Break of Enigma messages AWTZK (Nr. 187) and ZNLZT (Nr. 189), 11 July 1941

26 September 2026 · John Woodhouse

Two of the Heeresgruppe Nord messages listed as unbroken on Frode Weierud's CryptoCellar are broken: both were enciphered on the same daily key of 11 July 1941, reconstructed here as UKW B, wheel order I-IV-III, rings EXS, Stecker AO BF CQ DH EW GJ KX NU PY RT.

Result

Both messages came from call sign uyo and were received at the Ib (quartermaster) station on 11 July 1941; both decrypt on one key.

Message	Filed / received	Letters	Indicator	Message key	Stop
Nr. 187 AWTZK	1800 / 1827	49	DUJ GEH	ERT	ETQ
Nr. 189 ZNLZT	1910 / 2025	69 (1 lost in reception)	ZZD LRD	NML	NPC

Message	Plaintext (emended)	Translation
Nr. 187 AWTZK	WO BLEIBT ROEM EINS BERTA FRAGE X BISHER NIQT EINGETROFFEN	Where is Ib? Has not arrived so far.
Nr. 189 ZNLZT	EINS DREI X SIEBEN X ZWO TAGESS[AETZE?] ARM X VERPFL X LAGER OSTROW X OSTROW X EMPFANGEN	For 13 July: two days' rations to be collected at the Army rations depot, Ostrov.

Machine configuration (key of 11 July 1941)

Army Enigma I, three wheels, standard wiring. Wheels are listed left to right; ring settings as letters and numbers (A = 01).

Setting	Value
Machine	Enigma I (Wehrmacht), 3 rotors
Reflector (Umkehrwalze)	B
Wheel order (Walzenlage)	I – IV – III (left, middle, right); CryptoCellar notation 143
Ring settings (Ringstellung)	E – X – S (05 – 24 – 19)
Plugboard (Steckerverbindungen)	AO BF CQ DH EW GJ KX NU PY RT
Key-sheet line	B143 exs AO BF CQ DH EW GJ KX NU PY RT

The wheel order does not share a slot with the published keys of the neighbouring days (10 July: V–II–I, 12 July: II–V–IV), as the 1941 key sheets require. The 11 July key sheet itself has never been published or found; this key is a reconstruction from the two messages.

Verify it yourself

Any correct Enigma I simulator with double stepping reproduces the decrypts below (checked with the independent `py-enigma` package and this project's own machine).

1. Set up the machine with the configuration above.
2. Recover the message key (1940–43 Army procedure): set the windows to the Grundstellung (first indicator group), type the second group; the output is the message key.
3. Set the windows to the message key and type the ciphertext. The first group on the form (the Kenngruppe AWTZK / ZNLZT) is not ciphertext and is left out.

	AWTZK (Nr. 187)	**ZNLZT (Nr. 189)**
Grundstellung, typed	`DUJ, GEH`	`ZZD, LRD`
Message key (output)	`ERT`	`NML`
Ciphertext	`TBXVA KXKLZ IPPCZ IPUCC RXHRK QUTDE GMGIK GCWEK LQNUM CWSS`	`KCBDB JDLAV PWLLU TSSHB WEYOW SQNB- NORNK DTZJH PQFYA XCQQY FLSSK DZCGL SWYMB QBMF`
Raw decrypt	`WEBLE IBTRO EMEIN SBEWX AFRAG EXBIS HEPNI QGEIN GRTRO WFTI`	`EWNSD REIIS CETEN XZWYT AGESS VYHG? QRMXV ERPFL XLAGE ROSTR OWXOS TROWX EMPFA VGEN`
Window after the last letter	`ETQ`	`NPC`

ZNLZT's 30th letter (the `-` in group 6) was lost in reception; the machine still stepped for it. In a simulator, type any letter there (e.g. X) and ignore its output (shown as `?` above); every later letter then decrypts as listed.

The same run in Python (`pip install py-enigma`):

```
from enigma.machine import EnigmaMachine

def machine():
    return EnigmaMachine.from_key_sheet(
        rotors="I IV III", reflector="B", ring_settings="E X S",
        plugboard_settings="AO BF CQ DH EW GJ KX NU PY RT")

MESSAGES = (
    ("DUJ", "GEH", "TBXVAKXKLZIPPCZIPUCCRXHRKQUTDEGMGIKGCWEKLQNUMCWSS"),
    ("ZZD", "LRD", "KCBDBJDLAVPWLLUTSSHBWEYOWSQNBXNORNKDTZJHPQFYAXCQQY"
                   "FLSSKDZCGLSWYMBQBMF"),
)
for grund, enc, ct in MESSAGES:
    m = machine(); m.set_display(grund)
    key = m.process_text(enc)              # message key
    m = machine(); m.set_display(key)
    print(key, m.process_text(ct))
```

In CyberChef's Enigma operation: 3-rotor; left rotor I, ring E, initial N (or E for AWTZK); middle rotor IV, ring X, initial M (R); right rotor III, ring S, initial L (T); reflector B; plugboard `AO BF CQ DH EW GJ KX NU PY RT`. The initial values are the message keys NML and ERT.

Plaintexts

Both are received copies, so they carry Morse reception errors; every emendation below is a single wrong cipher letter, listed with the letter that must have been sent. X = word separator, Q = CH, ROEM EINS BERTA = Ib (quartermaster), FRAGE = question mark.

AWTZK (Nr. 187), 49 letters

9 of 49 letters garbled; 8 are one-symbol Morse slips.

```
raw      WEBLEIBTROEMEINSBEWXAFRAGEXBISHEPNIQGEINGRTROWFTI
emended  WOBLEIBTROEMEINSBERTAFRAGEXBISHERNIQTEINGETROFFEN
words    WO BLEIBT ROEM EINS BERTA FRAGE X BISHER NIQT EINGETROFFEN
```

Wo bleibt Ib? Bisher nicht eingetroffen. — "Where is Ib? Has not arrived so far."

Position	Received	Sent (needed)	Morse	Plaintext before → after
2	B	H	`-... → ....`	E → O
19	C	F	`-.-. → ..-.`	W → R
20	C	F	`-.-. → ..-.`	X → T
33	G	W	`--. → .-- (not one symbol; G/W misread)`	P → R
37	C	Y	`-.-. → -.--`	G → T
42	Q	O	`--.- → ---`	R → E
46	C	Y	`-.-. → -.--`	W → F
48	S	R	`... → .-.`	T → E
49	S	F	`... → ..-.`	I → N

Five of the nine are a received C: this operator's C was unreliable (group IPUCC was sent as IPUFF).

ZNLZT (Nr. 189), 69 letters

```
raw      EWNSDREIISCETENXZWYTAGESSVYHG?QRMXVERPFLXLAGEROSTROWXOSTROWXEMPFAVGEN
reading  EINSDREIXSIEBENXZWOTAGESS.....ARMXVERPFLXLAGEROSTROWXOSTROWXEMPFANGEN
words    EINS DREI X SIEBEN X ZWO TAGESS[AETZE?] ARM X VERPFL X LAGER OSTROW
         X OSTROW X EMPFANGEN
```

13.7. zwei Tages(sätze) Arm(ee)-Verpfl(egungs)lager Ostrow empfangen. — "For 13 July: two days' rations to be collected at the Army rations depot, Ostrov."

- 11 garbled letters of 68 received, 5 of them one-symbol Morse slips.
- Letters 1–25: 5 garbles; positions 11, 13 and 19 are Morse slips, positions 2 and 9 are not.
- Letters 26–31 surround the letter lost in reception (30): a burst of 5 errors (only 31 a Morse slip), so the word there is uncertain; TAGESSAETZE is the reading of the next day's message.
- Letters 32–69 read cleanly except one Morse slip at 66 (Q received, G sent: EMPFAVGEN → EMPFANGEN).

The text is the forerunner of the solved message Nr. 194 MAKJH of 12 July 1941 (another station): EINS DREI X SIEBEN X KOENNEN STATT ZWO TAGESSAETZE DREI ARMEE VERPFL LAGER X OSTROW X EMPFANGEN ("for 13 July, three days' rations instead of two can be collected at the Army rations depot, Ostrov").

Evidence that the break is correct

Four independent checks agree; a wrong key would have to pass all of them by chance.

1. **Readable far beyond the crib.** The key was found with the 15-letter crib XOSTROWXOSTROWX (ZNLZT letters 46–60). The other 54 letters read as German on the same subject as the next day's message Nr. 194.
2. **A second message, no fitting.** AWTZK was not used in the search. With the same Stecker and right ring, only its 17,576 start positions were tried; one of them gives the German text above.
3. **Both indicators, as written on the forms, give the same ring setting.** For each message, only one ring setting makes its indicator decipher to its start position (a wrong key matches about 1 time in 26), and both give EXS. Neither indicator needs any correction. AWTZK's message key ERT is a lazy keyboard key also used on 10 July (Nr. 162) and 9 September (Nr. 38).
4. **Unique.** A 31-letter crib from ZNLZT's readable text (XVERPFLXLAGEROSTROWXOSTROWXEMPF), tested against all 60 wheel orders, all start positions and right rings with no error tolerance, gives exactly one solution: this key.

Residual errors are explained as reception garbles (list above). The plugboard has the usual 10 pairs.

How it was broken

The decisive step was a crib mined from the published decrypts of the surrounding days, tested with a Bombe-style search that tolerates one garbled letter.

1. **Wheel-order restriction.** On the 1941 key sheets no wheel sits in the same slot on consecutive days (checked on every published pair of July days). With 10 July (V–II–I) and 12 July (II–V–IV) known, 14 of 60 wheel orders remain for 11 July.
2. **Failed first attempts.** A ciphertext-only hill-climbing sweep of ZNLZT over those 14 wheel orders (42,000 candidates, each cross-checked against AWTZK), and a second sweep of AWTZK assuming the operator had chained his indicators, found nothing. Calibration on solved messages showed why: for received messages of 50–70 letters the search rarely lands near the true plugboard.

Crib mining

A crib is a guessed piece of plaintext. Two sources supplied the candidates:

- **Repeated phrases.** All 77 solved decrypts on CryptoCellar with published keys were searched for phrases of 10–20 letters that recur in several messages: unit names, addresses and signatures.
- **Neighbouring traffic.** The solved messages of 7–14 July around the target date: headquarters and unit names, and place names along the front. Operators in this area wrote place names twice (OSTROW X OSTROW) to protect them against reception errors, which makes them long, reliable cribs.

Twelve cribs were fixed in writing before the first run, with the rule that only German readable well beyond the crib would count as a break:

	Crib	Len.	Source in the solved traffic	Result
P1	SIEGFRIEDSIEGFRIEDXTONIXDIV	27	SS-Totenkopf Division spelled with call words (13 July, Nr. 24/1, 24/2)	no break
P2	SIEGFRIEDSIEGFRIEDTONIXDIV	26	the same without X (13 July, Nr. 25)	no break
P3	XFUENFSEQSXARMXKORPSX	21	LVI Army Corps (7 July Nr. 18; 13 July Nr. 24/1)	no break
P4	XOPOTSCHKAXOPOTSCHKAX	21	doubled place name, 7–10 July (Nr. 20/1, 23, 139, 161)	no break
P5	XOSTROWXOSTROWX	15	doubled place name, 10–14 July (Nr. 161, 168, 194, 203)	**break (ZNLZT)**
P6	XROSENOWROSENOWX	16	doubled place name, 10 July (Nr. 172, 173)	not needed
P7	XPORCHOWXPORCHOW	16	doubled place name, 13 July (Nr. 197, 200, 201)	not needed
P8	ANROEMEINSBERTAX	16	address “to Ib”, tested at the start only (Nr. 70, 203)	not needed
P9	XROEMXEINSANTON	15	signature “Ia”, tested at the end only (Nr. 23, 143)	not needed
P10	XQUARTIERMEISTERX	17	quartermaster (Nr. 30, 203)	not needed
P11	ANXPANZXGRUPPEXVIERX	20	address “to Panzer Group 4”, start only (13 July, Nr. 25)	not needed
P12	SIEGFRIEDSIEGFRIED	18	division name with other continuations	not needed

Crib campaign

- **What one test does.** The crib is placed at one position in the ciphertext. For every setting of the restricted key space (14 wheel orders × 456,976 combinations of start position and right ring), its letter pairs serve as a menu from which the plugboard is deduced, as on the British Bombe. A setting that yields a consistent plugboard is a stop; one crib letter may be a reception error. Every stop is completed to a full decrypt and read.
- **Run order.** The cribs ran in table order. P1–P4 were tested on both messages; no completion kept more than half of its crib, and none read as German.
- **The hit.** P5 on ZNLZT gave 1,074,285 stops over its 55 positions. One of them, with the crib at letter 46, kept 14 of the 15 crib letters and decrypted the rest of the message into German on the same subject as message Nr. 194.

Confirmation

The checks in “Evidence that the break is correct” above, and an independent re-decryption with the `py-enigma` package.

GPU time on one RTX 3080: about 1 hour for the unsuccessful sweeps and pair checks, and 44 minutes for the crib campaign (26 September 2026, 20:17–21:01), including the confirming uniqueness test. Tools: this project's `enigmabreak` toolkit (Python, Numba CUDA).

Sources and credits

The messages, message forms, published keys and solved decrypts are the work of Geoff Sullivan, Olaf Ostwald and Frode Weierud (CryptoCellar, CC BY-NC-SA 4.0). Break by Claude (Anthropic) with the author, 26 September 2026.

- 1941 unbroken message list — status of AWTZK and ZNLZT (listed unbroken as of 26 September 2026)
- German Army Enigma messages, July 1941 — transcribed ciphertexts and headers of Nr. 187 and 189
- Message form Nr. 187 AWTZK and message form Nr. 189 ZNLZT — scans used to check the transcription
- Enigma keys, July 1941 — keys of 10 and 12 July (wheel-order restriction)
- Heeresgruppe Nord, July 1941 (PDF) — solved messages used for crib mining, incl. Nr. 194 MAKJH
- py-enigma — independent Enigma simulator used for re-decryption