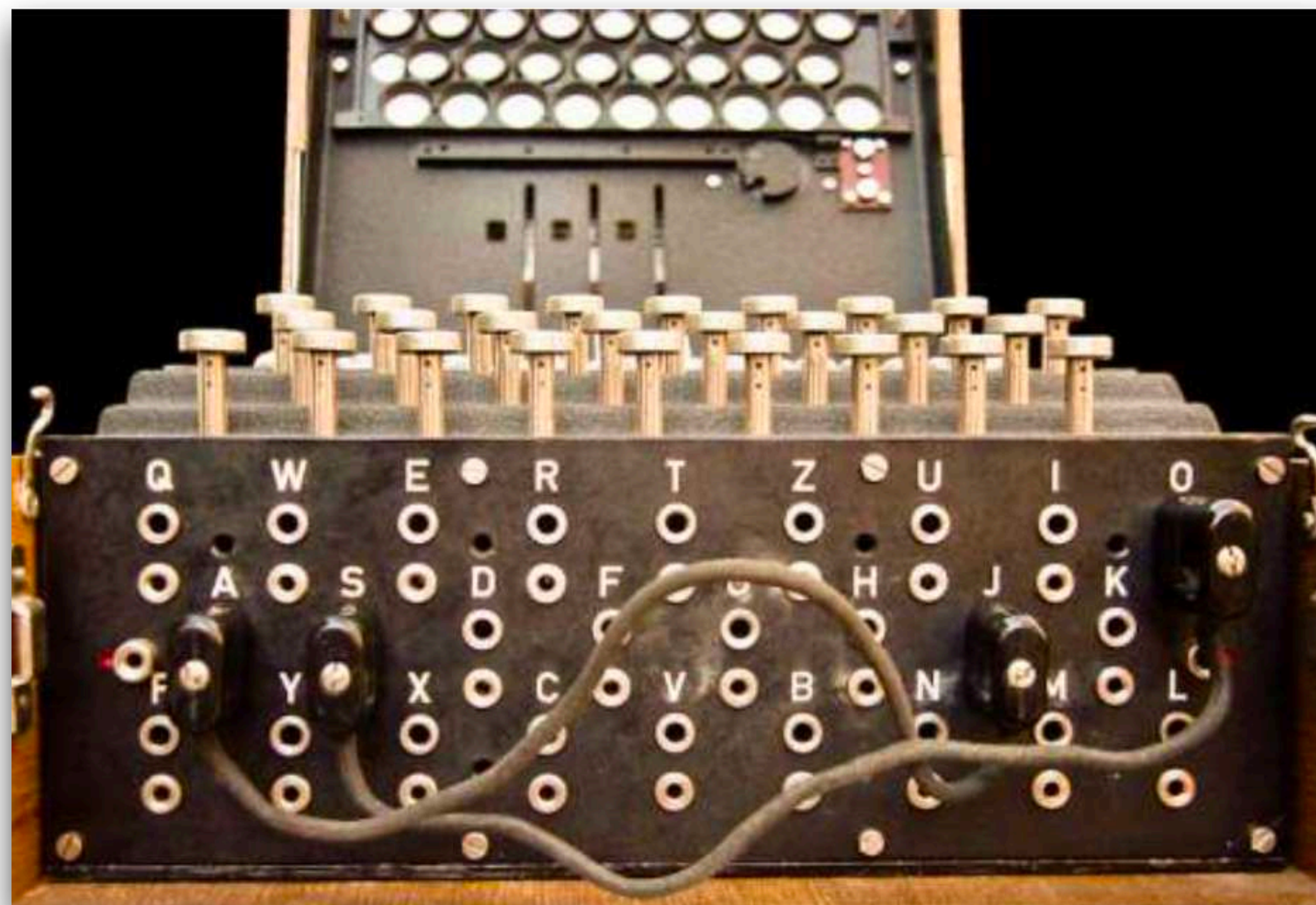




Co-funded by
the European Union



Енигма



www.euroqci.bg

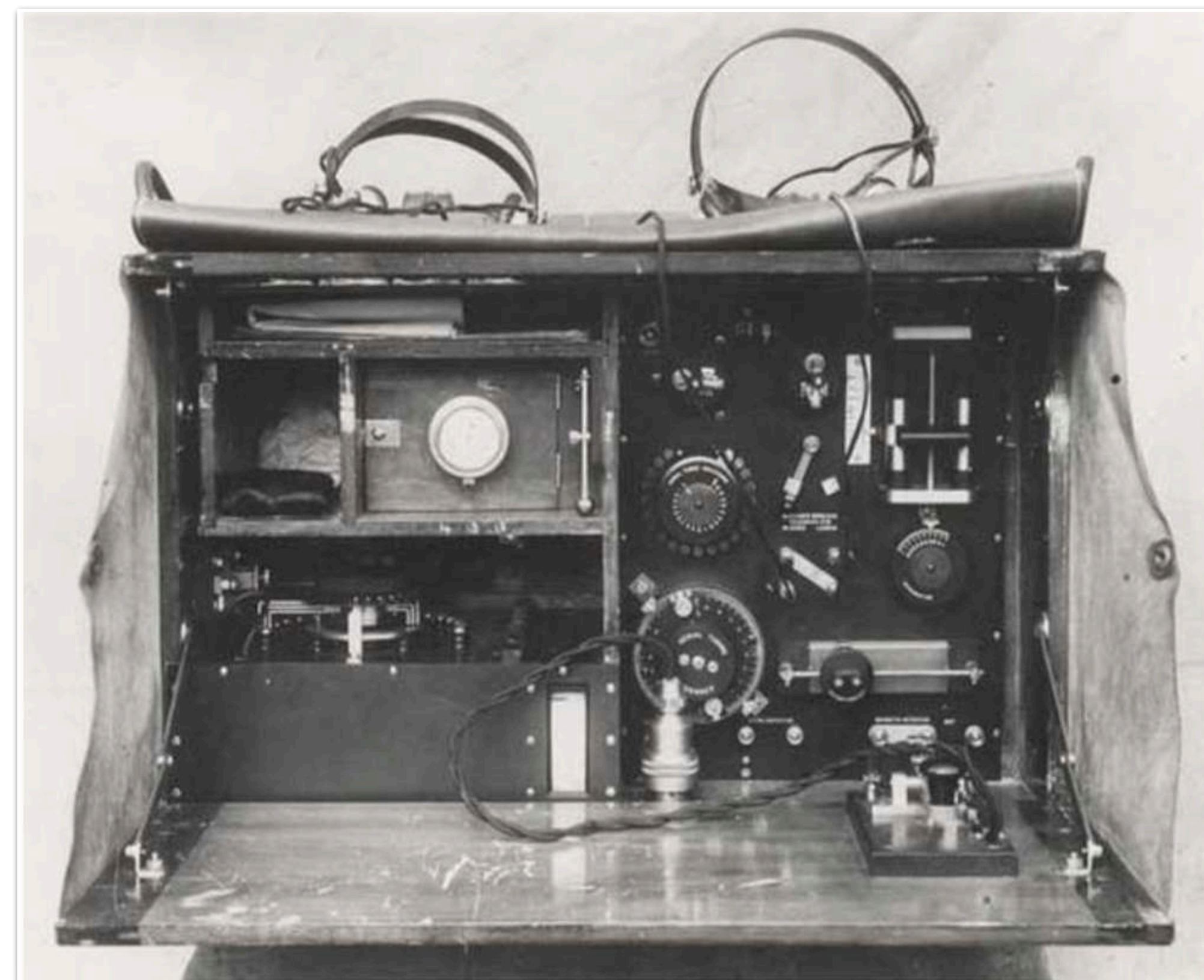
*Проект 101091399 “Национален план за изграждане на QCI за България” е съфинансиран от Европейския съюз.
Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.
Нито Европейския съюз, нито съфинансиращият орган носят отговорност за тях.*



Контекст

ПСВ - комуникации

- Развиването на комуникациите показва изоставането на шифрите
 - По-голямо количество данни
 - Извършва се на ръка



www.euroqci.bg

*Проект 101091399 "Национален план за изграждане на QCI за България" е съфинансиран от Европейския съюз.
Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.
Нито Европейския съюз, нито съфинансиращият орган носят отговорност за тях.*



Questions.		SHIPPING.		Fop.	
No.	SENTENCES.	No. of Ci-pher Word.	No.	Cipher.	No. of Sentence.
3139	What vessel did you ship by ?.....		3139	Foppish	
3140	When, how, and by what route shipped ?...		3140	Forage	
3141	When and how were bills of lading forwarded ?.....		3141	Forbade	
3142	When can you ship ?.....		3142	Forbear	
3143	When will a sailing vessel clear for—?.....		3143	Forbid	
3144	When will you ship ?.....		3144	Forbidden	
3145	Which did you ship ?.....		3145	Fordable	
3146	Who are the consignees ?.....		3146	Forego	
3147	Will a few days delay in shipping make any difference to you ?.....		3147	Forenead.	
3148	Will you receive consignment of—?.....		3148	Forelock	
3149	Ship		3149	Foremost ...	
3150	Ship additional.....		3150	Forest	

www.euroqci.bg

Проект 101091399 “Национален план за изграждане на QCI за България” е съфинансиран от Европейския съюз.

Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.

Нито Европейския съюз, нито съфинансиращият орган носят отговорност за тях.



Енигма машината

Общ поглед

- “Пишеща машина”
- Иновацията: електро-механични ротори
- Работата на оператора - по-лесна, но необходима



www.euroqci.bg

Проект 101091399 “Национален план за изграждане на QCI за България” е съфинансиран от Европейския съюз.
Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.
Нито Европейския съюз, нито съфинансиращият орган носят отговорност за тях.



Енигма машината

Ротори



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

www.euroqci.bg

Проект 101091399 "Национален план за изграждане на QCI за България" е съфинансиран от Европейския съюз.

Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.

Нито Европейския съюз, нито съфинансиращият орган носят отговорност за тях.



Енигма машината

Клавиатурата

- QWERTZ клавиатура с 26 букви
- Няма цифри, препинателни знаци, свободно място
- Всяко натискане задвижва роторите



www.euroqci.bg

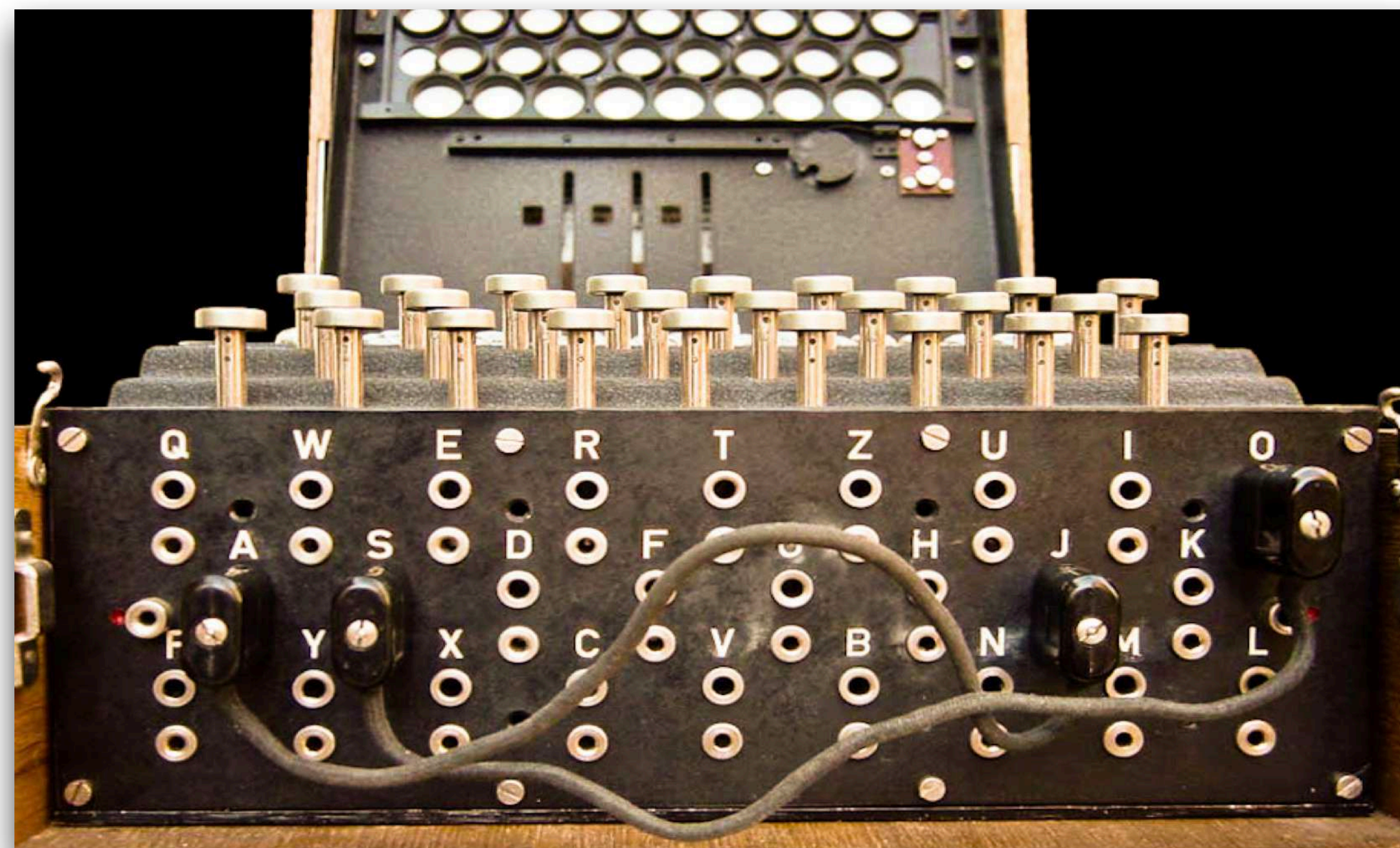
*Проект 101091399 “Национален план за изграждане на QCI за България” е съфинансиран от Европейския съюз.
Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.
Нито Европейския съюз, нито съфинансиращият орган носят отговорност за тях.*



Енигма машината

Комутационен панел

- 26 отвора за всеки един клавиш
- При свързване с кабел разменя позициите на двете букви
- Добавен 1930г от немската армия
- Съществуването му е пазено в строга тайна



www.euroqci.bg

Проект 101091399 "Национален план за изграждане на QCI за България" е съфинансиран от Европейския съюз.

Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.

Нито Европейския съюз, нито съфинансиращият орган носят отговорност за тях.

Енигма машината

Светлинен панел

- Показва с коя буква криптираме
входящата



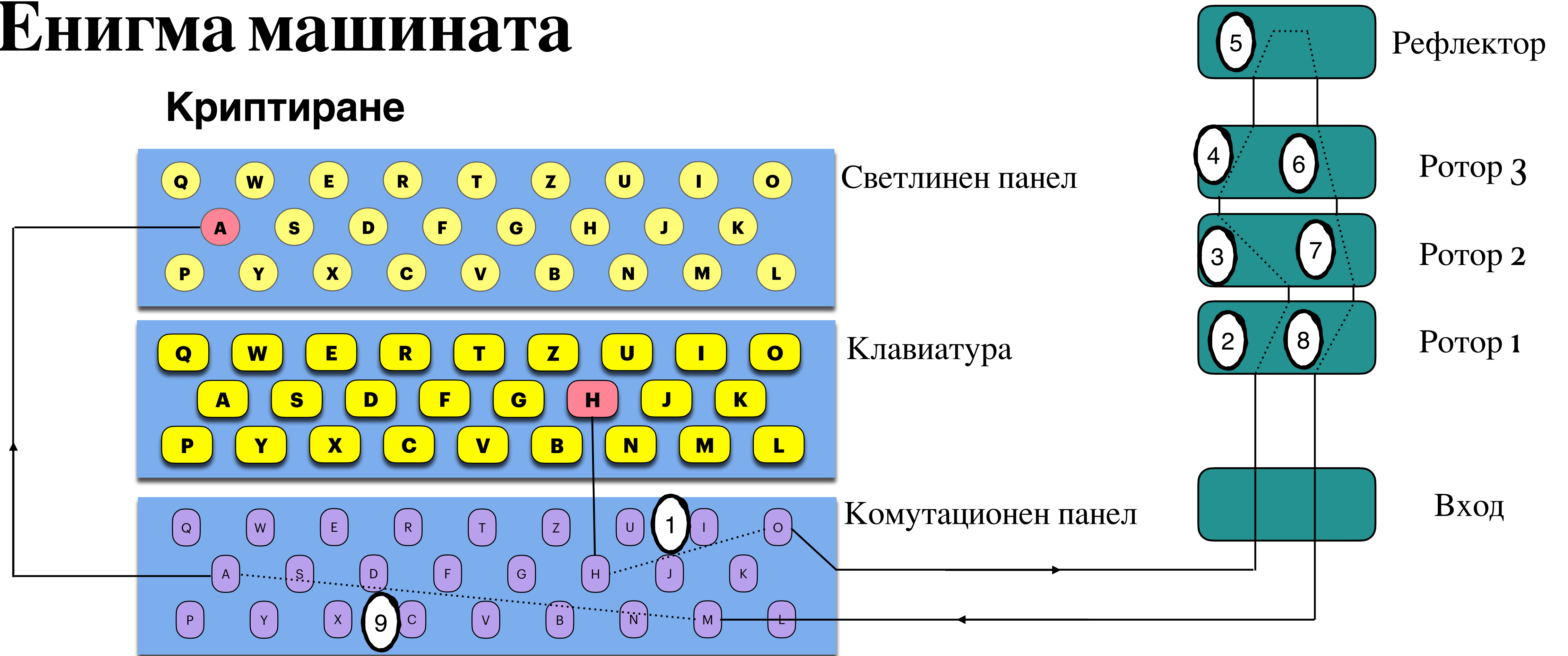
www.euroqci.bg

*Проект 101091399 "Национален план за изграждане на QCI за България" е съфинансиран от Европейския съюз.
Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.
Нито Европейския съюз, нито съфинансиращият орган носят отговорност за тях.*



Енигма машината

Криптиране

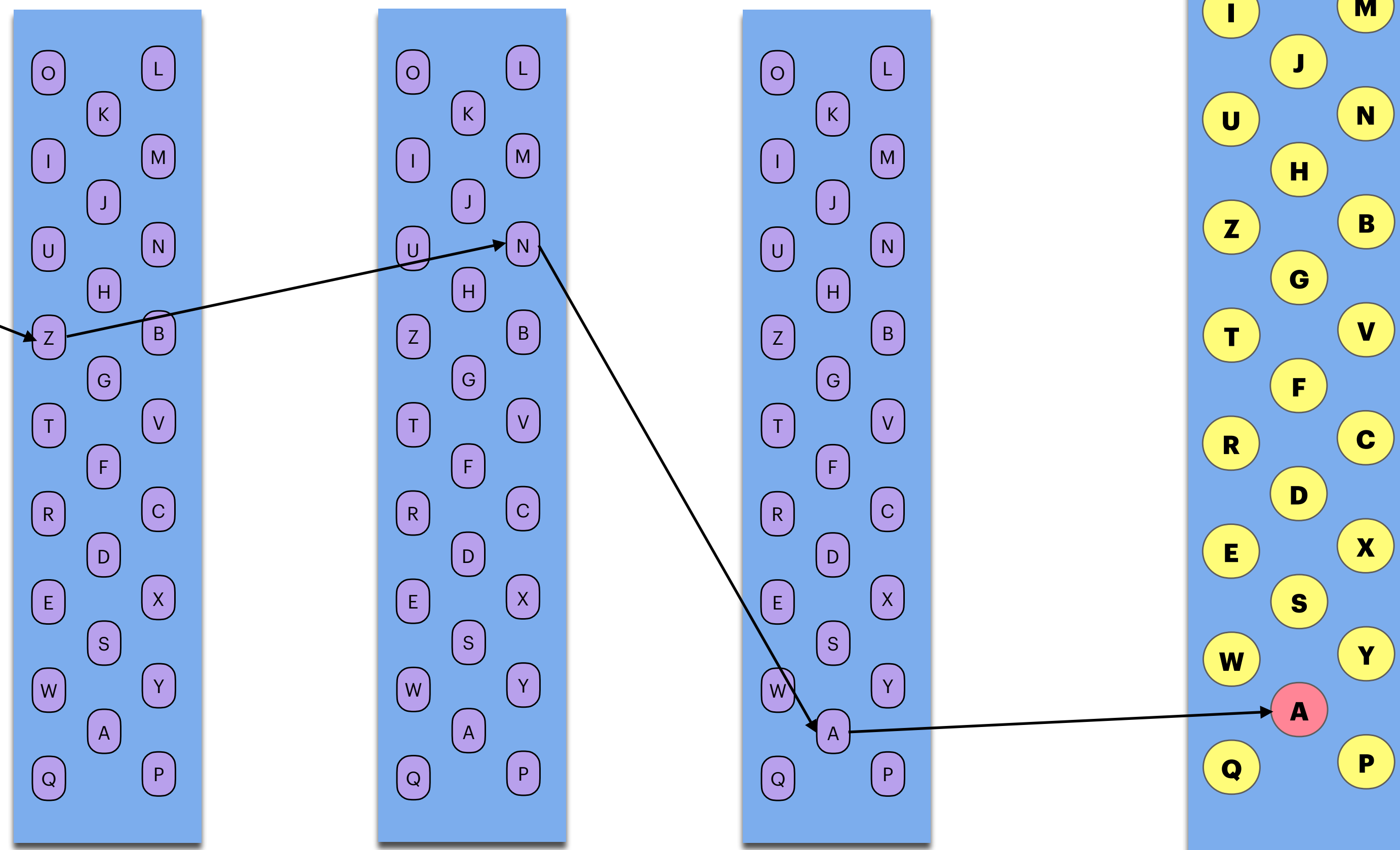
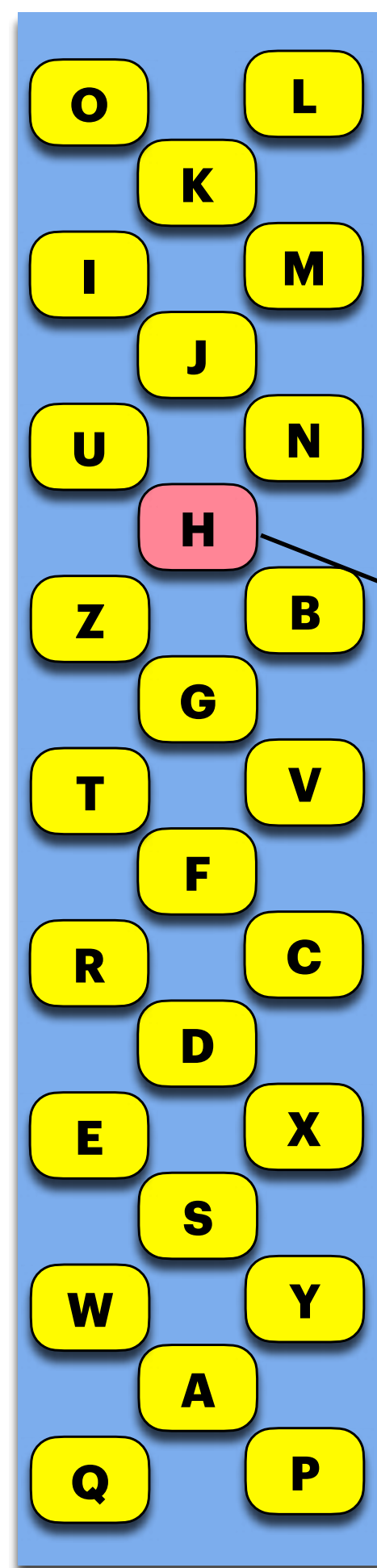




Енигма машината

Криптиране

Клавиатура



Светлинен панел

www.euroqci.bg

Проект 101091399 "Национален план за изграждане на QCI за България" е съфинансиран от Европейския съюз.

Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.

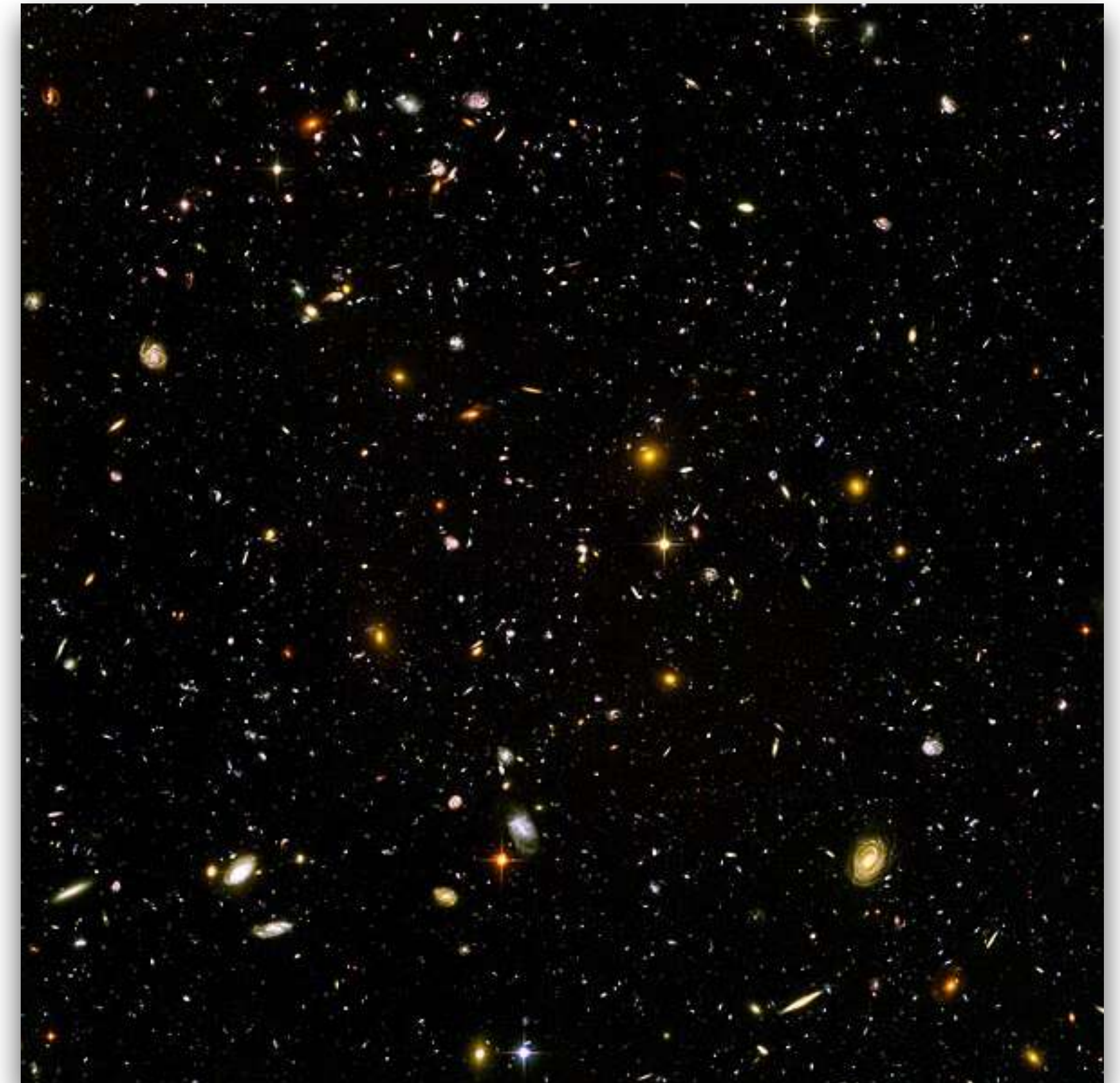
Нито Европейския съюз, нито съфинансиращият орган носят отговорност за тях.



Енигма машината

Брой възможни конфигурации

- Начална конфигурация = ключ
- Броя на всички възможни конфигурации е по-голям от броя атоми във Вселената
- За практическо ползване е ограничен броя конфигурации
- Ключа за енигма е 77 бита, като DES (1976-2002) използва 56 битови ключове





Употреба на Енигмата

- Месечни книги с ключове
- Сесийни ключове
- Допълнителни шифри = допълнителна сигурност



www.euroqci.bg

*Проект 101091399 “Национален план за изграждане на QCI за България” е съфинансиран от Европейския съюз.
Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.
Нито Европейския съюз, нито съфинансиращият орган носят отговорност за тях.*



Употреба на Енигмата

Geheim!
Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGS 08 *

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
31.	I II V	10 14 02	BF SD AY HG OU QC WI RL XP ZK	yqv vuc xxo gvf
30.	V IV I	04 25 01	DI ZL RX UH QK PC VY GA SO EM	mgy vts gvt csx
29.	III V II	13 11 06	ZM BQ TP YX FK AR WH SO NJ DG	aky vdv oyo tzt
28.	I III II	09 16 12	NE MT RL OY HV IU GK FW PZ XC	nfh vcc tur wnb
27.	III II I	06 03 15	BF GR SZ OM WQ TY HE JU XN KD	bec jmv vtp xdb
26.	I III V	19 26 08	GS VD CQ LE HI BO JP UZ FT RN	wvu yem buz rjk
25.	II I IV	05 01 16	KA ZH QP GR MF LJ OT EN BD YW	ktv muq cqm cpm
24.	III II IV	22 02 06	PI KM JB YU QS OV ZA GW CH XF	zcd iwo urp glg
23.	IV III II	08 11 07	SX TD QP HU FB YN CO IK WE GZ	epm mgz vqg vsm
22.	I V II	13 02 26	GP XH IW BO NU MD SA ZK QR LT	aam mvv jqq wqm
21.	IV I V	17 24 03	XC AQ OT UZ HD RG KM BL NS JW	ltl blu frk xrh
20.	IV I III	15 22 12	PO TV QC ZS EX WR BJ DK FU LA	non lic oxr usr
19.	V I III	13 24 21	HA GM DI VK JP YU EF TB ZL XQ	ecd ciq uvr ppt
18.	IV V I	23 09 20	XP PZ SQ GR AJ UO CN BV TM KI	fjh zts uqt cft
17.	III II V	21 24 15	UT ZC YN BE PK JX RS GF IA QH	oub eci pyf rqi
16.	IV III V	07 01 13	IN YJ SD UV GF BH TK QE AR OP	kex paw flw onw
15.	I IV II	15 04 25	TM IJ VK OY NX PR WL GA BU SF	sdr pbu byv khb
14.	III II IV	10 23 21	WT RE PC FY JA VD OI HK NX ZS	mhz lff lnq giy
13.	V I II	14 04 12	AN IV LH YP WM TR XU FO ZB ED	rqh ucm ldi ods
12.	II V I	07 19 02	HR NC IU DM TW GV FB ZL EQ OX	asy xza uvc fmr
11.	I V IV	13 15 11	NX EC RV GP SU DK IT FY BL AZ	gyd iuq ocb vef
10.	V II I	09 20 19	FN TA YJ SO EG PC VD KI XH WZ	pyz ace pru uyc
9.	I IV V	14 10 25	VK DW LH RF JS CX PT YB ZG MU	nyh fbd ohs jrp
8.	IV V I	22 04 16	PV XS ZU EQ BW CH AO RL JN TD	tck rts nro mkl
7.	V I IV	18 11 25	TS IK AV QP HW FM DX NG CY UE	mhw lwb mdm ybe
6.	IV I III	02 17 20	KZ FI WY MP DS HR CU XE QV NT	uwu vdk lrh mgd
5.	I V IV	26 09 14	VW LT PB FO ZK GS RI QJ HM XE	suw tsv nfp yjc
4.	IV III V	07 01 12	QS YA XW KR MP HT DU OV CL FZ	uby usi mhh mwb
3.	I II V	05 16 03	FW DL NX BV KM RZ HY IQ EC JU	tns von grw axl
2.	III I II	12 22 17	DW UO PY GR FS EQ KT CL AI ZB	smz lbl bkc sym
1.	I III II	04 18 06	ZN OM CR UI KP WQ SE JV LX TF	ghr vqv cya ayl

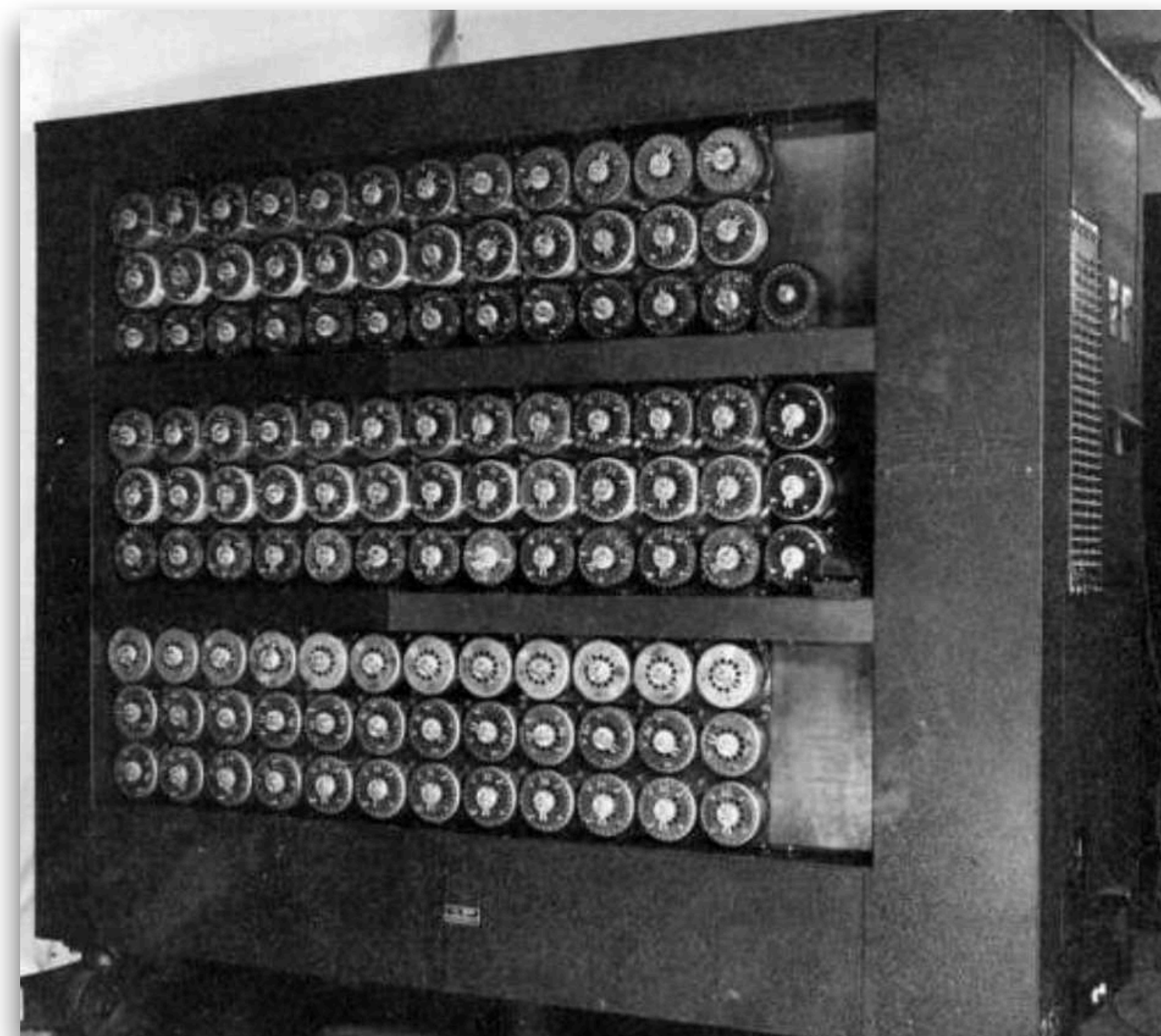
www.euroqci.bg

Проект 101091399 "Национален план за изграждане на QCI за България" е съфинансиран от Европейския съюз.
Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.
Нито Европейския съюз, нито съфинансиращият орган носят отговорност за тях.



Разшифроването на Енигма

- 1930 - френски шпиони - двойник на енигма
- 1939 - Блечли парк - 11000 човека
- Алън Тюринг - The Bombe и Crib attack
- U-Boats



www.euroqci.bg

*Проект 101091399 "Национален план за изграждане на QCI за България" е съфинансиран от Европейския съюз.
Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.
Нито Европейския съюз, нито съфинансиращият орган носят отговорност за тях.*



Енигма след войната

- Тайна до 1974г
- Руски и английски машини
- Ценни уроци:
 - Защитаваме информацията срещу бъдещи атаки
 - Сигурността на информацията е гарантирана от ключ
 - Можеш да имаш доверие само на себе си



www.euroqci.bg

*Проект 101091399 “Национален план за изграждане на QCI за България” е съфинансиран от Европейския съюз.
Изразените позиции са на автора/авторите и не отразяват непременно гледната точка на Европейския съюз и Европейската комисия.
Нито Европейския съюз, нито съфинансиращият орган носят отговорност за тях.*