Our Rabbis taught: When the Hasmonean kings made enmity against each other, Horkenos was on the outside [of Jerusalem] and Aristobulus was inside. Each day [those inside the walls of Jerusalem] would drop dinars in a basket and retrieve [animals for] sacrifices. There was one old man who was versed in Greek wisdom and whispered to them using Greek wisdom. He said to them: As long as they [inside Jerusalem] continue to bring sacrifices, they will never fall to your siege. The next day dinars were lowered in a basket, but a pig was raised [instead of a kosher animal]. When the basket reached half the height of the wall, the pig jabbed its nails into the wall and all of the land of Israel quaked to a distance of four hundred parasas. At that moment they said: cursed is anyone who raises pigs and cursed is anyone who teaches his son Greek wisdom.

Menachot 64b

The background for this episode is the civil war between the two sons of Salome Alexandra (who ruled from 76 to 67 BCE), Aristobulus II and Hyrcanus II. Hyrcanus held the office of kohen gadol during Salome’s reign and was named her successor. But the younger Aristobulus rebelled and enjoyed greater public support. Hyrcanus was backed by his fellow priests and took refuge in Jerusalem, though eventually Aristobulus prevailed and captured Jerusalem and the Temple. The strife between the brothers was short lived as they soon came to a compromise, so the above story probably took place sometime around the year 65 BCE.

The story is difficult to understand on a number of levels, but our concern relates primarily to the nature of the "Greek Wisdom" – chochmat yevanit – which plays such a crucial role. There are other places in the Talmud that refer to Greek wisdom (for example Menachot 99b) with a greater or lesser degree of stigma attached to studying it, but the fundamental determination regarding the nature, scope, and definition of this discipline remains vague.

Philosophy and Secular Studies

Throughout the generations, there have been two schools of thought and approaches in understanding the prohibition against studying chochmat yevanit. The predominant explanation holds it to be philosophies or ideologies associated with the regnant external culture. In this view, the old man in the story of the siege of Jerusalem must have been influenced by Greek culture and thinking, and therefore advised the enemy
accordingly. (It must be said, that in terms of a straight reading of the text, this understanding is problematic.)

This idea is brought down by Rabbi Elazar of Worms (1160–1230) in his commentary to the Siddur. On the words of the Shema "and these[האלה] words should be on your heart" he writes:\footnote{This [words] – means to exclude. All of the wisdom of the Torah you should research for that will stay with you beyond the grave, but not Greek wisdom and magic… and other worthless things.}

\begin{quote}
\text{{"האלה\[האלה\]בקבר\(\text{[ועמך\text{כבר\[ועמך\]}\]תלוך\[היא\]}\]כי\[תחקור\[התורה\]}\[חכמת\[כל\[ולא\]יוונית\[חכמת\[ולא\]|\]וכשפים\[ניגון\[גלחים\[וחכמת\[בטילים\[דברים\[ולא\]]\]]\]]\]]\]]\})
These [words] – means to exclude. All of the wisdom of the Torah you should research for that will stay with you beyond the grave, but not Greek wisdom and magic… and other worthless things.
\end{quote}

This understanding of Greek wisdom as external philosophy has been extended by the Rokach to apply to any non-Torah area of study that can be deemed "worthless".

The Meiri (1249-1310) takes this approach one step further, though distinguishing between Greek language and Greek wisdom.\footnote{Greek language, as we have described in Megilla, is one of the richest languages, in any event, it is prohibited to study their wisdom since it attracts the heart of men and destroys many of the foundations of religion.}

\begin{quote}
\text{לושם נו יכר אברג מגדהל (ביה למשנה ורש פサイズ) שדיא פאיירישיר שבלשנות. ושלכל}

\text{מקור החכמה שלמה אפור הלמד מכיר שופषת לבר של אד מרוהות התורה פשטות תודח.}
\end{quote}

Greek language, as we have described in Megilla, is one of the richest languages, in any event, it is prohibited to study their wisdom since it attracts the heart of men and destroys many of the foundations of religion.

The Meiri takes the position that the prohibition against studying chochmat yevanit applies to Greek philosophy, and presents the reason for the ban. He goes beyond the Rokach who merely claimed that such study constituted a waste of time. This discipline presents arguments that are compelling, teachings that are alluring, and positions that are at odds with the fundamental axioms of Jewish thought, and therefore it should be shunned.

A similar attitude is brought down by the Rabbi David ibn Avi Zimra (1479-1573) as he describes his pedagogical position.\footnote{A similar attitude is brought down by the Rabbi David ibn Avi Zimra (1479-1573) as he describes his pedagogical position.}

\begin{quote}
\text{וכבר פרשו עניינ מקורת הוגה, בכל למודם בחכמה המחקר את בנם אפור כמד שפתון, ואספנו,}

\text{שאם אם פנינו התכלדנ במנונים וב쫏 מלוחד החכמה ואמר פנינו שמלצון הלובוט}

\text{וכפה לנו מניין החכמה, והאמר לואד לדבר הבחא.}
\end{quote}

We have already explained the idea of Greek wisdom, that to toil in that discipline and research is not prohibited as we have written. However, in practice, I have consistently deterred my students from studying this subject because in our days the hearts have been reduced [i.e. the level of understanding is inferior] and the wells of knowledge have become clogged, and perhaps men will be led astray to valueless ideas.
Although the narrow focus here has been the study of Greek philosophy, the rationale given makes it easy to see how the scope could be expanded to encompass secular studies in general, or all non-Torah branches of learning. In many ways, the discussion regarding *chochmat yevanit* has shaped the way large sections of Jews throughout the ages have approached secular studies and has been the rallying point of the fundamentalist aversion to all research into anything other than traditional Jewish sources. Whether one feels such study is merely a waste of time or something more pernicious, the mind-set whose baseline approach to all secular knowledge is pejorative (typically associated with the Haredi community) can trace its origins back to an old man who ill-advised the besieging army as to how to subvert God’s protection of the Temple.

**Hints and Signs**

There is, however, another school of thought regarding the nature of Greek wisdom, whose study the Talmud seeks to prohibit. In his commentary on the story in Menachot, Rashi interprets *chochmat yevanit* as ṭרְמִיזָה – hints or signs.\(^4\) In his commentary to a parallel story brought down elsewhere in the Talmud, Rashi expands his explanation:\(^5\)

*Greek Wisdom* – a sophisticated language that is used by members of the palace and the common people do not recognize it

According to this view, the story of the Hasmonean siege can be simply understood. A traitor inside the walls of Jerusalem wanted to get a message out to his compatriots but the lines of transmission were being watched. Skilled as he was in a means of communication that others could not discern, he drafted his seditious communiqué and passed it undetected to the enemy. The resulting fall of Jerusalem and defiling of the Temple led to a ban on the use and study of such types of secret codes.

Rashi’s notion that *chochmat yevanit* is some sort of secret language was accepted by some later commentators and finds its way into the legal response as well. Rabbi Isaac ben Shefet Perfet (1326-1408) discusses this issue and, rejecting the view that Greek wisdom is to be associated with philosophy, writes:\(^6\)

From this it is clear, that those books [i.e., books on physics and metaphysics] are not included in this prohibition [i.e., the ban against the study of *chochmat yevanit*]. For regarding the fact that they are written in Greek, the language itself is not prohibited, and everyone is well versed in it.

---

\(^4\) ‏רש“א מפכת מנהות דף מ"א:‏

\(^5\) ‏רש“א מפכת פורים דף מ"ב:‏

\(^6\) ‏ש"ת הרוחי"ש סقس מה"ד ז"ה שסאלת
Moreover, the Talmud (Megilla 18) explicitly states that reading the Megilla in the Greek language is acceptable according to all opinions. And regarding the discipline itself, what precisely did the old man whisper to them? Therefore, in my opinion, Greek wisdom means to speak in the Greek language in riddles and with secret phrases, so that the general public will not understand, but only those who are well versed and practiced in those secrets.

The Rivash here challenges the view that Greek or secular philosophy was banned, on the basis of the difficulty in fitting this reading into the story of the siege of Jerusalem, as we have already noted. The problem lies rather with using Greek language to pass information in such a way that it can not be understood by the average listener.

The question that begs to be raised at this point is: What is special about Greek? If the Rabbis were troubled by the notion that secret messages could go undetected, then why should Greek be particularly useful in facilitating this channel?

In fact, Rav Moshe Feinstein (1895-1986) accepts the view that chochmat yevanit means secret codes, but (quite logically) expands the ban to any language.

It should be noted that in every language there is the straightforward usage that the common person speaks, and there is a more sophisticated plane on which the ministers communicate. We have seen in the Talmud that within the Greek language (that has great stature as it may be used in writing holy books – as in Megilla 8b) there is a dialect called Greek Wisdom that the Rabbis prohibited (as in Baba Kama 82b – see the Rambam's commentary on the Mishna at the end of Sotah, yevanit). And as Rabbenu Hillel explained, this type of sophisticated secret dialect, which exists in any language, is prohibited. The ban is not only on the language of Greek (chochmat yevanit), but in any language.

Rav Moshe's position follows logically from the assertion that the Rabbis' displeasure was with opening any channel of communication that could not be monitored. Nonetheless, the association of this manner of data transmission specifically with Greek influence seems central to the Talmud's description. It is difficult to pull out and marginalize the yevanit from the notion of chochmat yevanit.

Furthermore, the most central question that must be addressed is: why? What did the Rabbis find objectionable in passing secret messages between people?
Ancient Cryptography

Cryptography, literally the study of hidden writing or secret messages, dates back to ancient times. The methodology for passing written information in such a way that only the sender and the receiver can understand the note is straightforward. The sender encryps the message turning it into an unintelligible sequence of letters, which the receiver then decrypts thus retrieving the original text. The key to accomplishing this is the cipher, or the algorithm known only to the sender and receiver that is used in encryption and decryption.

Perhaps the oldest instrument used to implement a cipher is the Spartan scytale. The Greek historian Plutarch (46-127) describes it use:

They make two round pieces of wood exactly alike in length and thickness, so that each corresponds to the other in its dimensions, and keep one themselves, while they give the other to their envoy. These pieces of wood they call scytalae. Whenever, then, they wish to send some secret and important message, they make a scroll of parchment long and narrow, like a leathern strap, and wind it round their scytale, leaving no vacant space thereon, but covering its surface all round with the parchment. After doing this, they write what they wish on the parchment, just as it lies wrapped about the scytale; and when they have written their message, they take the parchment off and send it, without the piece of wood, to the commander. He, when he has received it, cannot otherwise get any meaning out of it,—since the letters have no connection, but are disarranged,—unless he takes his own scytale and winds the strip of parchment about it, so that, when its spiral course is restored perfectly, and that which follows is joined to that which precedes, he reads around the staff, and so discovers the continuity of the message.

Use of the scytale dates back to the 7th century BC. The way it works is straightforward. One side wraps a strip of paper around the scytale and writes across the spiraled strip. When the paper is unrolled the letters make no sense. Only someone with an identical scytale can understand the message by wrapping the strip around his own device. For example, if a person using the scytale writes the following message

<table>
<thead>
<tr>
<th>H</th>
<th>E</th>
<th>L</th>
<th>P</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>I</td>
<td>A</td>
<td>M</td>
<td>U</td>
</tr>
<tr>
<td>N</td>
<td>D</td>
<td>E</td>
<td>R</td>
<td>A</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>A</td>
<td>C</td>
<td>K</td>
</tr>
</tbody>
</table>

When the parchment strip is unrolled, the message is read vertically instead of horizontally, and thus becomes the garbled text

HENTEIDTLAEAPMRCMUAK

---

8 Plutarch, Lives Lysander 19
The problem with the scytale is that in order to make use of it, a physical object must be transferred from sender to receiver. It is much more practical to be able only to share the algorithm to be used for decryption. Even more efficient is to have a set algorithm where only a variable parameter, the key, need be mutually acknowledged. The most foremost implementation of this type of cipher is called the substitution cipher. In this scheme, every letter is replaced with another letter according to an explicit mapping routine. One of the earliest and perhaps the most famous substitution cipher is called the Caesar shift and was used by Julius Caesar in his military campaigns. Here, each letter in the plaintext message is replaced by a letter some fixed number of positions down the alphabet. The algorithm is set (i.e., replace each letter with the one \( n \) positions away) where only the number \( n \) need be shared between the correspondents. Seutonius describes Caesar’s method thus:\(^9\)

\[ \text{If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others} \]

I would like to propose that \textit{chochmat yevanit}, the Greek wisdom that was employed in the story of the Hasmonean civil war, should be understood as cryptography, and possibly more specifically as the Caesar shift. As previously noted, that episode took place around the year 65 BC, which corresponds roughly to the time in Julius Caesar’s career when he made the transition from general to politician. Cryptography in the ancient world was primarily studied and developed under Hellenic influence, and therefore, the association of the art of sending hidden messages with Greek wisdom is natural and accurate.

\textbf{The Prohibition}

But why should the Rabbis have taken issue with the study of cryptography? True, in particular case of our story, the enemy was aided by the ability of an old man to get a message across the lines. This, however, was an arbitrary outcome and could just as easily have been used in the other direction. To move from this isolated instance of treasonous behavior to a generic and widespread ban on the study of codes and ciphers seems misplaced.

In truth, the ruling establishment and prevailing institutions have always taken a disapproving posture towards the unauthorized study of cryptography. The regnant position (though by no means, the only one) taken by the Rabbis of the Talmud and by Jewish leaders throughout history was to strengthen the ruling powers that be, as opposed to undermining them. A strong and stable central authority tended to be the best option to ensure the safety of the minority Jewish community which benefited from the hospitality of the host government, and as such, the Rabbis looked to bolster the security of the current regime. The ability of the general population to carry out private and confidential communication was (and is!) seen by the governing bodies as a threat and potential avenue to plot against the regime.

\(^9\) Suetonius, \textit{Life of Julius Caesar} 56
The importance of cryptography has only grown over time as warfare hinged on the use of ciphers and battles were won or lost depending on which side had better expertise in code making and code breaking. The age old conflict between the rights of the individual to privacy and the responsibility of the government to protect itself and its citizens remains contemporary and continues to be hotly deliberated even in modern times. In its current incarnation, this debate has centered on the right to use advanced computer generated encryption algorithms to pass data (files, email, and even voice) in ways that are secure and can not be read or understood by intelligence gathering and local government law enforcement agencies.

During the 1990's, as encryption schemes such as public-private key methods became available, the advocates of freedom of speech fought to publicize these algorithms and make them available to the general public, while governments world wide (and in the US in particular) argued that they be restricted and regulated. The most famous challenge to US export regulations on cryptographic algorithms came from Phil Zimmerman and his Pretty Good Privacy (PGP) encryption program. A 1999 Supreme Court decision upheld that printed source code for cryptographic algorithms was protected as free speech by the US Constitution.

More recently, after the claim that terrorists have used these and other publicly available cryptographic programs to plan and carry out strikes, and particularly after the 9/11 attacks, the pendulum has swung slightly back towards support for tighter control over digital communication. Phil Zimmerman himself was quoted by the Washington Post as reconsidering his advocacy of the individual's rights to absolute and total confidentiality in communication, but later qualified his position.

In these emotional times, we in the crypto community find ourselves having to defend our technology from well-intentioned but misguided efforts by politicians to impose new regulations on the use of strong cryptography. I do not want to give ammunition to these efforts by appearing to cave in on my principles. I think the article correctly showed that I'm not an ideologue when faced with a tragedy of this magnitude. Did I re-examine my principles in the wake of this tragedy? Of course I did. But the outcome of this re-examination was the same as it was during the years of public debate, that strong cryptography does more good for a democratic society than harm, even if it can be used by terrorists. Read my lips: I have no regrets about developing PGP.

Personally, I can see valid arguments and legitimate concerns on both sides of the issue. In any event, this crucial and timely topic found expression within the Talmud whose sages anticipated the arguments and pronounced their position in accordance with their moral, legal, and political world view. Though I am sure this will not be the last word on the issue, it is instructive to take it into consideration. At the very least, the Talmud deserves the right to freedom of speech!

---

10 Phil Zimmermann, Sept. 24, 2001
(www.philzimmermann.com/EN/essays/PRZ_Response_WashPost.html)