Alan Turing et le décryptage des codes secrets nazis

10.05.2012, par

Charline Zeitoun

Mis à jour le 06.06.2014

Les Nazis codaient leurs messages avec des machines qui échangeaient les lettres tapées sur le clavier. Le modèle utilisé par la marine fut craqué dès 1942 par les Anglais avec l'aide d'Alan Turing

Le débarquement du 6 juin 1944 n'aurait peut-être pas eu lieu sans le mathématicien Alan Turing. Celui-ci a en effet joué un rôle déterminant pour briser le code secret de la marine allemande. Explications avec **François Morain,** *du Laboratoire d'informatique de l'École polytechnique.*

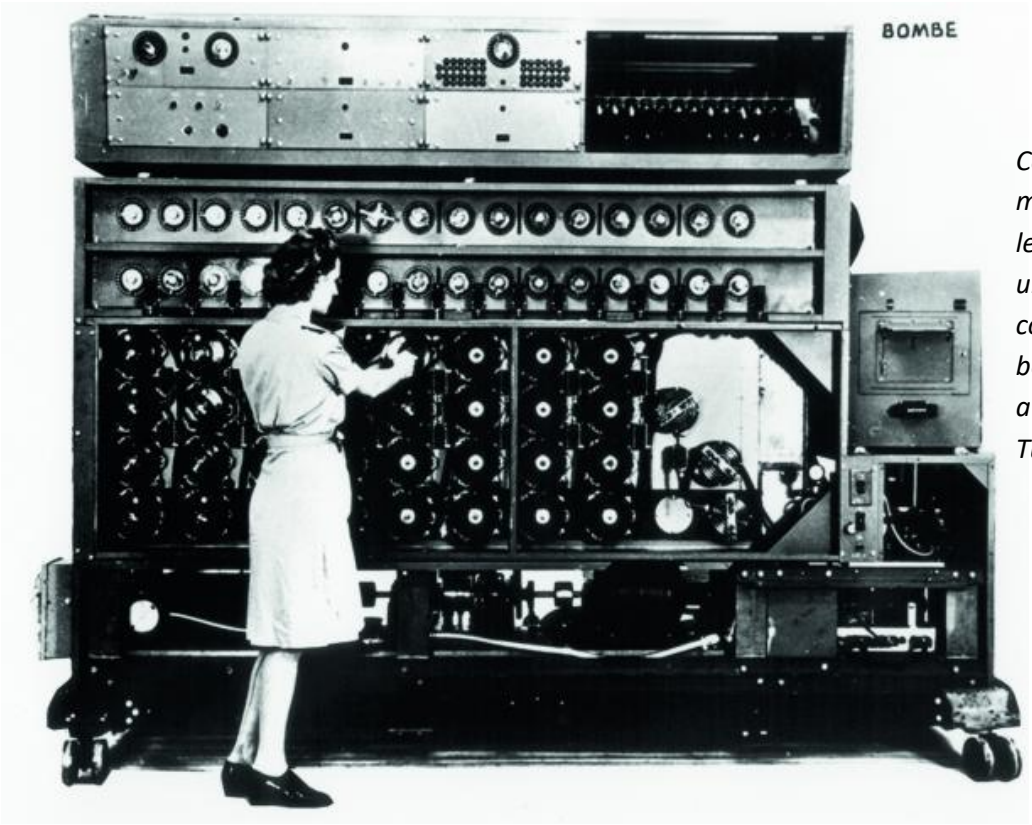
❖

En septembre 1939, Alan Turing rejoint le manoir de Bletchley Park, quartier général des services de renseignement britannique, pour briser le système de cryptage des sous-marins allemands, réputé inviolable. Il y parvient avec ses collègues dès 1942, contribuant à éviter l'invasion de l'Angleterre.
Comment ont-ils fait ?

François Morain: Bletchley Park était une usine à décrypter dans laquelle la quasi-totalité des mathématiciens de Cambridge et d'Oxford s'étaient enrôlés, travaillant dans des baraquements et faisant les trois-huit. Les réflexions de Turing sur le calcul le plaçaient en première ligne pour participer à cette entreprise. La marine allemande utilisait une machine à crypter, Enigma. Il s'agissait d'une version ultrasophistiquée d'autres modèles allemands du même nom, employés par les armées de terre et de l'air, et déjà étudiés par les services de renseignement polonais. Ces derniers avaient en effet construit des "bombes", machines qui permettaient de tester toutes les clés de chiffrement possibles dans un minimum de temps. Faire vite était indispensable, car la clé changeait tous les jours.

Turing n'a-t-il fait qu'utiliser les bombes conçues et construites par les Polonais ?

F. M. : Non, les bombes des Polonais ne permettaient de casser que les premières versions d'Enigma. Turing a participé à la construction de bombes adaptées à la version utilisée par la marine. Surtout, il a exploité différentes faiblesses dans la façon dont les Allemands utilisaient leur système de codage. Ils commençaient, par exemple, leurs messages par des formules de politesse assez convenues, de type *Herr Kommandant,* faciles à deviner. Tout comme les messages très courts et stéréotypés qu'ils envoyaient régulièrement pour donner la météo ou annoncer qu'il ne se passait rien. En cryptanalyse, justement, on cherche souvent d'abord à deviner ce que des mots veulent dire et ensuite on teste si la clé de chiffrement ainsi définie fonctionne sur l'ensemble du ou des messages. C'est dans cette approche déductive que Turing a fait preuve d'une grande intuition pour réduire le nombre de combinaisons à tester. C'est là que résident la prouesse et l'intelligence.



Cette « bombe », machine pour décrypter les messages codés, est un modèle de l'US Navy construite d'après les « bombes » anglaises, avec l'aide d'Alan Turing.

Que peut-on dire de l'apport de Turing à la cryptographie ?

F. M. : Peu de choses en réalité. Ses travaux n'ont jamais fait l'objet de publications scientifiques. On ne dispose que de son carnet de laboratoire, inaccessible jusqu'en 1996 à cause du secret militaire, et qui n'a pas été rédigé de manière scientifique. Il y consigne tout ce qu'il sait, mais on ignore la part entre ses propres réflexions et les informations glanées auprès des autres scientifiques et agents des services secrets. Ensuite, il faut bien comprendre la distinction entre la cryptographie, science du chiffrement qui nécessite la production d'algorithmes et de théories, et la cryptanalyse, qui consiste à casser un code secret. Il n'y a pas de théorie du cassage. Il s'agit essentiellement d'avoir l'intelligence et l'astuce d'exploiter les faiblesses d'un système ou de son utilisation par les opérateurs humains. Quoi qu'il en soit, la façon dont Turing y est parvenu à l'époque, sans ordinateur, reste un immense tour de force et fait partie de la mythologie de la discipline.

1- A ton tour, comme Alan Turing et son équipe, essaye de décrypter les messages secrets suivants.

Message 1 :

14	15	21	19		1	22	15	14	19				
3	15	13	13	5	14	3	5		1				
16	18	15	7	18	1	13	13	5	18				
14	15	20	18	5		8	9	19	20	15	9	18	5
19	21	18		20	1	2	12	5	20	20	5		

Quelle est la clé de cryptage utilisée ?

Message 2 :

T	D	S	B	U	D	I		K	V	O	J	P	S
F	T	U		V	O	F							
B	Q	Q	M	J	D	B	U	J	P	O			
Q	P	V	S		U	B	C	M	F	U	U	F	

Quelle est la clé de cryptage utilisée ?

2- Trouve une nouvelle clé de cryptage pour coder le message suivant :

Thymio est un robot programmable.

T	H	Y	M	I	O		E	S	T		U	N	
R	O	B	O	T									
P	R	O	G	R	A	M	M	A	B	L	E		

1- A ton tour, comme Alan Turing et son équipe, essaye de décrypter les messages secrets suivants. *CORRECTION*

Message 1 :

14	15	21	19		1	22	15	14	19				
N	O	U	S		A	V	O	N	S				
3	15	13	13	5	14	3	5		1				
C	O	M	M	E	N	C	E		A				
16	18	15	7	18	1	13	13	5	18				
P	R	O	G	R	A	M	M	E	R				
14	15	20	18	5		8	9	19	20	15	9	18	5
N	O	T	R	E		H	I	S	T	O	I	R	E
19	21	18		20	1	2	12	5	20	20	5		
S	U	R		T	A	B	L	E	T	T	E		

Quelle est la clé de cryptage utilisée ?

Les lettres sont remplacées par le nombre qui correspond à leur place dans l'alphabet.

Message 2 :

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

Quelle est la clé de cryptage utilisée ?

Chaque lettre est remplacée par la lettre qui la suit dans l'alphabet.

2- Trouve une nouvelle clé de cryptage pour coder le message suivant :

Thymio est un robot programmable.

T	H	Y	M	I	O		E	S	T		U	N	
R	O	B	O	T									
P	R	O	G	R	A	M	M	A	B	L	E		