Solutions: Breaking the Enigma

Part I: Cribs and Conditional Probability

1. The "Heil Hitler" Crib

Let M be the event that the Bombe flags a match, and let C be the event that the setting is correct.

We are given:

$$P(C) = \frac{1}{17576}, \qquad P(M \mid C) = 0.92, \qquad P(M \mid C^c) = 0.04.$$

A)

By Bayes' Theorem,

$$P(C \mid M) = \frac{P(M \mid C)P(C)}{P(M)}.$$

Since

$$P(M) = P(M \mid C)P(C) + P(M \mid C^c)P(C^c),$$

we have

$$P(M) = 0.92\left(\frac{1}{17576}\right) + 0.04\left(1 - \frac{1}{17576}\right).$$

Therefore,

$$P(C \mid M) = \frac{0.92\left(\frac{1}{17576}\right)}{0.92\left(\frac{1}{17576}\right) + 0.04\left(1 - \frac{1}{17576}\right)} \approx 0.001307.$$

So,

$$\boxed{P(C \mid M) \approx 0.001307 \approx 0.1307\%}.$$

B)

This probability is extremely small. Even if the Bombe flags a setting, there is only about a 0.13% chance that it is actually correct. The team should **not** trust a single flagged result on its own; additional evidence is clearly needed.

2. Combining Two Independent Cribs

Let H be the event that the "Heil Hitler" crib flags a match and A the event that the "ANX" crib flags a match.

We are given:

$$P(H \mid C) = 0.92, \qquad P(H \mid C^c) = 0.04,$$
$$P(A \mid C) = 0.85, \qquad P(A \mid C^c) = 0.08.$$

Because the tests are assumed independent,

$$P(H \cap A \mid C) = P(H \mid C)P(A \mid C) = 0.92(0.85) = 0.782,$$

and

$$P(H \cap A \mid C^c) = P(H \mid C^c)P(A \mid C^c) = 0.04(0.08) = 0.0032.$$

A)

By Bayes' Theorem,

$$P(C \mid H \cap A) = \frac{P(H \cap A \mid C)P(C)}{P(H \cap A \mid C)P(C) + P(H \cap A \mid C^c)P(C^c)}.$$

So

$$P(C \mid H \cap A) = \frac{0.782\left(\frac{1}{17576}\right)}{0.782\left(\frac{1}{17576}\right) + 0.0032\left(1 - \frac{1}{17576}\right)} \approx 0.013714.$$

Thus,

$$\boxed{P(C \mid H \cap A) \approx 0.013714 \approx 1.3714\%}.$$

B)

This is much larger than the answer to 1A, though it is still not very high in absolute terms. Combining independent evidence matters because each additional independent test helps separate the true setting from the many false positives. Independence is mathematically necessary here because we multiplied probabilities like

$$P(H \cap A \mid C) = P(H \mid C)P(A \mid C).$$

If the cribs were not independent, that multiplication rule would not be valid.

3. Herivel's Tip: Exploiting Operator Behavior

Let L be the event that the operator is lazy, and C the event that clustering is observed.

We are given:

$$P(L) = 0.40, \qquad P(C \mid L) = 0.90, \qquad P(C \mid L^c) = 0.05.$$

A)

Using the Law of Total Probability,

$$P(C) = P(C \mid L)P(L) + P(C \mid L^c)P(L^c).$$

Thus,

$$P(C) = 0.90(0.40) + 0.05(0.60) = 0.36 + 0.03 = 0.39.$$

So,

$$\boxed{P(C) = 0.39}.$$

B)

By Bayes' Theorem,

$$P(L \mid C) = \frac{P(C \mid L)P(L)}{P(C)} = \frac{0.90(0.40)}{0.39} = \frac{0.36}{0.39} = \frac{12}{13} \approx 0.9231.$$

So,

$$\boxed{P(L \mid C) \approx 0.9231 \approx 92.31\%}.$$

If clustering is observed, the team should be very confident that the operator was lazy.

Part II: Strategic Decision Making

4. Prioritizing Messages

Expected value is

$$\text{EV} = P(\text{success})(\text{intelligence value}).$$

A)

For the Weather Report:

$$\text{EV} = 0.70(25) = 17.5.$$

For the Naval Command:

$$\text{EV} = 0.30(90) = 27.$$

For the Luftwaffe Tactical:

$$\text{EV} = 0.50(55) = 27.5.$$

So,

$$\boxed{\text{Weather EV} = 17.5, \quad \text{Naval EV} = 27, \quad \text{Luftwaffe EV} = 27.5.}$$

B)

The team has 10 hours remaining.

- Weather only: 2 hours, EV = 17.5
- Naval only: 9 hours, EV = 27
- Luftwaffe only: 5 hours, EV = 27.5
- Weather + Luftwaffe: $2 + 5 = 7$ hours, total EV $= 17.5 + 27.5 = 45$
- Weather + Naval: 11 hours, not possible
- Naval + Luftwaffe: 14 hours, not possible

The best allocation is to decode the **Weather Report and Luftwaffe Tactical** messages, since together they fit within the time limit and give the largest total expected value:

$$\boxed{45}.$$

5. The No Self-Encryption Rule

A)

For one letter position, the chance of *not* matching itself is

$$1 - \frac{1}{26} = \frac{25}{26}.$$

Assuming independence across positions, for a crib of length n, the probability of zero self-matches is

$$\boxed{\left(\frac{25}{26}\right)^n}.$$

B)

The codebreakers want to be 99% certain that an incorrect alignment will produce *at least one* self-match.

So we want

$$1 - \left(\frac{25}{26}\right)^n \geq 0.99.$$

This gives

$$\left(\frac{25}{26}\right)^n \leq 0.01.$$

Taking logarithms,

$$n \ln\left(\frac{25}{26}\right) \leq \ln(0.01).$$

Since $\ln(25/26) < 0$, the inequality reverses when dividing:

$$n \geq \frac{\ln(0.01)}{\ln(25/26)} \approx 117.42.$$

Therefore the minimum integer n is

$$\boxed{118}.$$

6. The Diagonal Board

Let

$$A = \text{“A is connected to N”}, \qquad B = \text{“N is connected to A”}.$$

A)

These events are **not independent**. Because of the reciprocal property of the plugboard, if A is connected to N, then N is automatically connected to A. In other words, event A forces event B, and vice versa. So the events are completely dependent.

B)

If a naive codebreaker incorrectly assumed independence, then

$$P(A \cap B) = P(A)P(B).$$

Given

$$P(A) = \frac{10}{25},$$

and under the same naive assumption $P(B) = \frac{10}{25}$, this would give

$$P(A \cap B) = \frac{10}{25} \cdot \frac{10}{25} = \frac{100}{625} = \frac{4}{25} = 0.16.$$

So the naive independent-model answer would be

$$\boxed{P(A \cap B) = 0.16.}$$

But in reality, because of reciprocity,

$$P(A \cap B) = P(A) = \frac{10}{25} = 0.4.$$

So the actual probability is

$$\boxed{0.4}$$

which is much larger than the naive independent estimate.