About Project

* Information security
  + FIG: Stock image related to data
  + Digital information is everywhere. Lots of sensitive data
  + High-profile hacks and leaks and breaches
  + Need public to better understand how security works
* Learning information security with the BBC micro:bit
  + What micro:bit is
  + FIG: photo of microbit program working
  + Send and receive messages over wireless radio
  + Protect messages from eavesdroppers
  + Develop your own secret codes
* Teaching tools
  + [If we have time to develop them]
* Learning more
  + Resources for information security and cryptography
  + More about programming and the micro:bit
* About the project
  + FIG: photo of us holding microbits outside ARM
  + ARM Intern Innovation Challenge
  + About the team

Built It!

* Get started with the micro bit
  + FIG: picture of micro:bit
  + Link to BBC page
  + Setting up the micro:bit for [language]
* Send a message over the radio
  + About the micro bit radio
    - micro:bit has a built in radio that can send messages to other micro:bits
    - Radio is very complicated, but micro:bit makes it easy!
    - Link to documentation on radio
  + Code to send text message over radio
  + Code to receive text message over radio
  + FIG: photo of working message transmission
  + Radio broadcasts message to everyone within range. They can read it if they also have a micro:bit with the radio receive program
* Disguising messages
  + Problem: Everyone can see the message!
  + FIG: Message broadcast from Alice to Bob with Eve eavesdropping
  + Solution: Scramble the message so that the person who you want to receive it can understand it but other people who see it can’t.
  + FIG: Diagram of scrambling message with secret key
* Ciphers: disguising secret messages
  + About ciphers
    - Way of scrambing a message in a way that it can be unscrambled, but only if you know a secret that was used to scramble it.
    - Secret is sometimes called a key. It’s like a password.
    - Anyone who doesn’t know the key will get nonsense.
    - To keep the cipher safe you have to keep the secret safe. A really strong lock is no good if everyone has the key.
  + Caesar cipher
    - Used by Julius Caesar to send messages to his army
    - Replace every letter by another letter in alphabetical order, wrapping around from Z back to A.
    - The secret key is the number of letters you skip.
  + FIG: letter substitution diagram
  + Code to encode Caesar cipher
    - How the code works
  + Code to decode Caesar cipher
    - How the code works
* Building better ciphers
  + Caesar ciphers are easy to break
    - Just try every shift until the letters make sense
  + Can you come up with a better method?
* Protecting other data
  + What if you want to protect an image? Or any other file?
  + Computers store data as zeros and ones.
  + Code to send image
  + Code to receive image
* Bit flip cipher
  + Bit flip cipher
    - Same thing encodes and decodes!
  + Diagram of bit flip cipher
  + Code to encode and decode image
    - How it works
* Breaking the bit flip cipher
  + Is there a way to break the bit flip cipher?
  + In theory, totally unbreakable, as long as it’s only used once!
  + If you use the same pattern of flips over and over, you can guess the pattern
  + Can you think of a better way?
* More advanced encryption
  + Links to more resources on encryption
  + Dump Sam’s code on them