distribution, these taking place before perforation of the random sequence
- built-in autodiagnosis program for all function modules
- variable limitation for the maximum number of copies of identical punched tape pairs, discettes or ONE TIME KEY-pads
- production of ONE TIME KEY-pads in any format required (in literal and digital mode)

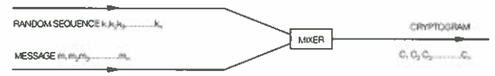
ME 600

Key Generator for Transmission of Secret Communications



Perfect security is in general an understandable wish, but it applies particularly to the exchange of secret information: unlike any other intrusion, an unauthorized access to information is virtually impossible to recognize, even after the offence has been committed.

This circumstance and the fact that information sometimes retains its topicality for many years are substantial reasons for the use of high-grade cipher systems. Of these, the ONE TIME KEY method (OTK) is without doubt the best: experts all over the world agree that this is the only absolutely crack-proof system – without any time limit. Added to this we have the transparency of the cipher process itself. Unlike electronic key generators, a OTK system requires no cryptological knowledge in order to be assessed as to its technical security. A clear text character mixed modulo 2 with the key character gives the corresponding cipher character.



Perfect security naturally demands special measures. Where an absolutely secure cipher system is concerned, this special measure is the distribution of a key (generally known under the specialist term ONE TIME KEY) that is obtained from a noise source. New equipment families and the use of microprocessors are, however, a major support in the organisation of this distribution, so no problems arise in this connection. This advantage and the great increase in intercepted messages are obviously a major reason why more and more departments engaged in the exchange of top secret communications choose the OTK method.

Apart from the sufficiently familiar cipher method with the random tape, discettes (floppy discs) provide a more up-to-date means of storing data for OTK ciphering. The benefits of this storage system considerably increase the operating security in comparision with random punched tape, human error being eliminated in such a system.

Hitherto the only disadvantage of these random discettes was that they could not be produced in cryptological compatibility with the existing punched tape.

Our new ME 600 unit meets with all user requirements in this respect, too, however. For this purpose the ME 600 is equipped with a discette system with which random discettes can be produced parallel to the pro-

duction of random punched tape. Thanks to the compatible key, ciphering units with random key tapes and ciphering units with random discettes can both be operated without any restrictions on the same network.

The modular construction, the plug-in electrical connections and highly perfected programmes represent an exceptional development concept, the unit being superbly simple to operate despite its remarkably complex functions. The ME 600 consists of a 19" housing with a discette drive, a feed winder for two separate rolls of punched tape, a perforator, a reading unit, a device for printing the insertion markings, a tape up winder for two separate rolls of tape and the electronics. The peripherals are a CRT terminal to service the entire system and a matrix printer to issue results of the statistical tests. ONE TIME KEY-pads can, of course, be produced with this in any required format, as used for manual ciphering or for random sequences in code setting on appliances with electronic key generators.

In order to ensure that both punched tapes are 100 % identical these are placed one on top of the other and are perforated in one process. They are printed with a serial number insert marking and this later helps to determine a certain starting position for the key punched tape in the actual ciphering procedure.

For reasons of security the user of random keys requires as precise information as possible regarding the distribution of the various characters and their correlation with each other. In order to comply with this requirement the random sequence taken from the noise source has to be subjected to relevant statistical tests. Permanent monitoring of the mechanism involved in the perforating process is at least of equal importance, this permitting a guarantee that every single character is perforated in exact accordance with the bit sample of the produced and tested random character. The ME 600 unit naturally fulfills the user's expectations in this respect, too: the entire mechanism is simply and effectively monitored with an authentic "read after write". A punched tape reader covers every punched character and this is then compared with the original bit sample from the noice source. Any deviation interrupts the key tape production process and an error message is issued by the attached monitor terminal which also shows how the error came about.

In order to ensure that only random punched tapes of a certain minimum quality (in respect of random distribution) are perforated, the random characters produced are no longer perforated immediately, but are first stored in a semiconductor memory. Character distribution within the random sequence stored (approx. 130000 characters) is then checked by means of many different tests. With the aid of these, all important statistical regularities can then be covered. Depending on the prescribed tolerance limits, all test results are calculated before perforation of the punched tape; they are then compared with the established threshold values (the 4th inside page of this catalogue shows a section of the test protocol). If overall the test is positive, the entire memory content is perforated, being available in less than half an hour as a complete pair of random key tapes.

Since a memory with the character capacity of a punched tape roll has to be available to carry out the statistical test, this can also be used to "copy" a punched tape. For reasons of security, the maximum possible number of such copies from one and the same memory content can be limited by a password so that no further copies of the relevant key sequence may be produced.

The built-in discette system makes it possible both to produce discettes compatible with random key tapes and to back up the key sequence of any required random key tape on discettes in order to be able later to reproduce certain random key tapes. The time-consuming copying process for many identical random key tapes (e.g. for secret circular messages) does not thus have to be carried out in one process, but can be interrupted at any time and recommenced at a suitable moment.

An integrated spooling device enables both random key tapes to be spooled back so that they can be packed and sent off directly after being removed from the winding plate. A visually readable identification number is punched at the beginning and at the end of the key tape so that the relevant roll of punched tape can be safely forwarded to the right recipient. Confusion by mistake, i.e. the erroneous assignment of a random key tape to the wrong recipient, is thus impossible.

To round off the universal application of our ME 600, ONE TIME KEY-pads in any format can be produced via the attached printer. By this we mean tables which are used for manual ciphering without any equipment. The format of the letter and figure tables can be freely programmed, i. e. the group length, the number of groups per line, the line spacing and the number of lines per page can be determined by the operator himself.

Excerpt from a Print out of Test Results showing statistical distribution of Random Characters

5 BIT OPERATION

POKER TEST

"1" BIT/BYTE	FREQUENCY	MEAN VALUE	DEVIATION
0	3747	3840	93 -
1	19137	19200	63 -
2	38277	38400	123 -
3	38513	38400	113 +
4	19387	19200	187 +
5	3819	3840	21 -

CHI SQUARE RESULT : 5,12
CHI SQUARE LIMITS : 0,21 TO 20,51
ACCEPTABLE : YES

BIGRAM TEST

NUMBER OF BIGRAMS : 61440
MEAN VALUE : 60,00
MAXIMAL DEVIATION FROM THE MEAN : 27 +

BIGRAM	DEVIATION	BIGRAM	DEVIATION
11 - 21	27 +	12 - 23	25 -
8 - 6	26 +	23 - 12	21 -
3 - 30	24 +	15 - 23	20 -
15 - 22	22 +	8 - 17	20 -
15 - 29	21 +	3 - 4	20 -
1 - 25	21 +	13 - 7	19 -
15 - 5	19 +	19 - 13	18 -
3 - 24	19 +	19 - 5	18 -
1 - 29	19 +	17 - 6	18 -
27 - 6	18 +	13 - 26	18 -

CHI SQUARE RESULT : 1035,55
CHI SQUARE LIMIT : 1162,67
ACCEPTABLE : YES