INTRODUCTION

It seems almost since President Franklin Delano Roosevelt delivered his now immortalized speech declaring December 7, 1941 a “day that will live on in infamy” that the attack on Pearl Harbor has been the target of conspiracy theorists worldwide. Questions as to how much the United States, and, possibly, Great Britain, knew about the imminent attacks have been raised by countless individuals citing fairly reputable-sounding sources. These conspiracy theories, however, have never been proven and, so, any real discussion on the attack must rely on the United States government’s claim that no prior knowledge existed before the attack in Hawaii. The question as to why the United States knew so little about the Japanese Navy’s attack plans, however, remains. The importance of this question becomes compounded when one looks back at the now decrypted correspondences between Japanese Naval command and its ships, clearly marking the date and target of their initial attack. This is not a question of government conspiracies, but, rather, it is a question of secrecy. How was the Imperial Japanese Navy (IJN) able to keep their messages hidden from the prying eyes of the US Navy? Before answering such a question, one must understand the nature of the science of secrecy, cryptology.

CRYPTOLOGY, NOW AND THEN

Cryptology is divided into two parts: cryptography and cryptanalysis. Although some would claim to be able to use all three terms synonymously, to do so would be a grave error. Cryptology is the overall science of secrecy; it is an applied mathematical discipline that, today, utilizes a large arsenal of tools derived from various mathematical fields. The two divisions within cryptology are counterparts to each
other. Cryptography is the science of encrypting a message. In other words, cryptographers apply mathematics to the development of new ways for keeping messages secret, away from the prying eyes of those not meant to read them. Cryptanalysis, however, is the science of breaking the ”cryptosystems” created by the cryptographers. It is important to note that the cryptographer is interested in two things when designing a cryptosystem. The first is the most obvious: secrecy. If a cryptosystem is not designed well enough to keep messages secret, its purpose becomes meaningless. Secondly, however, a cryptographer is interested in practicality of their system. In other words, if the cryptosystem can’t be adequately applied by the party, or parties, that need to use it, it becomes, equally, meaningless.

In a discussion about the Japanese Navy keeping their messages secret one must discuss both players: the Japanese cryptographers designing the systems the IJN is to use and the US Navy cryptanalyzers working on breaking the systems created. It is also important to keep in mind that the year of the attack on Pearl Harbor was 1941. In other words, although many of the mathematical methods employed by modern-day cryptographers were already in place, the technology for applying them in any practical amount of time simply was not. In short, any of the cryptosystems in use during World War II, including those of the Japanese Navy, can now be applied using a properly programed graphing calculator. At the time, however, the systems were both practical and effective when remembering most of the calculations were done either by hand or by primitive, mechanical machines. This was not a considerable disadvantage for the Japanese simply due to the fact that the US Navy’s cryptanalyzers were equally limited in their technological capabilities.
The Japanese Cryptosystems

The Japanese government and military used many different cryptosystems before and during World War II. The most famous of these cryptosystems are probably those given the codenames PURPLE and RED, its predecessor. Although these systems are fascinating in their own right, their key role with regards to the attack on Pearl Harbor is not apparent and will be discussed later. Because the attack on Pearl Harbor was a Japanese naval attack, it seems appropriate to deal solely with the cryptosystems of the IJN, specifically JN-25 and JN-25B (or ”baker”). These cryptosystems were, for all intents and purposes, identical in process. They were labeled “JN-25” due to the fact that they were the 25th IJN cryptosystem worked on by US Naval intelligence and were the systems most heavily in use by the Japanese Navy just prior to the attack on Pearl Harbor. Thus, to understand how the Japanese kept their plans secret, one must understand how the cryptosystem they used worked.

The Workings of JN-25. A message sent using the JN-25 cryptosystem is both encoded\(^1\) and enciphered\(^2\). This means in order to encrypt a message using the JN-25 system, the clerk, or whoever was sending the message, would have to follow a three-step process.

The first step was the encoding step. This step involved the clerk looking up in a book of tables, the “codebook,” each of the words being sent in the given message. The codebook consisted of approximately 33,000 commonly used words and phrases in the Japanese language and a preset five-digit number equivalence (see Table 1). If, for whatever reason, the clerk could not find the word needed in the codebook, the

---

\(^1\)To **encode** in the context used throughout this paper means the simple replacement of a letter, word, or phrase by a preset number which, for all intents and purposes, remains fixed throughout time. Intuitively, decoding is the reversal of this replacement.

\(^2\)To **encipher**, here, means to apply a process to a message in order to change what is to be sent. This process produces relatively random results. The undoing of this process is called deciphering.
Table 1. Step 1: Encode the Message

| SHIPBOARD ATTACK PLANES WILL CARRY OUT |
|-----------------|-----------------|-----------------|-----------------|
| 7877            | 23466           | 81246           | 90678           |
| SIMILAR BOMBING ATTACK |
| 12558           | 57798           | 23466           |

word could be spelled out in kana\textsuperscript{3} using the five-digit equivalances for each character needed.

The second step was a preliminary step for the enciphering portion of the cryptosystem. In this step, the clerk would refer to another book, the “enciphering manual.” This was another tabular book. This time, however, there was little rhyme or reason to the five-digit numbers found within. Simply put, the numbers were randomly generated. A clerk would then pick a random page and line number and start writing down the five-digit “aditives” under each five-digit code he found previously (see Table 2).

Table 2. Step 2: Additive Step

| SHIPBOARD ATTACK PLANES WILL CARRY OUT |
|-----------------|-----------------|-----------------|-----------------|
| 21445           | 78653           | 90072           | 12231           |
| SIMILAR BOMBING ATTACK |
| 12558           | 57798           | 23466           |
| 45521           | 67721           | 09112           |

Once each of the encoded “words” have a corresponding additive written beneath it, the enciphering step begins. This step entails what the US Navy cryptanalysts called “false addition.” It is addition modulo 10 on each of the five digits, or non-carrying addition. For instance, \(7 + 5 = 12\), so the clerk would write the digit 2 without carrying the 1 over to the next column. Using “false addition” as opposed to

\textsuperscript{3}kana, or katakana, is a syllabic character system used to “sound out” Japanese words
Table 3. Step 3: Enciphering Step

<table>
<thead>
<tr>
<th>SHIPBOARD ATTACK PLANES WILL CARRY OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>78777 23466 81246 90678</td>
</tr>
<tr>
<td>21445 78653 90072 12231</td>
</tr>
<tr>
<td>99112 91019 71218 02809</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SIMILAR BOMBING ATTACK</th>
</tr>
</thead>
<tbody>
<tr>
<td>12558 57798 23466</td>
</tr>
<tr>
<td>45521 67721 09112</td>
</tr>
<tr>
<td>57079 14419 22578</td>
</tr>
</tbody>
</table>

regular addition accomplished two things for the Japanese navy. It guaranteed each message group, or word, to be five digits long (i.e. even 99999 + 99999 would result in a five-digit number, namely 88888). It also simplified the task of addition enough that it could be applied using simple machines employed at the time, allowing for quicker calculations and faster transmission of the encrypted messages. Once all of the message groups were enciphered, the encrypted message was ready to be sent (see Table 3).

With all three of these steps completed, the Japanese clerk could then send the message. The first part of the message would indicate the page and line number the clerk started on in the enciphering manual. The five-digit, enciphered and encoded message blocks would then be sent to whomever the designated recipient was. Once the message received, the recipient would then use the information given (namely, the starting place in the enciphering manual) and work backwards using their own copy of the enciphering manual and codebook. Often the messages were also intercepted by US Naval intelligence. The US Navy cryptanalysts would then be set to work on reading the intercepted messages. Due to a few strengths on the part of JN-25 and

---

4This information was sent using a different cryptosystem altogether; it is not clear whether or not the US Navy had broken this cryptosystem by the time of the attack on Pearl Harbor on December 7, 1941.
a few weaknesses on the part of the US government, however, this proved to be an arduous task.

**Why JN-25 Worked.** It seems appropriate to remind the reader at this point of the circumstances surrounding the attack on Pearl Harbor. By December, 7, 1941, the United States had not yet entered World War II. Although there were numerous threats and a few skirmishes with both Japanese and German military forces, the United States was not in open warfare. Indeed, of the two nations, Germany seemed the more imminent threat with the presence of German “u-boats” in the Atlantic Ocean threatening US trade. Because of these facts, US intelligence was focused primarily on German messages sent using their “Enigma” machine and the aforementioned Japanese diplomatic codes RED and PURPLE. Although there was some interest in the Japanese military codes, especially their naval codes, the number of cryptanalysts assigned to breaking them paled in comparison to the number focusing on Enigma and PURPLE. Those who were working on the IJN’s cryptosystems were met with the strengths inherent in the system.

The first such strength derives directly from the lack of present-day technologies in 1941. To the modern reader, thousands of calculations can be done in fractions of a second using today’s computer technology. During the time of World War II, however, most calculations were still done by hand or through fairly primitive mechanical means. JN-25 used five-digit additives and codes. This meant that, for each message “word”, there were a total of 100,000 (10^5) possibilities for the additive used. If a message contained, for instance, 100 words, the message could have been enciphered in any of 10^1,000,000,000 ways! Suddenly, the idea of deciphering such a message in any amount of time seems impossible with the technology in use at the time.
It is also important to note that such a message cannot be properly deciphered without the cryptanalyzer having an idea of what to look for. This is where the Japanese two-step process becomes a clear strength. Consider the small sample excerpt given in Table 4. The first line is the message as it would have been sent, encoded and enciphered. The second line represents the same message after the deciphering process had been completed successfully. This illustration clearly indicates the problem: without knowing what the codes were, how would one hope to decipher the message? In other words, even after finding the correct additive, the cryptanalyzer would still be looking at a five-digit number. How could he/she be sure this was the correct result? It seems, therefore, that one could not decipher the message without being able to decode it and, because the enciphering step was applied after the encoding step, one couldn’t hope to decode the message without being able to decipher it!

**How JN-25 Fell.** Despite its strengths, JN-25 was, eventually, successfully broken. Understanding how the US Navy cryptanalysts were able to read the messages requires an understanding of the weaknesses of the cryptosystem. There were, for instance, a number of logistic issues the IJN was never able to overcome. Because of the funding and organization structure of the Japanese Navy, neither the codebooks nor the enciphering manuals were able to be changed on a regular, or frequent, basis. This meant that the additives were, eventually, reused. This mistake allowed US Naval intelligence to slowly piece together the enciphering manual, itself.

The nature of the Japanese language and of military correspondences was also a weak point for JN-25. Like English, and unlike many Latin and Greek-based languages, word order in Japanese matters. This means the connotation of a word when

---

5i.e., encoding then enciphering
used in a sentence is the direct result of where it is in the sentence\(^6\), with few exceptions\(^7\). Military messages are, by their nature, formal. A message sent from one ship to another, for instance, would begin with the name of the receiving ship, the name of the transmitting ship, the commander of that ship, the location of the ship, and the date and time on which the message was sent. As will be discussed shortly, these weaknesses would help US Naval intelligence during the decoding (and, in some ways, the deciphering) step of decrypting the message.

Perhaps the largest, and most glaring, weakness in JN-25, however, exists within the codes, themselves. Many cryptosystems provide for a way to check for errors in transmission; JN-25 was no different. The way in which this was done, however, seems to have provided little assistance to the Japanese and was a great contributor to the breaking of the system. The error check devised by Japanese cryptographers was to make all of the numbers in the codebook divisible by three. Theoretically, the recipient of a message could then ensure the message was sent correctly simply by ensuring the codes sent (after being deciphered) were divisible by three. If they were not, the message could either be read disregarding the errors, or resent. Although this did provide for some error-checking, it was a grave mistake on the part of the Japanese cryptographers. In essence, the strength of the two-step process was compromised; US Naval cryptanalysts no longer needed to know what the codes they were looking for were in order to decipher the message, they now needed only to look for additives that would result in codes divisible by three.

Using this information, US Naval intelligence was able to start piecing together the enciphering manual. In order to ensure the additive was truly the correct one used (as,
even with knowledge that the codes were all divisible by three, there were still 33,333 possible additives), multiple message “words” that all used the same additive had to be found. This is where the fact that the Japanese Navy had to reuse the additives periodically became useful. Because the additives were reused, eventually the same word would be enciphered using the same additive. This meant that message words would be sent that were identical in two different messages. The message words that were the same distance from this equivalent word in each message, therefore, would have used the same additive (see Table 5). Once a number of message words that used the same additive were found, the additive that resulted in each deciphered code being divisible by three was found. If enough message words were examined that all used the same additives (say 10 or 12), then the probability that a $k$ found that, when subtracted, would result in codes all divisible by three was not the actual additive used would be very small. Once these additives were discovered, US Naval intelligence was able to start piecing together parts of the enciphering manual used by the IJN.

Table 4. A Two Step Process

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>99112</td>
<td>91019</td>
<td>71218</td>
<td>02809</td>
<td>57079</td>
<td>14419</td>
</tr>
<tr>
<td>21445</td>
<td>68653</td>
<td>90072</td>
<td>12231</td>
<td>45521</td>
<td>67721</td>
</tr>
</tbody>
</table>

Table 5. Finding the same additive

| Message 1: | 84762 | 19234 | 54233 | 90123 | 11287 |
| Message 2: | 84762 | 76231 | 28123 | 74621 | 92146 |

Table 6. Finding the additive used

$$
\begin{align*}
11287 &= \text{CodeA} + k = 3(A) + k \\
50310 &= \text{CodeB} + k = 3(B) + k \\
74366 &= \text{CodeC} + k = 3(C) + k \\
82967 &= \text{CodeD} + k = 3(D) + k \\
92146 &= \text{CodeE} + k = 3(E) + k
\end{align*}
$$
Although having codes that were all divisible by three considerably lessoned the difficulty of the deciphering step, messages could still not be read unless they were properly decoded. The decoding step, it turned out, requires much more ingenuity and hard work. Because, as mentioned previously, the United States was not yet in open warfare with Japan, it was infeasible to successfully capture an enemy codebook. The codebook, then, had to be pieced together slowly through cryptanalysis. This meant using simple tabulator machines developed by IBM at the time to analyze which message words were sent together most frequently. Using common cryptological practices such as probable word analysis based on this information, it was possible for US Navy cryptanalyzers to start recreating the IJN codebook. Understandably, this meant spending thousands of man-hours tackling this problem; man-hours that were, simply, unavailable for those working on the JN-25 cryptosystem prior to the attack on Pearl Harbor.

PEARL HARBOR, A JAPANESE SUCCESS AND A US FAILURE

Blame has been placed by an uncountable number of conspiracy theorists worldwide on the United States for “letting” the attack on Pearl Harbor happen. The question, then, becomes, is this placement of blame appropriate? How the Japanese kept their attack plans a secret has been, thus far, discussed. It seems appropriate, therefore, to analyze this data and either credit Japan for its success in keeping their intents a secret, or to uphold the placement of blame on the United States for not acting appropriately in order to prevent such an attack on US Naval interests. It is important to note that, unlike many of the conspiracy theorists, no accusation of actual prior knowledge of Pearl Harbor is considered. Rather, only the reasons behind the United States not having prior knowledge is discussed.
Why not Pearl Harbor? From a logistical standpoint, Pearl Harbor was an improbable target for the Japanese Naval fleet. Consider, for instance, the relative position of Pearl Harbor compared to Japan. It is also important to consider the favored attack methods of the IJN. The aircraft carrier was not only employed but was in heavy use during the build up to and during World War II. Japanese “dive bombers” could launch from an aircraft carrier and deploy air-to-sea torpedoes against a naval target. Pearl Harbor’s waters, however, were too shallow for the traditional Japanese air-to-sea torpedo, and, thus, it would be harder to inflict serious damage on the ships harbored there. Added to this was the complication of conducting a surprise attack via aircraft. Any kind of surprise would be forfeit if aircraft carriers close to Hawaii were detected. This meant that the normal, close-range support role of the Japanese Naval aircraft would have to be extended to a long-range attack role, requiring more fuel than was normally kept on carriers.

Why Pearl Harbor? Given the above mentioned complications, why should the IJN have wanted to strike such an unlikely target? Although the Japanese Navy was considered one of the strongest fleets in the world by 1941, there were considerable gaps in their ability to conduct a successful attack against the US Pacific Fleet. This meant that success would only be guaranteed if the US fleet was crippled considerably. With much of the Pacific Fleet stationed at Pearl Harbor, Hawaii, it seems a logical target for attack to accomplish just that goal. Added to this was the considerable psychological impact such an attack, on US soil, would have on the United States, both its citizens and its military.

The question, then, becomes, how were the Japanese able to conduct such an improbable attack at all, let alone in secret? Simply put, the Japanese “compensated”
for each of the difficulties of attacking a target such as Pearl Harbor. These compensations can be seen through a series of correspondences of the Imperial Japanese Navy\(^8\).

The first complication to be addressed is that of the shallow waters of Pearl Harbor. In order for their torpedoes to inflict damage, they would have to be modified in order to run in shallower waters\(^9\):

FROM: CHIEF OF STAFF FIRST AIR FLEET 28 OCTOBER 1941
TO: CHIEF GENERAL AFFAIRS SECTION NAVAL TECHNICAL BUREAU
   GENERAL AFFAIRS SECTION AERONAUTICS BUREAU
   CHIEF FIRST SECTION NAVAL SECTION IMPERIAL HEADQUARTERS
   CHIEF SECOND SECTION NAVAL SECTION IMPERIAL HEADQUARTERS
INFO: CHIEF OF STAFF COMBINED FLEET
   KURE NAVY YARD

ON 30 OCTOBER, THIS FLEET WILL PICK UP FROM 5 TO 10 NEAR SURFACE TORPEDOES AT SASEBO MILITARY STORES DEPARTMENT(.). CLASSES ON THIS TORPEDO WILL BE HELD AT KANOYA FOR ABOUT FIVE DAYS FROM THE 31ST AND THEN WILL BE SHIFTED TO FIRING PRACTICE ... BY WORKING NIGHT AND DAY, IT SHOULD BE POSSIBLE TO COMPLETE 10 BY 5 NOVEMBER.

Even with modified torpedoes, the Japanese Navy still needed to get the attacking planes to Pearl Harbor. This feat required an immense amount of fuel and a complex refueling system to be in place prior to the attack:

FROM: CHIEF OF STAFF FIRST AIR FLEET 30 OCTOBER 1941
ACTION: KUROSHIO MARU OR SHINKOKU MARU
INFO: KURE NAVY YARD
   KURE SANDA SECTION

\(^8\)Each of the messages here are reproduced from “The Unsolved Messages of Pearl Harbor,” by Frederick D. Parker and published in Cryptologia. See the references page for more details.

\(^9\)It may also be advantageous for the reader to look for the “formality” weakness in the IJN’s correspondences in the messages reproduced here.
WHEN INSTALLATION OF GEAR FOR REFUELING UNDER TOW AND PREPARATIONS FOR ACTION HAVE BEEN COMPLETED, KUROSHIO MARU AND SHINKOKU MARU WILL DEPART SASEBO AND KURE RESPECTIVELY ON THE 13TH AND PROCEED TO KAGOSHIMA BAY, CONDUCTING EXERCISES WITH CARRIERS ENROUTE.

REQUEST THEY LOAD FUEL OIL FOR REFUELING PURPOSES BEFORE THEY DEPART.

All of the reasons why Pearl Harbor was an improbable target, therefore, were taken care of. It seems clear from these two messages (and many others like them) that, had the United States decrypted the messages in time, the attack of Pearl Harbor could have been realized and, perhaps, prevented. Why, then, weren’t the messages decrypted and read in time? The reasons were hinted at during the discussion of the cryptosystem, itself. Put simply, the United States government and military intelligence did not feel the Japanese Naval codes were worth working on prior to open hostilities. Indeed, it wasn’t until late in 1941 that more than five cryptanalysts were assigned to work on the Japanese Naval codes at all, let alone to focus on JN-25\textsuperscript{10}. During the last six months of 1941, increased pressure was put on US military intelligence to provide speedy and accurate decryption of the Japanese diplomatic codes. In other words, the United States wanted to know what Japan was telling its ambassadors, a worthwhile cause except for the fact that Japan never told its diplomats of the upcoming attack.

\textbf{Minimal Success & Major Setbacks.} Despite the lack of attention paid to the IJN’s cryptosystems, there was some minimal degrees of success for US cryptanalysts.

\textsuperscript{10}There were, at the time, five other naval codes in heavy use by the Japanese navy at the time: JN20, JN22, JN39, JN40, and JN61. Although beyond the scope of this discussion, these codes represented naval activity spanning from minor construction work to naval attaches.
Near the end of 1940, the first JN-25\textsuperscript{11} was almost fully decipherable. This meant that, although most of the codebook was still unknown, cryptanalysts would be able to work on them without the further trouble of first breaking the enciphering step. However, December 1, 1940 saw Japanese cryptographers introducing JN-25B\textsuperscript{12}. This second generation JN-25 cryptosystem introduced an even larger codebook than was previously used and expanded on the enciphering tables, adding more additives and reducing the number of times an additive was reused. Further complications were introduced throughout 1941 as new enciphering books were released by the Japanese. These enciphering books were designated “Baker-1,” “Baker-2,” etc. by US Naval cryptanalysts with “Baker-8” being released for use just three days prior to the attack on Pearl Harbor. Although Japanese transmission errors and the utilization of deciphering techniques previously described allowed for each successive new additive lists to be broken, the decreased man-hours being spent on IJN cryptosystems due to climaxing diplomatic negotiations meant the enciphering manual, “Baker-8” would take months to fully decipher. This decrease in manpower coupled with the change in the codebooks late in 1940 also meant that only about 10% of JN-25B’s codes could be read by December 7, 1941.

\textbf{Conclusions}

When reviewing the facts, it seems inappropriate to accept conspiracy theorists’ claims that the United States knowingly allowed the Japanese to attack Pearl Harbor on December 7, 1941. Looking back on the numerous intercepted messages leading up to the attack, it seems almost inevitable to assume that someone had to know something. This same phenomenon has occurred numerous times over the last century

\textsuperscript{11}JN-25 ‘Able’
\textsuperscript{12}JN-25 ‘Baker’
(i.e., the Oklahoma City bombing, the terrorist attack on the World Trade Centers in 1993 and 2001, etc.); it seems a natural human faculty to try and place blame on someone. To quote an old undying, and incredibly accurate, cliche, “hindsight is 20-20.” The truth of the matter is that the United States just wasn’t paying attention to the Japanese Naval cryptosystems. It was felt, by the US government, that, were the Japanese to declare war, they would do so through their diplomats. Because of this, the Japanese diplomatic codes, dubbed “PURPLE” and “RED” by US Military intelligence, became distractors; coupled with the German u-bout threat in the North Atlantic, this increased attention to the Japanese ambassadors pulled key personnel away from the IJN codes during the last half of 1941.

The major strength of the JN-25 cryptosystem was its two-step process. Messages sent with it were enciphered and encoded. Because of the major flaw in the system, namely the fact that the codes were all divisible by three, however, the deciphering portion of the decryption process was fairly easily accomplished. This was combated by the replacement of enciphering manuals at a more frequent rate once JN-25B was developed by the Japanese cryptographers. Nevertheless, analyzing now decrypted IJN messages sent during the build-up to the attack on Pearl Harbor, it is clear that the United States government could have and should have known what the Japanese intentions were in late 1941.

Despite its immediate and tragic consequences, the Japanese attack on Pearl Harbor did, however, bring with it a unified United States government, military, and country into the middle of World War II. After the attack, the United States Naval cryptanalysts were set hard at work breaking the Japanese military cryptosystems and were, by late January, 1942, fairly successful. This meant that, although not in time to prevent the tragedy in Hawaii, US military intelligence played a critical role in
uncovering future plans of the IJN which led to many US naval victories. As Isoroku Yamamoto is credited with saying, all the Japanese accomplished was to “awaken a sleeping giant and fill him with a terrible resolve.”
References


