

WWII Carrier Pigeon Cipher Investigation – Detailed Summary

Overview

This document summarizes the full investigation into the WWII carrier pigeon cipher message, including cryptographic analysis, procedural findings, historical reconstruction, and archival research steps undertaken to date.

The Cipher Message

The recovered message consists of 27 five-letter groups followed by an administrative footer ('27 1525/6'). The formatting matches British WWII field communication standards. The repeated group 'AOAKN' appears as both the first and last group, indicating a procedural indicator or framing group rather than plaintext.

Cryptographic Analysis

Extensive testing ruled out substitution ciphers, Vigenere or Beaufort systems, book ciphers, and transposition methods. Statistical properties—low repetition, flat frequency distribution, lack of periodicity—are consistent with a correctly used one-time pad (OTP). Crib-dragging and key-reversal attempts fail immediately, as expected for OTP traffic.

Procedural Indicators

The message includes standard British procedural features: five-letter grouping discipline, group count footer, time-of-origin notation, and use of indicator groups. 'X02' appears as a routing or desk identifier, consistent with forward command HQ practice.

NURP Identification

Handwritten annotations (e.g., 'NURP 40 TW 194' and 'NURP 37 OK 76') conform to National Union of Racing Pigeons wartime registration formats. These identify the pigeons used, confirming authenticity and operational use rather than training or hoax material.

Historical Reconstruction

A coherent hypothesis identifies the sender as Sergeant William Stott (RAAF), wireless operator aboard a Liberator of No. 120 Squadron RAF. The message was likely sent during an ultra-long-range anti-submarine patrol operating from Iceland. A probable date is 4 October 1943, coinciding with known North Atlantic operations and aircraft losses involving U-boat encounters.

Why Iceland

No. 120 Squadron RAF was based in Iceland during October 1943, flying Liberator aircraft on North Atlantic patrols. The mission profile, routing identifier (X02), timing metadata, and lack of a pigeon return entry align best with an Iceland-based origin. This remains a hypothesis pending confirmation from squadron records.

Archive Research

The correct Operations Record Book (ORB) for further confirmation has been identified as AIR 27 / No. 120 Squadron RAF, 1943 (National Archives reference C7159250). This ORB is expected to document patrol activity, aircraft losses, crew roles, and relevant timings.

Crack Feasibility

Plaintext recovery is mathematically infeasible without pad reuse or discovery of a sibling ciphertext. No such sibling message is currently known in public archives. The cipher appears to have been used correctly, with failure occurring only due to message non-delivery.

Current Status

The investigation is awaiting access to ORB record C7159250 to confirm operational details for 4 October 1943. Further progress depends on correlating archival records with the message metadata.