Math Circle - Hacking Secret Codes

A **formal grammar** is a collection of four things:

i. A finite alphabet denoted Σ. Elements in Σ are called **terminals**. Usually *terminals* are denoted with lower-case letters. Strings of *terminals* are called **words**.

ii. A finite set of **states** denoted by Ω. Usually *states* are denoted with upper-case letters.

iii. A particular starting state $S \in \Omega$.

iv. A finite set of **rules** for transforming states into words consisting of both *states* and/or *terminals*.

An elite international team of software developers has created an operating system for nine different countries. Each country wants its own set of codes so that if you enter a valid code you are allowed on the system, and if you enter an invalid code you are automatically detected as a spy and dealt with accordingly.

The nine grammars on the next page are used to generate these codes: one grammar for each country. The language that each grammar generates is exactly this set of codes for that country. The alphabet in each case consists of just two characters: $\Sigma = \{a, b\}$. Remember that λ is used to denote the **empty word** of length 0.

You are a member of a notorious ring of global hackers, and you want to try to break in to each of the nine systems. Through some shady black market dealings, you were able to discover this list of grammars. If possible, for each system give at least three different codes which will get you into the system, and also three different codes which will get you exposed as a spy.

To get a little more cash on the side, you also decide to sell these codes to some other group of not-so-notorious hackers. These other guys have no idea what a "formal grammar" is, so you and your team have to first come up with some simple-language explanation of each set of codes (that is, the language which each grammar generates). Happy Hacking!

1. $S \rightarrow aS$
   $S \rightarrow bS$
   $S \rightarrow b$

2. $S \rightarrow aSa$
   $S \rightarrow bSb$
   $S \rightarrow a$
   $S \rightarrow b$
   $S \rightarrow \lambda$

3. $S \rightarrow ABA$
   $A \rightarrow aA$
   $A \rightarrow \lambda$
   $B \rightarrow bB$
   $B \rightarrow \lambda$

4. $S \rightarrow AA$
   $A \rightarrow aS$
   $A \rightarrow \lambda$
   $B \rightarrow bB$
   $B \rightarrow a$

5. $S \rightarrow aSaa$
   $S \rightarrow B$
   $B \rightarrow bB$
   $B \rightarrow \lambda$

6. $S \rightarrow aSbS$
   $S \rightarrow bSaS$
   $S \rightarrow \lambda$

7. $S \rightarrow ST$
   $S \rightarrow TS$
   $S \rightarrow SS$
   $S \rightarrow a$
   $T \rightarrow aTbT$
   $T \rightarrow bTaT$
   $T \rightarrow \lambda$

8. $S \rightarrow U$
   $S \rightarrow V$
   $U \rightarrow UT$
   $U \rightarrow TU$
   $U \rightarrow UU$
   $U \rightarrow a$
   $V \rightarrow VT$
   $V \rightarrow TV$
   $V \rightarrow VV$
   $V \rightarrow b$
   $T \rightarrow aTbT$
   $T \rightarrow bTaT$
   $T \rightarrow \lambda$

9. $S \rightarrow SS$
   $S \rightarrow aSb$
   $S \rightarrow ab$