МАТЕМАТИК, ЩО РОЗШИФРУВАВ КОД «ЕНІГМИ»
«ЕНІГМА»

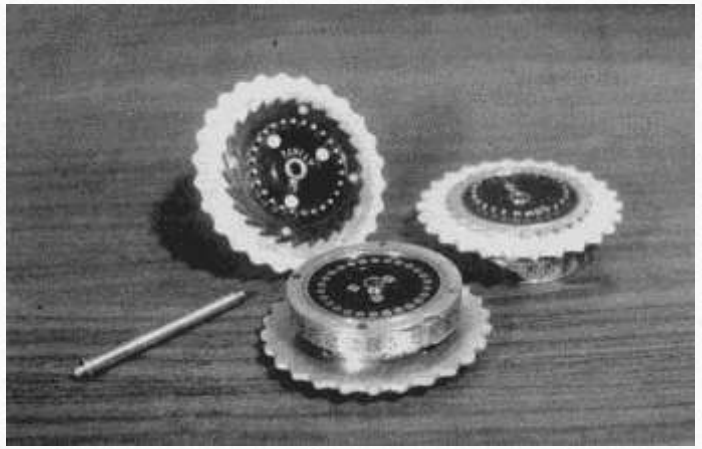
Підготував студент групи МІ18Б
Левицький Ярослав

«Енігма» - представник дискових шифрувальних машин(основа механізму є диски з 26-ма перепайками». «Енігма» використовувалася в комерційних, а також у військових і державних службах в різних країнах світу, проте найбільшого поширення набула в нацистській Німеччині під час Другої світової війни. З точки зору криптографії шифр «Енігми» був слабкий, а на практиці поєднання цього чинника з іншими(помилки операторів, припущення про текст повідомлень тощо) і захоплення розвідкою екземплярів «Енігми»(+ шифрувальних книг), дозволило розгадувати її шифри і читати повідомлення

«Енігма» працювала шляхом постійної зміни електричного кола, за рахунок обертання внутрішніх роторів, через які йшов струм. При кожному натисканні букви на клавіатурі машина видавала букву шифру, а ротори ставали в нову позицію.

(Ліва сторона ротору)

(Права сторона ротору)



(Три ротора)

(Ротори в зібраному стані)

Таким чином працював поліалфавітний шифвр підстановки. Найпростішою версією поліалфавітного шифру є шифр Віженера.
Для того часу це досить криптографічно-стійкий шифр, якщо не знати ключового слова – його не розшифрувати.

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

(Квадрат Вінжера)

Як підбирався колектив дешифрувальників?

Керівником проекту був призначений ветеран військової розвідки Алістер Денністон. Роботу з дешифрування очолив колега Денністона по кімнаті №40, відомий лінгвіст і криптоаналітик Альфред Нокс. За загальну організацію роботи відповідав професор математики – Гордон Уелчман. Денністон почав набирати штат криптоаналітиків за принципом розумових здібностей: лінгвістів, математиків, шахістів, чемпіонів за рішенням кросвордів, єгиптологів і навіть палеонтологів. Зокрема, одним з перших був прийнятий відомий шаховий майстер Стюарт Мілнер Беррі. Серед математиків був і молодий професор логіки з Кембріджа – Алан Тьюрінг.

Кімната №40

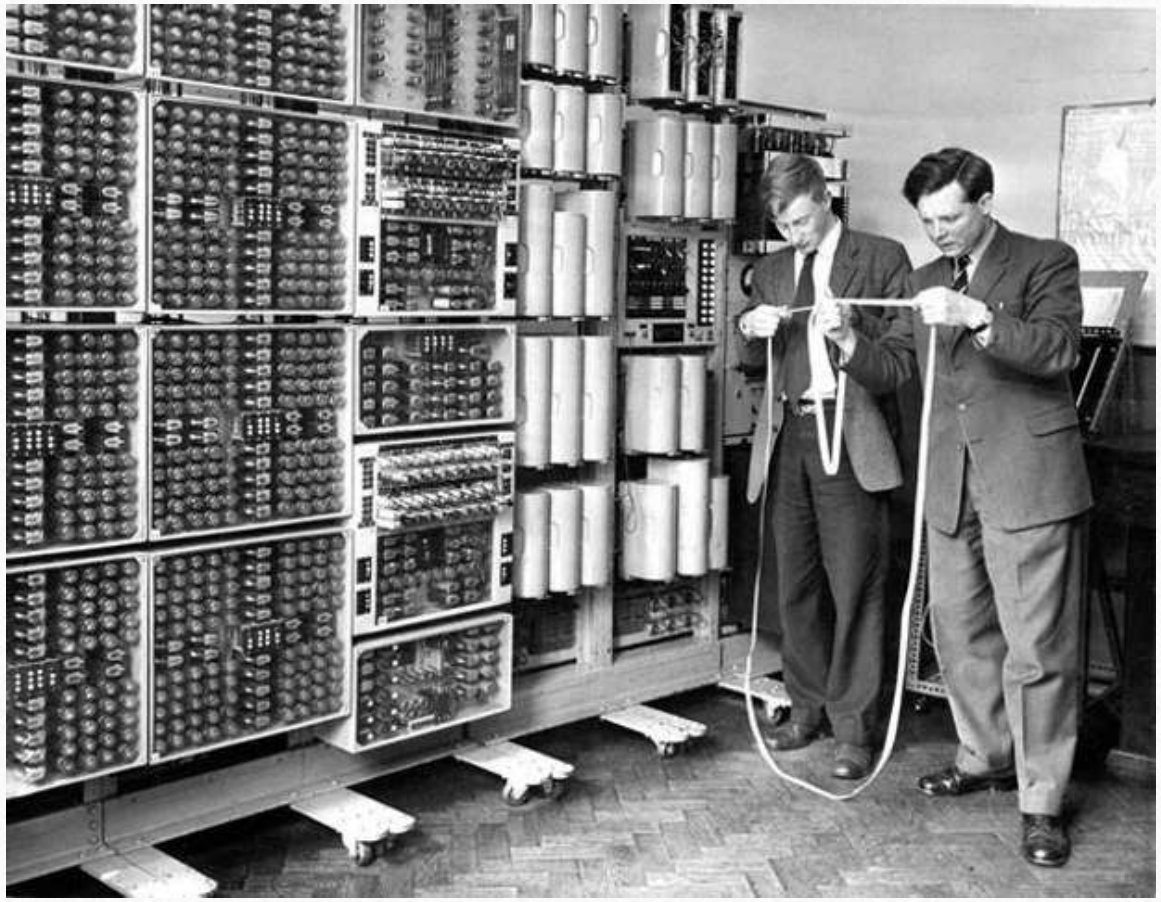
Чому саме Алану Тьюрінгу доручили розшифрування?

Одним з основних теоретиків Блетлі-парку був Алан Тьюрінг. Після вивчення польских матеріалів Тьюрінг прийшов до висновку, що використовувати колишній підхід з повним перебором повідомлень вже не вийде. По-перше, це поведе за собою створення більше 30 машин польського типу, що у багато разів перевищувало річний бюджет «STATION X», по-друге, можна очікувати, що Німеччина може виправити конструктивний недолік, на якому грунтувався польский метод.

Тому він розробив власний метод, заснований на переборі послідовностей символів вхідного тексту. Незабаром німці додали в конструкцію Енігми комутуючі пристрої, істотно розширивши цим кількість варіантів коду. Цю ситуацію для англійців вирішив Гордон Уелчман, запропонувавши конструкцію «діагональної дошки». В результаті цієї роботи в серпні 1940 року була побудована криптоаналітична машина Bombe. Згодом в Блетлі – парку було встановлено понад 200 машин , що дозволило довести темп розшифровки до двох-трьох тисяч повідомлень в день. Передбачається, що ці знання зіграли важливу роль в ключових битвах. На думку багатьох експертів, винахід Алана Тьюрінга дозволив скоротити війну на два роки.

Що допомогло остаточному рішенню проблеми дешифрування?

Точно управляти машиною Тьюрінга міг тільки сам Алан Тьюрінг, інші люди не могли зрозуміти логіки , на якій базується робота цієї машини. Але пізніше замість того, щоб вгадувати ключ, Bombe використовувала логіку, щоб відхилити певні можливості.



Як сказав Артур Конан Дойл: «Коли виключили неможливе, все, що залишається, яким би неймовірним воно не було, має бути правдою». Цей метод, хоча і був успішним, все ж надавав цілий ряд можливих правильних відповідей для налаштувань німецького кільця. Тому необхідно було виконати додаткову роботу, щоб звузити його до правильного. За допомогою перевірочної машини процес повторювався до тих пір, поки не була знайдена правильна відповідь. Це дало хакерам частину ключа, але не весь. Потім доводилося використовувати отримані знання і з'ясовувати іншу частину ключа. Після того, як код зламувався, команда Тьюрінга встановлювала машину Enigma з правильним ключем дня і розшифровували кожне повідомлення, перехоплене в той день.

Який був ефект появи механізму дешифрування?

У числі отриманої Великобританією інформації були і відомості про підготовку вторгнення в СРСР. Незважаючи на ризик розкриття джерела, відомості були передані радянському уряду. Однак Сталін вимагав, щоб інформація походила від трьох незалежних джерел. Незважаючи на побоювання про можливість Німеччини слухати радянські радіопереговори 24 липня 1941 року Черчилль розпорядився все-таки ділитися з СРСР інформацією, одержаної в результаті операції «Ультра», за умови повного виключення ризику компрометації джерела. Після війни машина Тьюрінга була повністю знищена, відновити машину намагалися, але існує тепер вона в невеликих екземплярах і тільки у проекті.

МАШИНА ТЬЮРІНГА

Під час Другої світової війни в Англії для розшифровки повідомлень, зашифрованих за допомогою «Енігми», була створена машина з назвою «Turing Bombe», яка справила неабияку допомогу антигітлерівської коаліції. Даний агрегат працює із стрічкою, яка складається із комірок, в яких записані символи, а також дана машина має голівку для запису та читання символів із комірок, яка може рухатись вздовж стрічки. На кожному кроці машина зчитує символ із комірки, на яку вказує голівка і на основі цього символу робиться наступний крок. Алан Тьюрінг переконливо показав розмаїтість можливостей запропонованої ним конструкції: всякий алгоритм може бути реалізований машиною Тьюрінга(основна гіпотеза теорії алгоритмів).

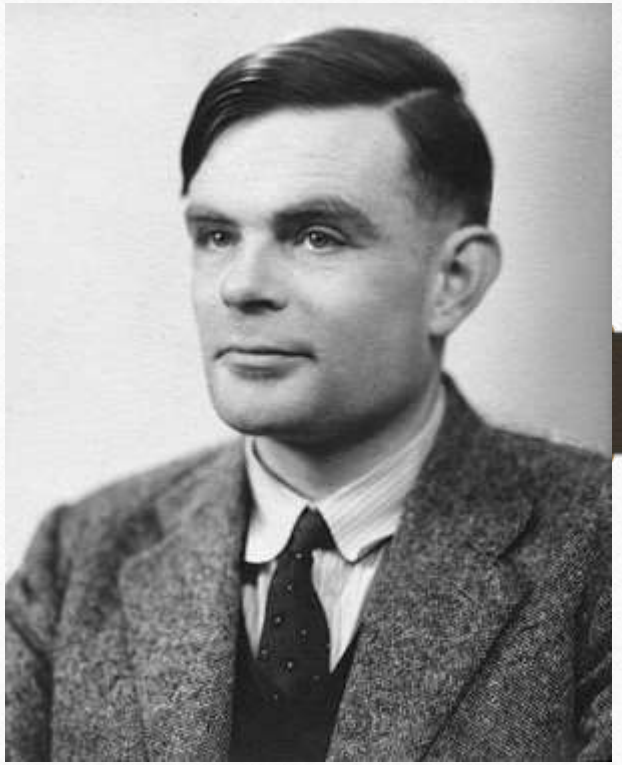
(Машина Тьюрінга)

Розшифрувати повідомлення «Енігми» можливо у випадку, якщо відомо положення роторів. Машина Алана Тьюрінга повторює дії декілької з’єднаних разом машин «Енігма». На початку 1940 року машина Тьюрінга вже дозволяла читати повідомлення «Люфтваффе», через півроку вдалося зламати і «Крігсмаріне», машина Тьюрінга використовувалася до кінця війні, допомагаючи союзникам у війні. На відміну від роторів «Енігми» , машина Тюрінга мала барабани з вхідними і вихідними контактами. Такчим чином вони можуть бути з’єднані послідовно. Кожен такий барабан мав по 104 дротяні щітки, які торкалися пластин, на які вони були завантажені. Щітки і відповідний набір контактів на пластині були організовані в чотирьох концентричних колах із двадцяти шести. Зовнішня пара кіл була еквівалентна струму, що проходив через «Енігму» в одному напрямку, в той час як внутрішня пара була еквівалентна струму, що проходить у протилежному напрямку.

БАТЬКО КОМП’ЮТЕРА. АЛАН ТЬЮРІНГ.

ЖИТТЯ ПІСЛЯ ВІЙНИ

Після війни в 1945 році Алан Тьюрінг очолив проект створення комп’ютера Automatic Computing Engine , а в 1948 році став співпрацювати з Manchester Automatic DigitAl Machine – комп’ютер, який мав найбільшу пам’ять у світі на той час. Роботи А.Тьюрінга з ЕОМ і розвитку програмування мали неоціненну важливість і дали основу більшості досліджень у галузі штучного інтелекту. Його думка – комп’ютер зможе мислити, як і людина. 8 Червная 1954 Алана Тьюрінга знайшли мертвим у його квартирі(отруєння ціанідом), на тумбі було знайдено надкушене яблуко(ймовірно Тьюрінга отруївся, бо полюбляв досліджувати різні хімічні речовини, які брав з популярних продуктів), за деякими даними надкушене яблуко стало логотипом компанії Apple, проте біографія Стіва Джобса спростовую цю теорію. Алана Тьюрінга переслідували у підозрі за гомосексуальність, але його помилували 24 грудня 2013 року посмертно



(Алан Тьюрінг)

ЦІКАВІ ФАКТИ ПРО АЛАНА ТЬЮРІНГА

- **Умів в’язат**и і в воєнні роки сам собі в’язав рукавиці.
- **Був аллергиком**. В період цвітіння рослин він не приймав антигістамінні препарати, а одягав протигаз.
- **Ніколи не був одружений**. Але був заручений з Джоан Кларк, з якою разом працював над зломом «Енігми». Про свої нетрадиційні захоплення сказав їй через пару днів після заручин. Але її це не відлякало. Їх пов’язувала платонічна любов і духовні зв’язки. Але незабаром вони розійшлися. Трохи пізніше Тьюрінг запропонував Джоан почати все спочатку, але жінка відмовилася. Незважаючи на те, що вона вийшла заміж за іншу людину, з Аланом вона була до самого кінця, залишаючись з ним в теплих, дружніх видносинах
- **Був хорошим спортсменом** і **брав участь в марафонському забігу**

А. Тьюрінг – біжить марафонську дистанцію в 1946 р.

Алана багато хто вважав невиправним диваком. На початку літа він добирався до роботи на велосипеді з протигазом на обличчі. Велисопед періодично ламався, у нього спадав ланцюг. Будь-яка розсудлива людина віднесла б його в ремонт, але тільки не Алан. Він прорахував скільки оборотів робить велосипед, перш, ніж ланцюг спаде, і зупинявся перед цим, щоб поправити його.

КІНЕМАТОГРАФ

У кінематографі. Є чудовий фільм, який показує про тріумф Алана Тьюрінга і його команди спеціалістів – дешифрувальників. Фільм має назву «Гра в імітацію» - це американський історичний трилер 2014 року про британского математика та батька інформатики «Алана Тьюрінга». Світова прем'єра відбулася у серпні 2014 року. У фільмі йдеться не тільки про тріумф Тьюрінга, а й про його життя(переслідування, останні роки, друзів і т.д).

(Фільм «Гра в імітацію»)