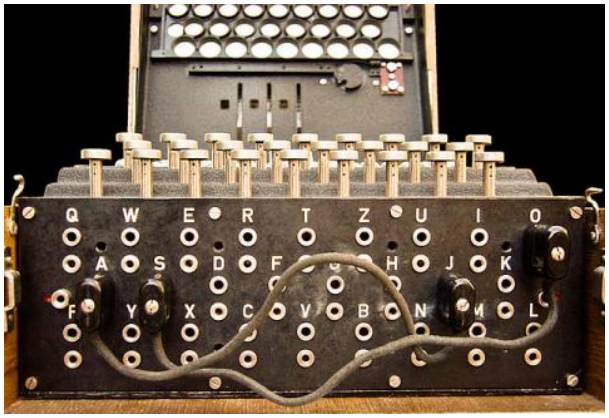
ALAN TURING TACKLES DOLPHIN - GERMANY'S NAVAL ENIGMA CODE



The Enigma system used by Germany's naval forces (the *Kriegsmarine*), during World War II, was more complicated than the system used by Germany's air force (the *Lufftwaffe*). One of the things which made the naval code more complicated was the use of a plugboard (*Steckerbrett*), at the front of the machine (below its keyboards). In this image, we see two pairs of swapped plugboard letters (S↔O and A↔J). Photo by Bob Lord; license CC BY-SA 3.0.

Every Morse Code message could be intercepted, during World War II, but not every Morse Code message could be understood. That was particularly true of Morse-Code messages transmitted by Germany's navy.

German code transmitters sent messages which only the Enigma operator would know. The operator was told to think about three opening letters; then type up three more for the content of the message. On the surface, this might seem foolproof given the formidable odds against breaking Enigma-sent messages.

But ... a built-in weakness, of this approach to message-sending, was allowing the operator to select the three random letters. Human beings are not random. Code breakers can anticipate. Sometimes an operator used a girlfriend's name as his random letters. Sometimes operators used actor names - like Tom Nix.

By believing that Enigma was completely unbreakable, the Germans duped themselves into thinking that no one could ever figure it out. But Station X code breakers were able to second- guess names of people. If they were able to second-guess any part of a transmitted dispatch, they were closer to deciphering the whole message.

Sometimes, according to Station-X code breaker Mavis Batey, Enigma operators used "dirty words" as part of their outgoing codes. She later recalled that she'd read so many "dirty-word encoded messages" that she (in her own mind) became an expert in such words.

Still ... without more to help them than second-guessing the work of a German Enigma operator, code breakers at Bletchley Park endured frustrating hours and weeks of unproductive work.

Despite the odds again them, Station X was making steady progress. To use an oft-repeated adage, Alan Turing was "the right man, in the right place, at the right time."

He was, by all accounts, a genius who was without peers. According to a Station X code breaker, Professor Peter Hilton, Turing came up with ideas which other highly intelligent people had never considered.

To the people working with him, Turing was in a class totally by himself. The originality of his thinking was, according to Hilton, "marvelous."

At the age of 23, Turing was a Cambridge professor. According to those who knew him, he had the most

brilliant mind of his generation. Working at BP suited him well. His work on intelligence machines was years ahead of his time.

Andrew Hodges, Turing's biographer, describes this eccentric genius:

> *He had funny manners. He didn't like wearing a tie. He always looked untidy. But he quite liked being out in the country where he could cycle around. He'd cycle with a gas mask on, during hay-fever period. He didn't care what he looked like. He just thought that the job is what mattered.*

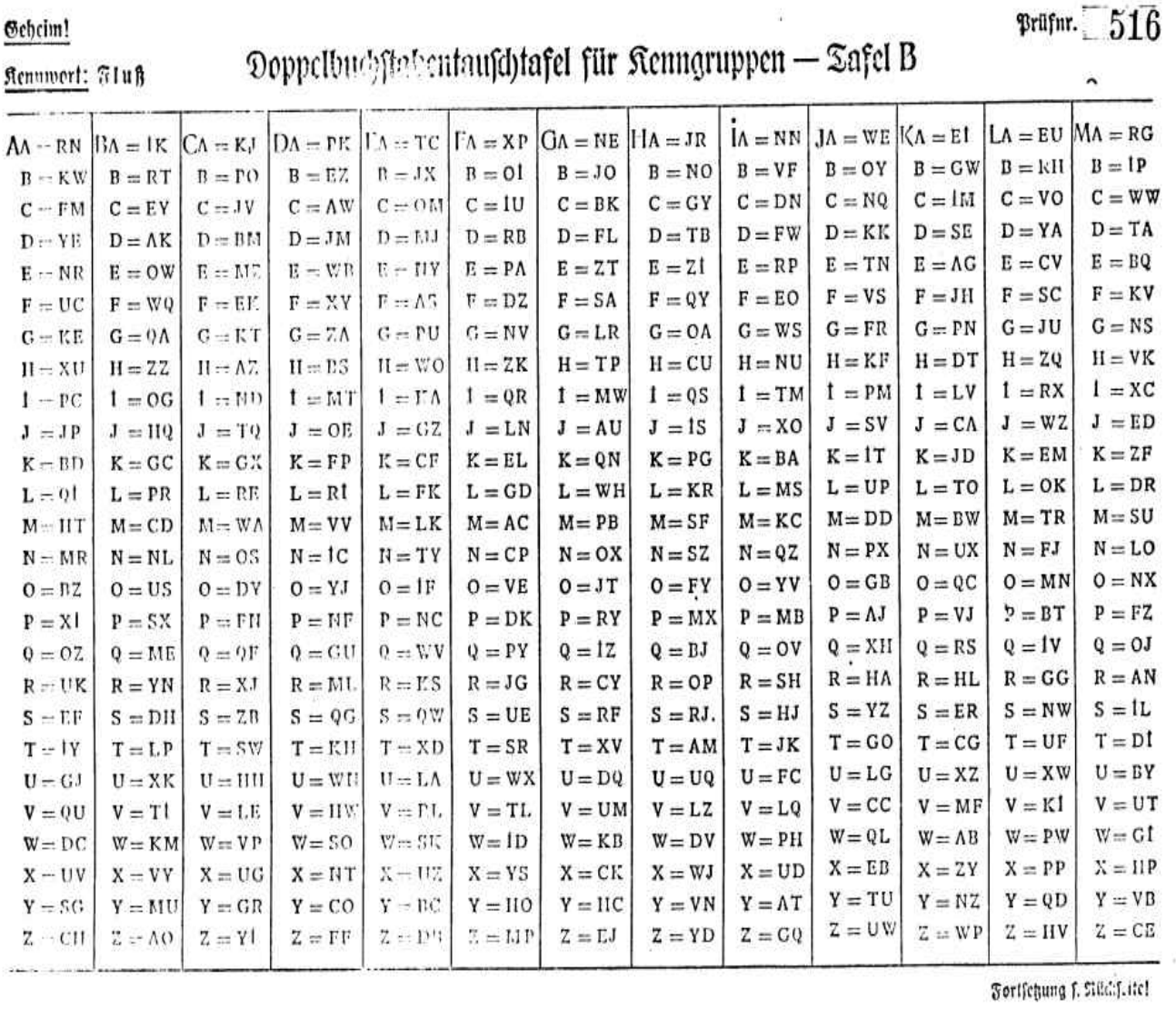
According to one of his female colleagues, Sarah Baring, Turing didn't really know much about young women. She once offered him a cup of tea, and:

> *...he shrank back as if he was going to be shot. And he used to, bless his heart, walk down to the canteen in a curious sideways motion, with his head down. But he was such a star. We all thought he was the best wonderful thing.*

Turing set himself the challenge of breaking the Naval Enigma. In an attic room at the old Bletchley Park mansion, initially working alone, he began to unravel its secrets. All he had to go on were the scrambled letters of U-boat messages.

Incredibly, as he studied them, he was able to discover how the Germans were hiding the key message setting. Unlike the Luftwaffe, the German Navy left nothing to chance. The naval message operator had to get his settings from a code book, not select three letters at random.

With practically nothing to go on, Turing discovered how the Navy operators selected their keys from a list for each day. He rightly guessed that to hide the key, these letters were encoded using secret tables. Instead of substituting one letter for another, the tables used pairs of letters. He referred to those pairs of letters as "bigrams." The Germans called them *Doppelbuchstabentauschtafel* ("double-letter conversion table").



Geheim! Prüfnr. 516

Kennwort: Fluß

Doppelbuchstabentauschtafel für Kenngruppen — Tafel B

AA = RN	BA = IK	CA = KJ	DA = PK	EA = TC	FA = XP	GA = NE	HA = JR	IA = NN	JA = WE	KA = EI	LA = EU	MA = RG
B = KW	B = RT	B = PO	B = EZ	B = JX	B = OI	B = JO	B = NO	B = VF	B = OY	B = GW	B = KH	B = IP
C = FM	C = EY	C = JV	C = AW	C = OM	C = IU	C = BK	C = GY	C = DN	C = NQ	C = IM	C = VO	C = WW
D = YE	D = AK	D = BM	D = JM	D = MJ	D = RB	D = FL	D = TB	D = FW	D = KK	D = SE	D = YA	D = TA
E = NR	E = OW	E = MZ	E = WB	E = HY	E = PA	E = ZT	E = ZI	E = RP	E = TN	E = AG	E = CV	E = BQ
F = UC	F = WQ	F = EK	F = XY	F = AS	F = DZ	F = SA	F = QY	F = EO	F = VS	F = JH	F = SC	F = KV
G = KE	G = QA	G = KT	G = ZA	G = PU	G = NV	G = LR	G = OA	G = WS	G = FR	G = PN	G = JU	G = NS
H = XU	H = ZZ	H = AZ	H = BS	H = WO	H = ZK	H = TP	H = CU	H = NU	H = KF	H = DT	H = ZQ	H = VK
I = PC	I = OG	I = ND	I = MT	I = FA	I = QR	I = MW	I = QS	I = TM	I = PM	I = LV	I = RX	I = XC
J = JP	J = HQ	J = TQ	J = OE	J = GZ	J = LN	J = AU	J = IS	J = XO	J = SV	J = CA	J = WZ	J = ED
K = BD	K = GC	K = GX	K = FP	K = CF	K = EL	K = QN	K = PG	K = BA	K = IT	K = JD	K = EM	K = ZF
L = QI	L = PR	L = RE	L = RI	L = FK	L = GD	L = WH	L = KR	L = MS	L = UP	L = TO	L = OK	L = DR
M = HT	M = CD	M = WA	M = VV	M = LK	M = AC	M = PB	M = SF	M = KC	M = DD	M = BW	M = TR	M = SU
N = MR	N = NL	N = OS	N = IC	N = TY	N = CP	N = OX	N = SZ	N = QZ	N = PX	N = UX	N = FJ	N = LO
O = BZ	O = US	O = DY	O = YJ	O = IF	O = VE	O = JT	O = FY	O = YV	O = GB	O = QC	O = MN	O = NX
P = XI	P = SX	P = FH	P = NF	P = NC	P = DK	P = RY	P = MX	P = MB	P = AJ	P = VJ	P = BT	P = FZ
Q = OZ	Q = ME	Q = QF	Q = GU	Q = WV	Q = PY	Q = IZ	Q = BJ	Q = OV	Q = XH	Q = RS	Q = IV	Q = OJ
R = UK	R = YN	R = XJ	R = ML	R = ES	R = JG	R = CY	R = OP	R = SH	R = HA	R = HL	R = GG	R = AN
S = EF	S = DH	S = ZB	S = QG	S = QW	S = UE	S = RF	S = RJ.	S = HJ	S = YZ	S = ER	S = NW	S = IL
T = IY	T = LP	T = SW	T = KH	T = XD	T = SR	T = XV	T = AM	T = JK	T = GO	T = CG	T = UF	T = DI
U = GJ	U = XK	U = HH	U = WH	U = LA	U = WX	U = DQ	U = UQ	U = FC	U = LG	U = XZ	U = XW	U = BY
V = QU	V = TI	V = LE	V = HW	V = DL	V = TL	V = UM	V = LZ	V = LQ	V = CC	V = MF	V = KI	V = UT
W = DC	W = KM	W = VP	W = SO	W = SK	W = ID	W = KB	W = DV	W = PH	W = QL	W = AB	W = PW	W = GI
X = UV	X = VY	X = UG	X = NT	X = UZ	X = YS	X = CK	X = WJ	X = UD	X = EB	X = ZY	X = PP	X = HP
Y = SG	Y = MU	Y = GR	Y = CO	Y = BC	Y = HO	Y = HC	Y = VN	Y = AT	Y = TU	Y = NZ	Y = QD	Y = VB
Z = CH	Z = AO	Z = YI	Z = FF	Z = DP	Z = MP	Z = EJ	Z = YD	Z = GQ	Z = UW	Z = WP	Z = HV	Z = CE

Fortsetzung s. Stück s. titel

Turing was making great progress, toward cracking the German Navy's Enigma code, but he needed to get the bigram tables which U-boat crews used before he could actually decipher the messages. He needed to see the paired tables.

He had a stroke of good fortune when U-110 got into trouble.

See Alignments to State and Common Core standards for this story online at:
http://www.awesomestories.com/asset/AcademicAlignment/ALAN-TURING-TACKLES-DOLPHIN-GERMANY-S-NAVAL-ENIGMA-CODE-The-Imitation-Game

See Learning Tasks for this story online at:
http://www.awesomestories.com/asset/AcademicActivities/ALAN-TURING-TACKLES-DOLPHIN-GERMANY-S-NAVAL-ENIGMA-CODE-The-Imitation-Game

Questions 2 Ponder

When Is a Number Computable?

When he was a university student, Alan Turing wrote a paper foreseeing computers when no one used computers. What did Turing mean when he said that "a number is computable if its decimal can be written down by a machine?"

How Do We Identify Genius?

As a student, Alan Turing envisioned something which did not seem possible to others and was undeterred when others did not understand his vision.

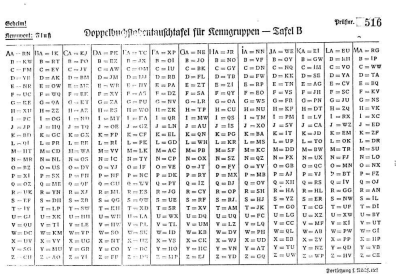
Turing, in other words, dared to be different. He dared to think differently.

Then ... despite whatever anyone else thought ... Turing followed-through. Acting on his own intuition, he changed not just the progress of WWII but also the future of computing. He accomplished what did not seem possible—at all—to others.

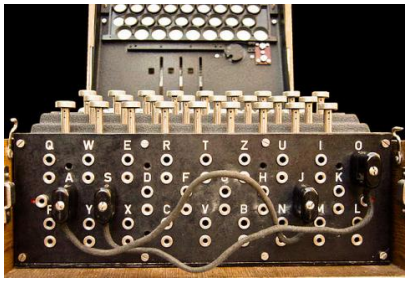
Can you think of anyone alive today who has accomplished—or is capable of accomplishing—a similar feat? What do Turing and that individual have in common?

Have you ever been in a situation where you saw things differently? Were you able to speak your mind? If so, how did your friends react?

Media Stream



Enigma Bigram
View this asset at: http://www.awesomestories.com/asset/view/



ALAN TURING TACKLES DOLPHIN - GERMANY'S NAVAL ENIGMA CODE
View this asset at: http://www.awesomestories.com/asset/view/