[0:03](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[If you think back to the start of this course, you learned a little bit](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [about cryptography and implemented the Caesar cipher.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [Now you're going to learn a bit about the Vigenere Cipher, which historically](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [is quite important, as it was thought to be unbreakable for hundreds of years.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[0:20](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[However, as you're going to see and](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [do, the cipher is quite easy to break with the computer.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [Now, let's see how this cipher works.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[0:29](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[The key in Vigenere was classically a word.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [For example, here we picked dice as our key.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[0:36](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[You write down the word repeatedly to match the message length.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[0:42](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[Each letter represents a number for how much to shift by, so](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [dice means shift by 3, 8, 2, and 4, repeatedly.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [In a Java program,](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [it would be quite convenient to represent the key as an array of ints.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[1:00](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[Now to encrypt, you shift each letter by the amount written under it,](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [much like you in a Caesar cipher, but each letter gets shifted by a different amount.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[1:12](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[The first letter is M, which has 3 added to it, so you get P.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [The second letter is E, which has 8 added to it, so you get M.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[1:22](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[Then you repeat this process across the entire message.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[1:27](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[As we did for Cesar, we'll have to skip anything that's not a letter.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[1:32](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)

[Notice that conceptually, this cipher is like four different Cesar cyphers.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [One with a shift of three, shown in blue.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [One with a shift of eight, shown in red.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [Another with a shift of two, shown in green.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [And a fourth with a shift of four, shown in purple.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [This similarity means that a programmer who has already written an implementation](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [of Caesar cipher could make use of it to help implement a Vigenere Cipher.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [In fact, you could make an array of Caesar cipher objects,](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [one with each shift specified in the key and use them for your encryption.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [If you did something like this, you could use the mod operator to wrap](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [a count into the pattern, 0,1,2,3, 0,1,2,3.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [For this mini-project, we're going to give you the code for](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [a Vigenere cipher and you are going to write the code to break it.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [Your goal is to take messages that we have encrypted with Vigenere and](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [find the decrypted message without knowing the key we used.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [You will start with breaking a message that you know is in English,](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [and then expand your program so](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction) [that you can try to break encryption in a variety of languages.](https://www.coursera.org/learn/java-programming-arrays-lists-data/lecture/GRRkv/introduction)