Worksheet: Breaking the Enigma

Unit: Probability, Random Variables, and Probability Distributions (AP Stats Unit 4)

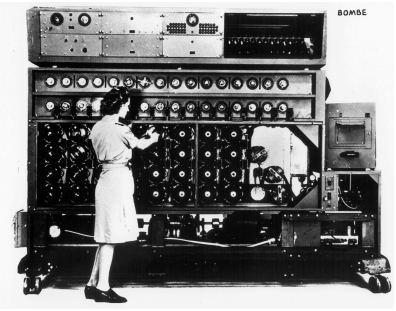
Topics: Conditional Probability & Bayes' Theorem, Independence, Expected Value

In this worksheet, students take the role of Bletchley Park codebreakers, using Bayes' theorem to evaluate the reliability of the Bombe machine, combining independent cribs to strengthen evidence, and calculating expected value to prioritize which intercepted messages to decode.

Introduction:

It's 1940, and you're a mathematician at Bletchley Park, the center of Allied codebreaking operations. The Germans are encrypting their messages using the Enigma machine, a device with over 10^{20} possible settings that produces an entirely new code every day, making brute force impossible. Instead, your team must use different techniques to whittle down possible options.

Part I: Cribs and Conditional Probability:



The Bombe machine, designed by Alan Turing, worked by testing hypotheses of known fragments of messages, known as "cribs," to narrow down possible options. If codebreakers suspected a message contained a specific phrase, the Bombe could test whether a given Enigma setting was consistent with that crib. It wasn't perfect, however, and could flag incorrect settings as matches (false positives) and occasionally miss the correct setting (false negatives). Your job is to evaluate how much confidence each test actually provides.

1. The "Heil Hitler" Crib

Out of the Enigma's 17,576 possible rotor settings, exactly one is the correct setting for today. The Bombe tests each setting against the crib "Heil Hitler." Suppose:

- P(Correct setting) = $\frac{1}{17,576}$
- P(Bombe flags a match | setting is correct) = 0.92
- P(Bombe flags a match | setting is incorrect) = 0.04

A) The Bombe has just flagged a particular setting as a match. Use Bayes' Theorem to find the probability that this flagged setting is actually the correct one

B) Interpret your result. Should the codebreaking team trust a single flagged result from the Bombe, or is additional evidence needed?

2. Combining Two Independent Cribs

In practice, codebreakers didn't rely on a single crib. Suppose the team runs a second, independent test using the "ANX" crib (German for "to" followed by a spacer, which appeared at the start of many messages). For this test:

- P(ANX flags a match | setting is correct) = 0.85
- P(ANX flags a match | setting is incorrect) = 0.08

A) Assume the two crib tests are independent. A setting has been flagged for both the "Heil Hitler" and "ANX" cribs. Find the probability that the setting is correct, given that both tests flagged it

B) Compare this with your answer to 1A. Why is combining independent evidence so important, and why is it mathematically necessary that the two cribs are independent?

3. Herivel's Tip: Exploiting Operator Behavior

Mathematician John Herivel realized that lazy Enigma operators might not randomize their rotor starting positions properly, instead leaving them close to the daily setting. On a given day, define the following events:

- L = the operator is lazy (doesn't randomize the rotors)
- C = the indicator letters cluster near the true daily setting

Suppose P(L) = 0.40, P(C | L) = 0.90, P(C | L^C) = 0.05

A) Find P(C), the overall probability that clustering is observed on a given day

B) If clustering is observed, find P(L | C). How confident should the team be that today's operator was lazy?

Part II: Strategic Decision Making:

Bletchley Park had limited resources. The Bombe machine took time to run, and codebreakers had to decide which messages to prioritize and which techniques to invest in. These decisions were, at their core, problems of expected value: weighing the probability of success against the cost of each attempt.

Bletchley Park Codebreakers

4. Prioritizing Messages

The team has intercepted three types of Enigma messages today. The Bombe machine has about 10 hours of operational time left today. The table below shows, for each message type, the probability of successfully deciding it and the intelligence value (how beneficial it would be) if decoded

Message Type	P(Success)	Intelligence Value	Time Needed
Weather Report	0.70	25	2 hours
Naval Command	0.30	90	9 hours
Luftwaffe Tactical	0.50	55	5 hours

A) Compute the expected intelligence value for each message type

B) What would be the best way for the team to allocate their remaining time? Explain your reasoning using the expected value.

5. The No Self-Encryption Rule

An important property of the Enigma was that no letter could ever encrypt to itself. This meant that if a codebreaker aligned a crib against the ciphertext and found any position where the same letter appeared in both, that alignment could immediately be ruled out.

A) Assume a wrong alignment has a $\frac{1}{26}$ chance of matching at any given letter position. Assuming independence across positions, write an algebraic expression to represent the probability that a crib of length n produces zero self-matches across its entire length.

B) The codebreakers need to be 99% certain that an incorrect alignment will produce at least one self-match so it can be safely eliminated. Using your expression from Part A, calculate the minimum crib length n required to achieve this level of confidence

6. The Diagonal Board

Gordon Welchman's diagonal board improved the Bombe by exploiting the fact that Enigma's plugboard connections were reciprocal. If the plugboard swapped A with N, then it also swapped N with A, creating dependencies between letter pairings that could be used to eliminate false positives.

Suppose the plugboard connects 10 pairs of letters (out of 26). Define the events:

- A = letter A is connected to letter N
- B = letter N is connected to letter A

A) Are events A and B independent? Explain why or why not, referencing the reciprocal property of the plugboard

B) If events A and B were independent, as a naive codebreaker might assume, and P(A) = $\frac{10}{25}$, what would P(A and B) be? Compare this to the actual P(A and B) given the reciprocal property