

How IoT(Internet of Things) Has Changed Our Lives



Internet of Things (IoT)

IoT and Security

Diverse IoT Services



How to Use This Program

Software is changing the world. The programs installed in computers and apps that make it more convenient to use smartphones are all software. Software is in every part of our lives, so it is difficult to find areas where we are not affected by software.

The state-of-the-art science and technology that we see in the news is also helped by software. In turn, progress in math, science and technology advances software further. As such, math, science and technology are closely related with and cannot be separated from software.

These module series were created through collaboration between experts in related fields and software education, and its suitability for classrooms has been verified. As students follow teachers' direction through each module, they will be able to better understand the world that has been changed by software.



software

education module

CONTENTS

Intro	IoT That Communicates without Talking!	02
PART1	Internet of Things (IoT)	08
Activity1	Make your home smart, create a smart home	13
PART2	IoT and security	18
Activity2	Collecting friends' birthday information with RSA encryption	22
PART3	Diverse IoT Services	24
Activity3	Making smart bulbs	28
Career Exploration	IoT developer	32
Maker Activity	Make an IoT parking system	34





IoT That Communicates without Talking!

"As I rushed out of my house, I left my electric stove on! I'm on a week-long business trip. What should I do?"

Mr. Blink left home almost an hour ago. Should he go back home? Not at all. As there has been no sign of human movement, the lighting that decided the house was empty already turned off the stove.

When IoT is realized in every corner of life, this kind of scenario will become normal. IoT that we see in the news or advertisements! How does it work? Let's take a closer look.



HERE COMES THE AGE OF IOT!

“The age of IoT will be an age of superconnectivity where all devices and products talk to each other.” This is how globally renowned futurist Jeremy Rifkin (President of the Foundation on Economic Trends) describes the future. It means that objects will exchange information by themselves without humans in the middle to connect them. This “Internet of Things”, objects connected through a network, is drawing attention as a key technology of IT. For short, it is called IoT.

Objects around us are already connected through the Internet. We can see the photos we took on a TV screen right away and print out what we wrote with a smartphone. However, humans still need to connect the camera to the TV and the smartphone

With IoT, not only smartphones and computers but also all objects around us including cars, street lights and cameras are connected to the Internet. And there are no borders in their interaction.



to the printer. In the future, however, objects will not only do such simple tasks by understanding the situation on their own but also complete more difficult tasks by themselves. For example, lighting that decides there is no one home will communicate this to the electric stove and it will shut off to prevent a fire.

Less than 1% of objects are currently connected to the Internet. There are around 1.5 trillion objects in the world, and around 10 billion of them are connected to the Internet. 10 billion sounds like a lot, but it means that less than one out of a hundred objects around us is connected to the Internet. However, a report published in 2013 stated that 24 billion objects will be connected to the Internet by 2020. As time goes by, the number will continue to increase. Eventually, we will enter the age of “super-connectivity” when most of the objects around us are connected as one.

The key to IoT is sensors!

In the age of IoT, “sensor technology” that enables the quick recognition of changes in the environment is the key technology.

The tactile sensor developed by ETRI’s Ph. D.Ki-uk Kyung’s team. The sensor, that is thin like a film, can be conveniently attached to anywhere like clothes or objects.

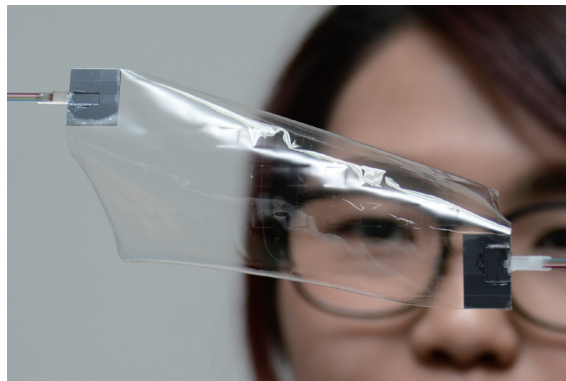
A sensor is a device that converts information such as temperature, pressure and speed into an

electric signal. Sensors are categorized based on what is being measured, and we are most familiar with sensors that measure physical information such as temperature sensors, humidity sensors and pressure sensors. There are also bio sensors that measure health status information such as heart beat, blood pressure and blood sugar. Sensors are also being actively developed that recognize human faces, motions and brain waves to measure our changing thoughts.

However, even the best sensor can be hard to attach to a product if it is too big or thick. So, it is also important to develop sensors that can be easily attached to objects and are flexible.

In June 2014, the research team of Ph.D. Ki-uk Kyung of the Electronics and Telecommunications Research Institute (ETRI) developed a tactile sensor that is so thin that it can be freely rolled or bent. The research team attached a transparent film to an almost invisibly thin and long pipe and passed light through one side of the pipe. So, if one touches the film, the amount of light that reaches the other side changes as the path of the light is disturbed. The difference in light is detected by the sensor on the end of the pipe, and it measures information such as where or how strong the touch was.

The film is thinner than hair and can be easily attached anywhere. If attached to human skin, the human body itself becomes a sensor - "smart skin".



The tactile sensor developed by ETRI's Ph. D.Ki-uk Kyung's team. The sensor, that is thin like a film, can be conveniently attached to anywhere like clothes or objects.

New internet address is needed

For objects to be connected to the Internet, a unique Internet address (IP) is needed. The current Internet address system is "IPv4", which is like "210.113.039.224", and up to around 4.3 billion (232) addresses can be created. However, as the number of objects connected to the Internet will increase to 24 billion by 2020, far more Internet addresses are needed. To resolve this issue, "IPv6" has emerged as an alternative.

With IPv6, it is possible to allocate 4.3 billion⁴ addresses by using numbers expressed in hexadecimal value. As it is possible to almost infinitely create Internet addresses, there is no need to worry about running out of addresses even when the number of connected objects increases exponentially.

As with all devices connected to the Internet, security is also an important issue with IoT. In the

PREVENT HACKING!

world of IoT, countless sensors on the body, at home and even on the streets collect information at all times. Some of this information might be so minor that you would not care if anyone knows it, but some could be used by someone to harm you. In fact, maybe there is no such thing as minor personal information. With the smart TVs and refrigerators that are being launched today, we are taking steps toward the age of IoT, but these products do not even have IDs or passwords, which are so common elsewhere.

According to Korea Internet and Security Agency (KISA), economic damage by IoT hacking could amount to around 18 trillion won. Considering the same numbers are 2.7 trillion won for natural disasters and 4.6 trillion won for cyber attacks, the number is huge.

A spoon turning into a zombie PC?

Security is even more important with IoT because all objects are connected as one. It only takes one object to be hacked to paralyze the whole IoT network.

One of the most common hacking methods around the world is a “DDoS attack”. DDoS is a way of paralyzing a whole system by turning a certain computer into a zombie PC. In the world of IoT, not only smartphones and computers but even a spoon or a chair could become a zombie PC.



In January 2014, the US security company Proofpoint disclosed cyber attack cases using appliances such as TVs or refrigerators. According to the company, for around 15 days from December 23, 2013, to January 6, 2014, 750,000 malicious emails were sent.

Korean security companies already demonstrated a few years ago how home audio equipment and printers can malfunction when they are infected by malicious codes. Another warning is that if a TV with a camera is hacked, viewers’ private lives can be filmed secretly and relayed through the Internet. Another possible new crime is that a smart TV’s home shopping program can be hacked so that when the viewer places an order, the money is transmitted to the hacker.

By hacking a car, hackers can manipulate the speed or direction of the car to cause accidents. As

this could be possible simply by connecting a circuit board that only costs tens of thousands of won, to enjoy the convenience of IoT, comprehensive security systems should be established at the same time as product development.

Efficient encryption algorithms are needed

For this reason, there is a lot of ongoing research on encryption for IoT devices.

Basically, an encryption algorithm goes through the process of encryption and decoding. The process of converting certain messages through a mathematical formula is called “encryption”, and the process of solving the encryption and converting it back into the original message is called “decoding”. The encryption algorithm commonly used for IoT is “PRINCE”, which was proposed by Julia Borghoff of the Technical University of Denmark in 2012. PRINCE is broadly used because its decoding process is very simple, making it possible to use a chip that is 10 times smaller and less electricity than other encryption algorithms.

To protect information, we can also consider disclosing information selectively with encryption technology. In other words, we can grade information based on its importance level and use settings so that only the desired information is delivered to the server. Through this, we can disclose only part of our information or make it public only to the person or group we want.

Slower but safer can be a better way

One of the areas where IoT can be helpful in life, going beyond simple convenience, is medicine. If a patient with heart disease or diabetes attaches sensors to the body, the sensors can immediately detect when there is a problem and communicate this to the hospital, enabling the patient to get quick treatment. The information collected by sensors is gathered in a “Gateway” and then delivered to hospital servers.

The problem is that hackers can steal the information during this process. To prevent this, SDN (Software Defined Network) security, where the information takes a safer route instead of the existing route, is emerging as one of the ways to ensure information security.

Let’s assume patients’ health information was hacked while it was being delivered to hospitals following the existing route. A sensor would immediately block that route and find another safe route to send the information to hospitals.

As such, IoT should chase two hares - information delivery and security - at once.

While perfect encryption technology is needed for information protection, using different routes of disclosure through SDN security is emerging as a slower but safer alternative.



PART 1

Recommended target

Elementary creative experience activities

Relevant subjects

Practical course, elementary school

IoT(Internet of Things)

* RFID

RFID refers to technology that enables the identification of objects using Radio Frequency. It is also called electronic tags and smart tags, etc. RFID is composed of tags that contain information such as the object's name, date of manufacture, etc., and the reader that can read the tags. It is conceptually similar to the barcodes that are currently broadly used but it can contain far more information than barcodes and the reading speed is far faster.

The term “IoT” was first used in 1999 by Kevin Ashton of P&G, a company that manufactures and sells soaps and shampoos. Working as a brand manager, he thought if RFID* or sensors were applied to the objects in our daily lives, they could also exchange information among themselves. This meant that not only computers but also general daily goods could be connected to the Internet. When the Internet was still relatively new, the IoT he described seemed like something that could only be realized in the far future. However, in less than 20 years, what is the world we are living in like? We have already entered the age of IoT.

What is IoT?

You may have seen the electronic displays that show where the bus you should take is now and how long it will take to get to your stop. Of course, you can also check this information with smartphone apps.



IoT refers to general objects used in our daily lives connected through a network and exchanging information.

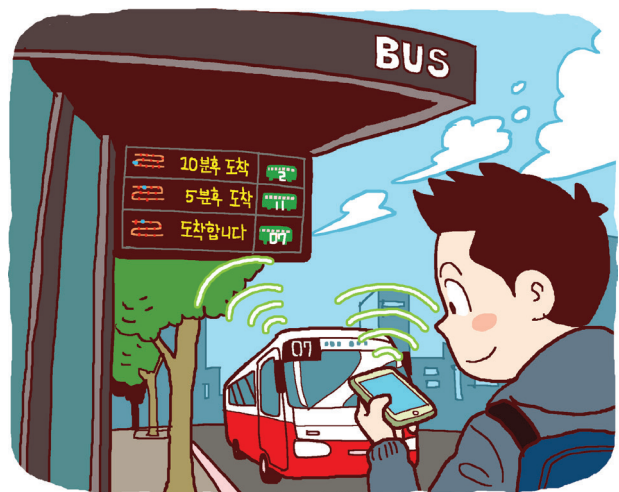
This “bus information system” is a great example of IoT. The bus information system locates the buses in real-time through GPS receivers and wireless communication devices installed on the buses and calculates its operational status or estimated arrival time. When this information is sent to server, the information is then transmitted to the electronic displays at bus stops or smartphones.

While there are various definitions of IoT, they commonly have the following three characteristics.

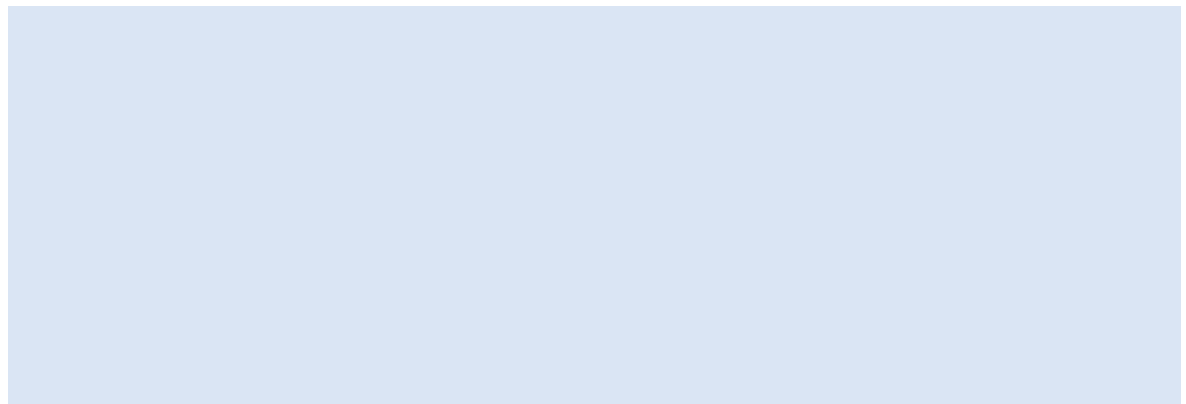
First, each object has the intelligence to collect and analyze data on its own and execute given commands. Intelligence here does not refer to the tremendous power of artificial intelligence. It means that the object can carry out functions independently without humans giving commands for every detail.

Second, each object should be connected through a network. This means that information can be exchanged between objects or between objects and humans.

Lastly, the information created by the objects connected through the network is not only delivered but also used to provide new services. This means that it should provide services helpful in our daily lives like buying tickets to performances or exhibitions based on the personal schedules saved in smartphones and show transportation.



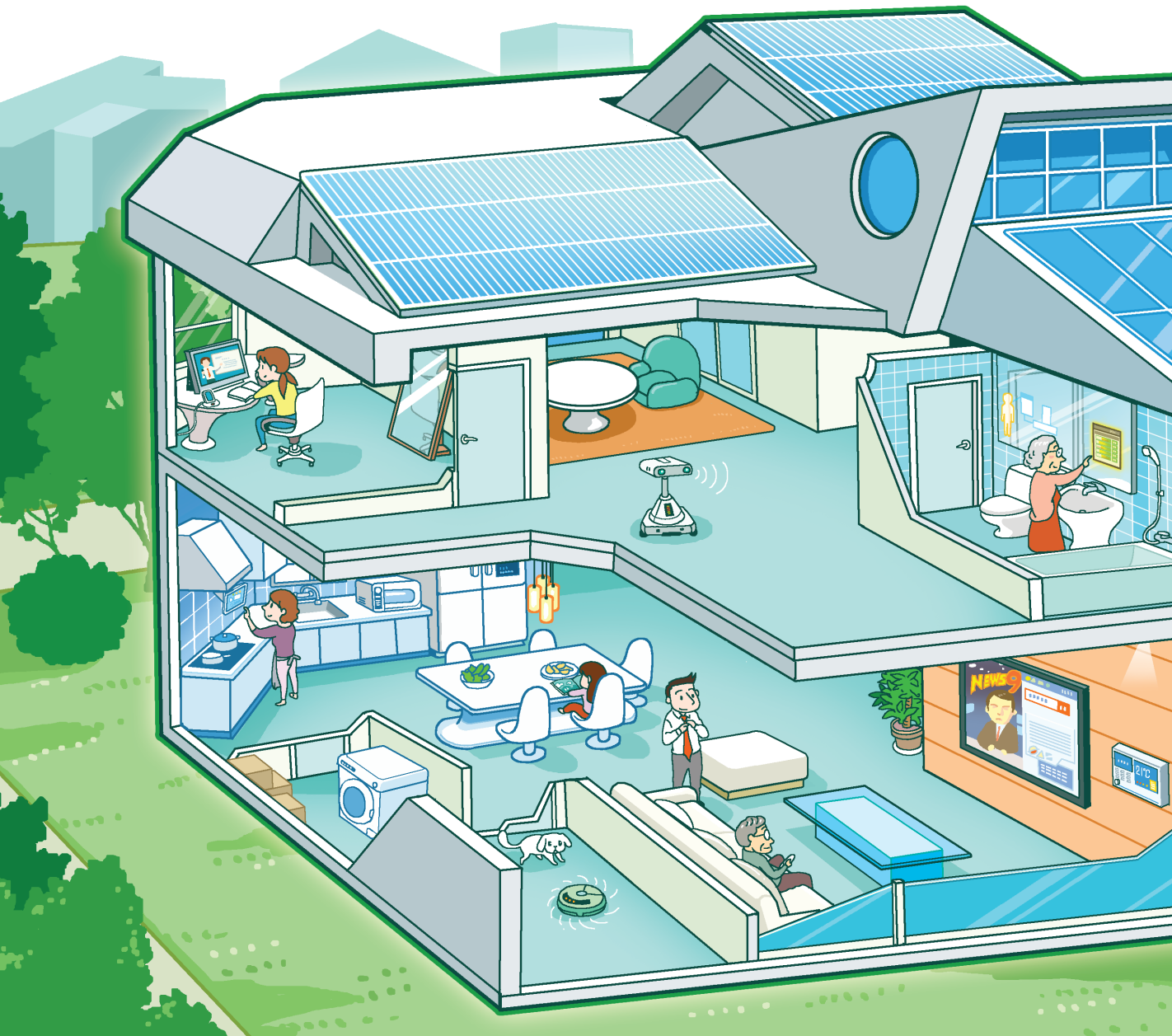
The bus information system that lets us know when our bus will arrive at the stop through sending the bus' operating information including location and speed to a server is a type of IoT.

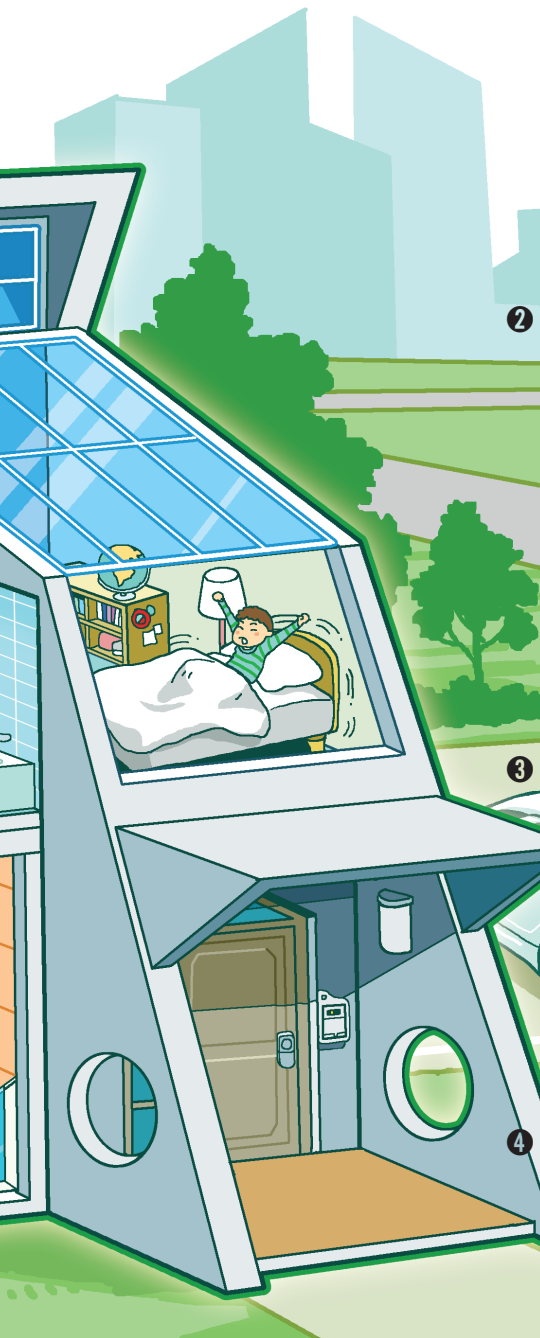




Components of IoT Four components of IoT

Korea Internet and Security Agency, which comprehensively manages matters related to the Internet in Korea, lists the four key technologies of IoT as follows. Read the description right Consider how the core technology used in smart home.





1 Sensing | This is the key technology of IoT that gathers information on the surrounding environment by attaching sensors to objects or venues and delivers the information in real-time. It includes everything from sensors for temperature, humidity, heat and gas and ultrasonic sensors that are already commonly used in other areas as well as physical sensors that detect changes in the surrounding environment and objects. Sensing technology can gain information using remote detection, Specific Absorption Rate (SAR), radar, location, movement and image sensors. In other words, perceiving the surrounding environment through diverse sensors and processing the collected information based on users' demands is the key technology of IoT. Today, such physical sensors are being developed into smart sensors that can process information.

2 Wired/wireless communications and network infrastructure |

Infrastructure refers to foundation facilities or groundwork. Put simply, it means the basic environment required to broadly utilize and develop certain technologies into an industry. In terms of IoT, it is the technology that supports the connection of objects to the Internet such as the provision of IP or the installation of wireless communications equipment.

Diverse network technologies commonly used today are included in this and can be categorized into wired communications, wireless communications networks (3G, 4G), wireless LAN (WiFi) and WPAN (Bluetooth, Zigbee, RFID, NFC), etc. WPAN refers to a personal communications network where information can be wirelessly exchanged within 10m.

3 Service interface | This refers to technology that changes the information objects have based on the contents and forms of services or converts many technologies, etc., to help IoT operate efficiently. Diverse technologies including Big Data technology, security and authentication and web service, etc., are used. The Semantic Web is also included. This refers to the web for computers, instead of the general web where people visit websites, access needed information with a keyboard or mouse and make commands. As IoT objects need to mutually exchange information, the technology to create such a web is essential.

4 Security | This refers to the technology to prevent hacking and information leakage. The function or method of execution of IoT or the network environment differ based on where it is applied. Therefore, in terms of information security, which is of critical importance in IoT, the most appropriate technology based on the characteristics of the object should be applied.



Hot IoT items that we will carry on our body!



When the age of IoT is fully ushered in, many devices we carry now will be connected to the Internet and upgraded to be smarter. Let's take a look at what their functions will be.

Smart earrings

These can also be used as earphones, sometimes playing relaxing music when you are stressed.

Smart watch

You can check the weather and current location as well as time. You can also make a phone call.

Mobile phone charger

A sensor converting body heat to electricity is attached to your clothes, automatically charging your nearby mobile phone.

Smart shoes

They can adjust the temperature in your shoes and show destinations and directions by using GPS and LED. They also let you know where you should go when you need to change directions.

Smart glasses

It is possible to run a program or search data by accessing the Internet by blinking. The search results will be displayed on the lens.

Smart necklace

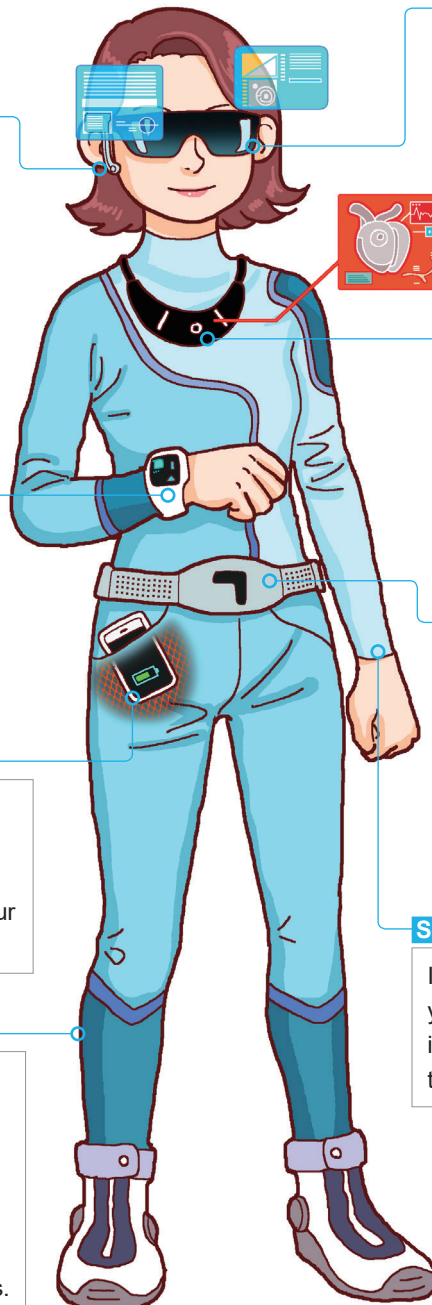
It checks health status such as heartbeat and body temperature and immediately alerts the primary doctor in an emergency.

Smart belt

It measures waist size and breathing rate. It can recommend rest if you sit for a long time working or eat too much.

Smart band

It projects images on your arm to show health information, location, time and weather, etc.



Activity 1

Make your home smart, create a smart home

If you look around your home, there are many devices that operate automatically, including a boiler that turns on and off based on the set temperature, lighting that uses a timer and a robot cleaner that cleans and recharges itself on its own. However, taking one step further, these devices are now connected to the Internet so that you can operate the boiler from outside the home and search recipes from the monitor on the refrigerator door. These are examples of IoT in our daily lives. Just like the mobile phone became a smartphone when connected, your home becomes a smart home thanks to IoT. Why don't we make a smart home service with simple programming?

What to prepare Computer that can run Scratch

Activity

1 Plan a smart home project

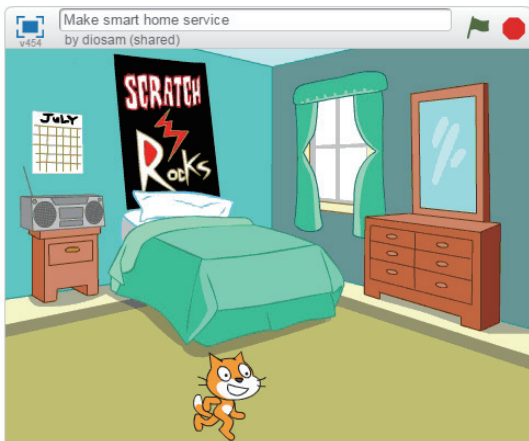
- ① Explore smart home functions using diverse sensors.

Sensor name	Sensor description	How to be utilized in a smart home
Distance sensor	Measuring the distance between objects and the sensor	
Human body detection sensor	Detecting motion to see if someone is home	
Illumination sensor	Detecting the brightness of light	
Gyro sensor	Detecting the inclination and acceleration of objects	
Pressure sensor	Measuring the level of pressure from pushing	
Temperature/humidity sensor	Measuring temperature/humidity	

- ② Think about what kind of smart home service to make with which sensor.
Think about how to make a sensor control two or more devices.

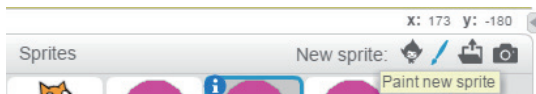
2 Programming

① Make a background screen.



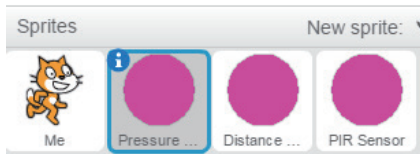
Click <Choose backdrop from library> and choose the home background.

② Create a sensor Sprite.



Create a Sprite to use as a sensor by selecting <Paint new sprite> from the Sprite panel.

③ Copy the sensor Sprite and change its name.



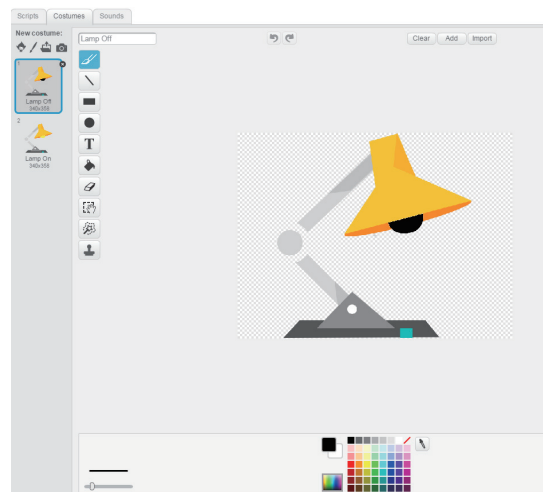
Simply create a sensor Sprite using a circle shape and change its name.
E.g., pressure sensor, distance sensor, PIR sensor

④ Place lamp, door and sensor Sprites.



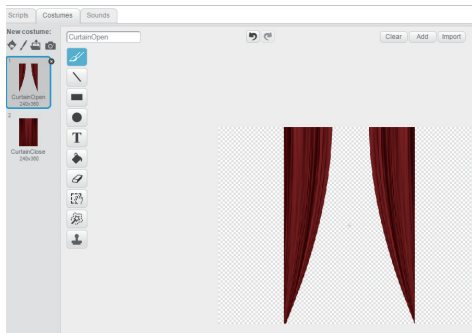
Select <Upload sprite from file> and take a lamp and door and place them as above. Place a human body detection sensor in front of the door, pressure sensor on the bed and distance sensor in front of the mirror.

⑤ Add the lamp Sprite shape.



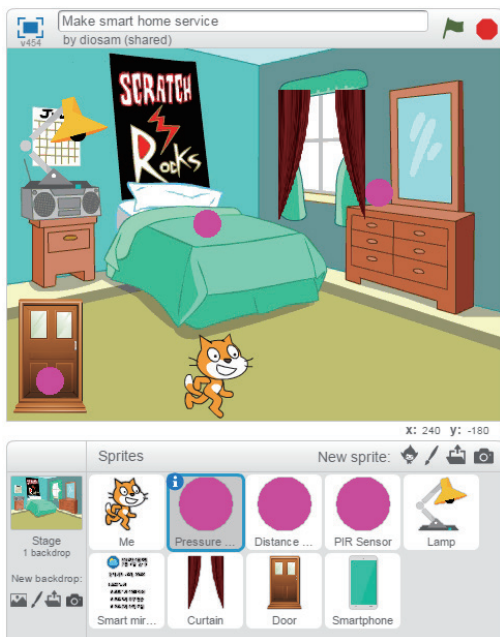
Copy the lamp and change the color of light. Color <Lamp Off> with black and <Lamp On> with yellow.

⑥ Add a curtain Sprite.



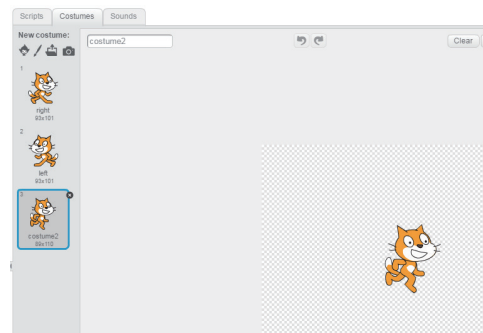
Open an image file in the shape of a closed curtain and add an image in the shape of an open curtain to make a curtain Sprite. Adjust the size of the curtain Sprite and move it to the place for the curtain in the background.

⑦ Change the location and name of the Sprite.



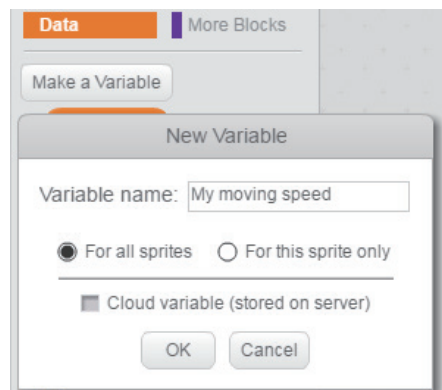
Finally, place them as above and change the name of the Sprites.

⑧ Add a direction of cat Sprite.



Copy a cat Sprite and change the direction to right/left and make two cat shapes that face right and left.

⑨ Create a variable of my moving speed.

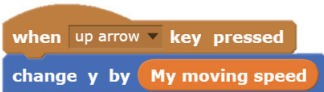


You will make the cat move using direction keys. To make it easier to adjust moving speed, create a "my moving speed" variable.

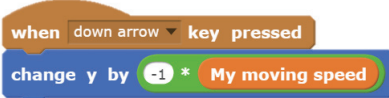
⑩ Input the cat's moving script.



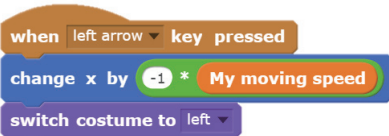
As it may be located behind other Sprites, change the order to put it in the front and set the moving speed at around 20.



Make it change Y coordinates when clicking the up arrow key.



To move downward, make it negative by multiplying -1 on moving speed.



Make the cat face left when moving to the left.



Make the cat face right when moving to the right.

⑪ Input the lamp script.



Input the event that the lamp will execute when the lamp Sprite receives a broadcast. We will make the lamp Sprite change colors when the cat Sprite contacts the pressure sensor and sends the broadcast.

⑫ Input the curtain script.



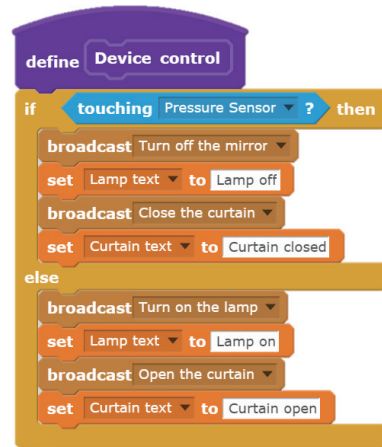
Also, change the curtain Sprite to change its shape to open/closed when receiving the broadcast.

⑬ Add variables.



Add the variables “lamp text” and “curtain text” to mark the status of each device on other devices.

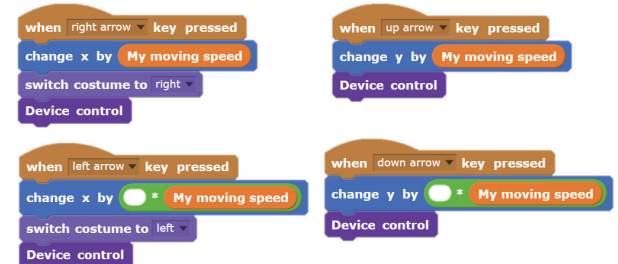
⑭ Create additional blocks.



Create additional device control blocks to use one control script in many places.

If a cat Sprite contacts the pressure sensor on the bed, decide that the cat is lying down to sleep and turn off the lamp and close the curtain. Otherwise, turn on the lamp and open the curtain.

⑮ Add additional blocks for device control.



Check whether the additional blocks for device control are executed and detected by sensors every time the cat Sprite's direction keys are pushed.

⑩ Add a smart mirror Sprite.



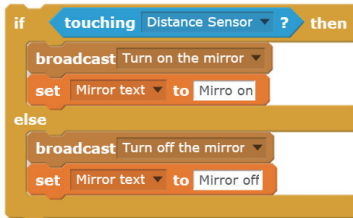
Open the smart mirror image, create a smart mirror Sprite and place it on the mirror.

⑪ Input the smart mirror script



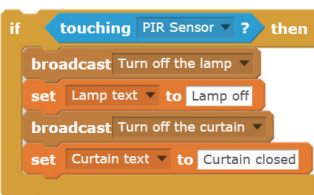
Input showing/hiding the script when the mirror Sprite receives the turn on/off broadcast, respectively, and input greetings.

⑫ Add the distance sensor script



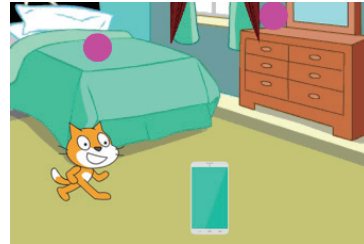
Add script to the additional device control bloc so that the smart mirror turns on when the cat contacts the distance sensor in front of the mirror and off when it goes away from the mirror.

⑬ Add the PIR sensor script.



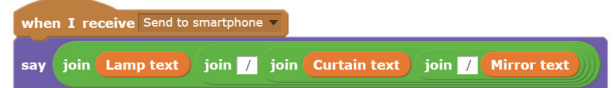
Add script related to the human body detection sensor in front of the door to the additional device control bloc. Make it turn off the lamp and close the curtain by recognizing that the cat has left home when the cat is in front of the door.

⑭ Add a smartphone Sprite.



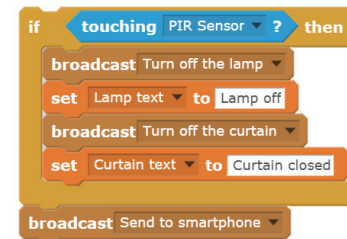
Create the smartphone Sprite by using a smartphone image.

⑮ Add the smartphone script.



Mark the status of the lamp, curtain and mirror as currently at home when sending a transmitted broadcast to a smartphone

⑯ Input the script showing the smartphone status in the additional device control block.



Add the “transmitting broadcast to smartphone block” to the end of the additional device control block.

⑰ Go further.

If you have functions that you want to add, add sensors and devices controlled by the sensors.

PART 2

Recommended target
middle school liberal semester

Relevant subjects
Property of the natural numbers in math
2nd grade, middle school

IoT and Security



In the “superconnectivity” society where the number of objects connected to the Internet through IoT increases exponentially, the issue of the security of personal information will become even more important. With objects exchanging more personal information as our lives get more convenient, we also need strict security and systems to minimize the damage of hacking. We also need institutional support so that individuals can have the “right to informational self-determination”.

* Right to informational self-determination

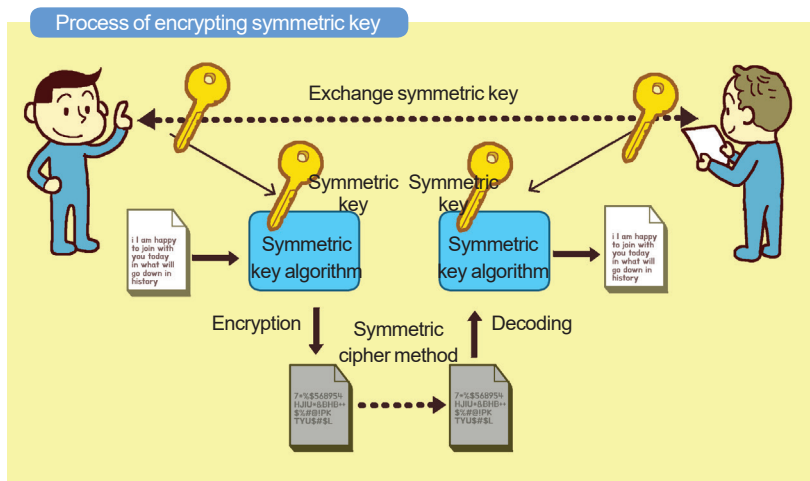
This refers to one’s right to determine when, where, to whom and what kind of personal information is delivered and utilized.

The most basic way to protect information is to encrypt and deliver it. As all IoT objects are connected through the Internet, someone can invade in the network between objects and steal information. Therefore, the encryption of information makes it impossible to know what the information is about even if it is stolen. The methods of encryption are largely divided into symmetric key ciphers and asymmetric key ciphers.

Symmetric key ciphers using the same key for encryption and decoding

The symmetric key cipher method is the representative encryption

method that has been used in the past. With this method, the same key is used for “encryption”, which is the step of encrypting information into the cipher, and “decoding”, which is converting the cipher back into the original information. Therefore, the encryption side and decoding side need to share the



encryption key.

The symmetric key cipher method has the advantage that it enables the exchange of encrypted data using relatively less computing resources thanks to its fast encryption calculation speed. However, as both the provider and receiver of information use the same encryption key, the encryption key is more likely to be leaked. Moreover, when exchanging information with multiple people, there is the hassle of having to make, maintain and manage many encryption keys. The symmetric key cipher method can be further divided into block cipher and stream cipher.

① Block Cipher | This is a way of dividing general information (plain text) that is not encrypted into specific units and encrypting each unit. Changing the location of letters or replacing one letter with another letter fall into this category.

By repeating the methods of changing the location of letters and replacing certain letters with other letters, it is safe to make a cipher as it is almost impossible to identify the contents of the sentence.

② Stream Cipher | Unlike a block cipher, this is a way of encrypting by sequentially processing the data stream* by bit unit. For example, A is converted to its binary number, 1000001, and it is encrypted with the encryption key (key stream) of “1110011” and “XOR operation*”. A stream cipher is often used when data should be encrypted while it is being transmitted as its encryption speed is fast.

Public-key encryption

In 1976, Whitfield Diffie and Martin Hellman proposed using two encryption keys instead of one. The two keys are the private key and public key and they can be used only as a pair.

The public key is disclosed to anyone and it can encrypt information but cannot decode information. Decoding is possible only by using the private key. So, when several people send information to one receiver, if each of them sends information using their public key, the receiver can decode the information by using the private key.

* Stream

Stream is the flow of data sequentially transmitted. You don't need to wait until you download all of the data when you watch a Youtube video because the streaming technology processes the inflow of data in real-time.

* XOR operation

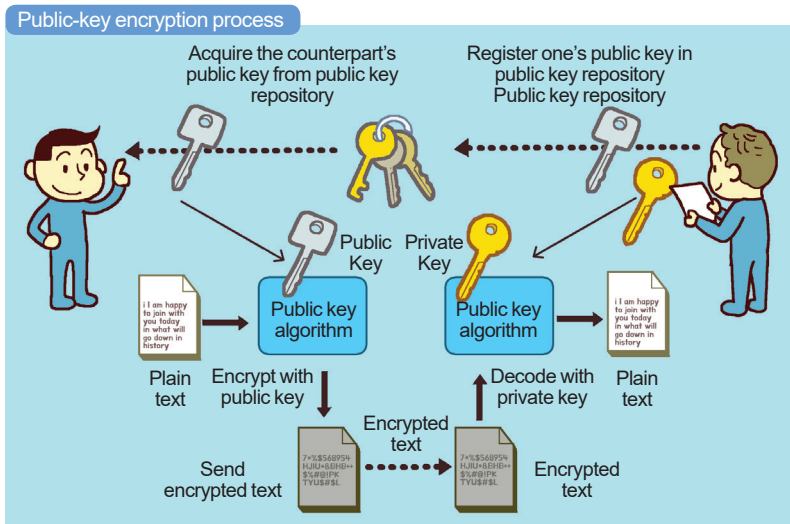
명제 P	명제 Q	$P \vee Q$
1	1	0
1	0	1
0	1	1
0	0	0

XOR operation is a logical operation that takes it as true when only one of the two theses are true.

As demonstrated in the above table, it produces 1 when only either P or Q is 1, and 0 when both are 1 or both are not 1.

Therefore, in the example on the left, the XOR operation of “1000001” and “1110011” is “0110010.”

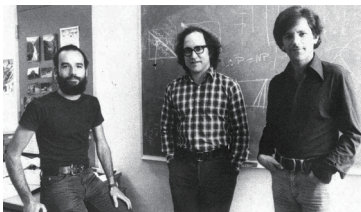
$$\begin{array}{r} 1000001 \\ 1110011 \\ \Rightarrow 0110010 \end{array}$$



Therefore, the public-key cipher method has the advantage of exchanging encrypted information without sharing the key to decode the cipher with others because, while anyone can carry out encryption, only the one with the private key can decode it.

The public-key cipher method is designed based on challenging mathematics and complicated mathematical

operations are required for encryption or decoding. Therefore, it is slower than the symmetric key methods.



From the left, Shamir, Rivest and Adleman. In 1977, they opened a new chapter of encryption by developing the RSA encryption algorithm. © www.ams.org

RSA encryption algorithm

In 1977, the three MIT students Rivest, Shamir and Adleman published their newly developed encryption algorithm. Taking the first letter of their names, this algorithm is called the “RSA algorithm”. By actually realizing the concept of public-key encryption, they opened a new chapter in the history of encryption.

The reliability of the RSA encryption algorithm is based on the idea that it is very difficult to do prime factorization of a very big number. Let's assume that we get n by multiplying the prime numbers p and q .

$$p \times q = n$$

If $p=11$ and $q=3$, n is 33. It is also easy to find that 33 is the product of $p=11$ and $q=3$ through the prime factorization of 33. But if the value of p and q gets bigger, while it is easy to find the product (n) of the two values, it is very difficult to find p and q through prime factorization.

When n is 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541, it takes decades even for a super computer to find p and q .

How does the RSA encryption algorithm work?

By utilizing this characteristic of prime numbers, the RSA encryption algorithm produces the public key and private key. This process is very difficult to understand, even at the middle-school level. For reference, just take a look.

Production of keys

1. When p and q are prime numbers, calculate $n=p \times q$.
2. Subtract 1 from p and q respectively and multiply them. Call this result ϕ .
 $\phi = (p-1)(q-1)$
3. Find e that satisfies all of the following.
 $1 < e < \phi$, $\gcd(e, \phi) = 1$
(Find e that is bigger than 1 but smaller than ϕ with the greatest common denominator as 1. The greatest common denominator being 1 means that e and ϕ are prime numbers with only 1 as their common denominator.)
4. Find d that satisfies all of the following.
 $1 < d < \phi$, $ed \equiv 1 \pmod{\phi}$
(Find d that is bigger than 1 but smaller than ϕ with the remainder being 1 when dividing $e \times d$ by ϕ .)
5. Now, (n, e) is the public key, and (n, d) is the private key.

Reference) $\gcd$ is the symbol for greatest common denominator, and mod is the symbol for finding the remainder.

$\equiv$ is a symbol for congruence.

After producing the public key and private key using the above method, when B wants to send message m to A, it sends it as the following.

Encryption $c = me \text{ mod } n$ (c is the remainder of me divided by n)

B sends the encrypted message c to A. A decodes it using the private key as follows.

Decoding $m = cd \text{ mod } n$ (m is the remainder of cd divided by n)

For example, if the public key (n, e) and private key (n, d) found through the above key production algorithm are $(33, 3)$ and $(33, 7)$ respectively, one can encrypt and decode as follows. Here, let's send the message 7.

Encryption $c = me \text{ mod } n \rightarrow c = 7 \times 3 \text{ mod } 33 \rightarrow \text{remainder of } 21 \text{ divided by } 33 \rightarrow c = 21$

Decoding $m = cd \text{ mod } n \rightarrow m = 21 \times 7 \text{ mod } 33 \rightarrow \text{remainder of } 147 \text{ divided by } 33 \rightarrow m = 7$

Activity ②

Collecting friends' birthday information with RSA encryption

The RSA encryption algorithm begins from the assumption that prime numbers are infinite and it is very difficult to find two prime numbers through the prime factorization of a very large number. Let's explore the RSA encryption algorithm through the process of the prime factorization of the product of two prime numbers with friends.

What to prepare Scientific calculator or computer connected to the Internet

Activity

1 Prime factorization

- ① Select two prime numbers below 20 and exchange the product of the prime numbers with each other. Do not share the two prime numbers you chose with your partner.
- ② Find the two prime numbers multiplied through prime factorization of the numbers you exchanged with each other.

2 Find remainders

One of the critical parts of the RSA encryption algorithm is the operation to find the remainder. The remainder operation is also used in very diverse ways in other areas of computer programming. Solve the below question and fill in the empty cells. Here, mod is a symbol of operation that refers to the remainder when the former number is divided by the latter.

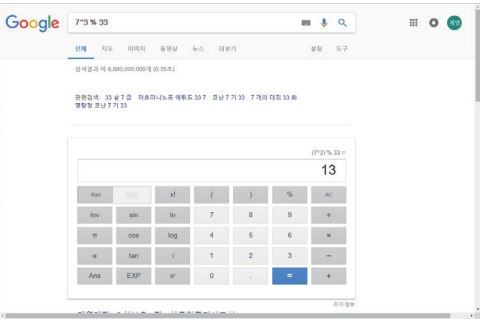
e.g., $6 \bmod 4 = 2$, $8 \bmod 5 = 3$, $100 \bmod 10 = 0$

20 mod 6	
36 mod 4	
17 mod 9	
88 mod 9	

3 Encrypt and exchange birthdays

Now, let's exchange information using the RSA encryption algorithm. It requires a very complicated mathematical operation to create the public key and private key. However, if the keys have already been created, we can easily encrypt and decode information with calculators.

Select one of the public key-private key pairs below and decode your friends' encrypted birthdays. Share the public key with your friends and send it encrypted. By entering the equation in a scientific calculator, Windows' calculator app or the Google search box, you can get automatic calculation results.



E.g., If you are using Google search, enter 73 mod 33 as “7^3%33” in the search box. Here, % is a symbol of operation to find the remainder and the results are the same if you enter mod, i.e. 7^3 mod 33, instead of %.

Public key (n, e)	Private key (n, d)
(33, 7)	(33, 3)
(187, 7)	(187, 23)
(119, 5)	(119, 77)
(143, 23)	(143, 47)

4 Resolving the RSA encryption algorithm

So far, the RSA encryption algorithm is recognized as one of the safest encryption algorithms. However, just as there is no perfect thing in the world, someday a way to easily break the RSA encryption algorithm will be developed. How could we break the RSA encryption algorithm? Freely write down your ideas.

PART 3

Recommended target

Elementary creative experience activities

Relevant subjects

Practical course, elementary school

Diverse IoT Services

Just as there are endless things we need in our lives, companies around the world are competing to launch IoT services in diverse areas. From traditional chipset manufacturers to home appliance makers, communications firms and automobile makers, companies are making services that we have never experienced based on creative ideas and technology. Let's take a look at some of these interesting IoT services.

Taking responsibility for health — healthcare

A longer, healthier life is one of humanity's oldest desires. And thanks to this desire, impressive and intelligent health management products continue to appear one after another. While these are currently at the stage of sensors simply identifying users' health status, it will be possible to not only diagnose but also treat diseases when related technology advances further in the future. Already, renowned hospitals around the world are demonstrating smart hospital systems by introducing IoT technology.



Vitality's smart medicine bottle. This bottle let users inform users that it is time to take medicine through light and sound on the present times. © Vitality

Smart medicine bottles | Those with tuberculosis, diabetes or high blood pressure need to take medicine on a regular basis. Vitality, a US company, launched a smart medicine bottle that enables users to take their medicine following a schedule. This product lets users know it's time to take their medicine through light and sound on its lid according to pre-set times. If the lid is not opened after the pre-set time, it even calls the users' mobile phone or home phone to let them know it's time to take their medicine. The patients' records of taking medicine are saved on Vitality's server, and Vitality organizes the information and sends emails to the patients, their guardians and even their primary doctors. That way, their families and primary doctors can

also check whether the patients are taking their medicine properly.

Dosage administration device | Vigilant, a Swiss company, developed Bee+ to manage the insulin injections of diabetes patients. When a patient injects insulin with an insulin dosing device on the market that is inserted in Bee+, information on the dosage is transmitted to the registered smartphones in real-time. If users enter additional information including their blood sugar information, they can efficiently manage their insulin-taking cycle with smartphone apps, which can greatly help doctors' treatment.

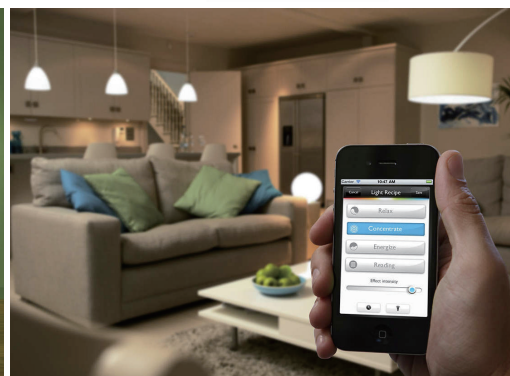
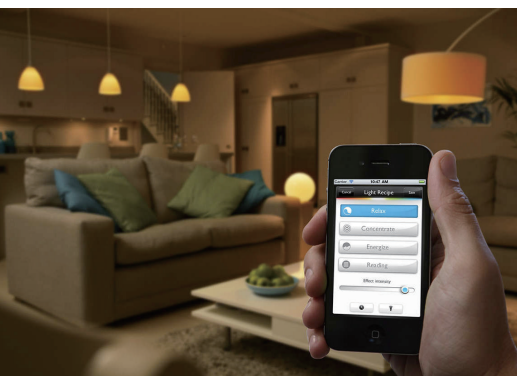


Bee+ developed by Swiss Vigilant effectively manages insulin-taking by transmitting diabetic patient's insulin-taking information to smartphones on real time.
© Vigilant

Homes getting smarter — smart home

Our homes are the main stage for IoT. Every part of our daily lives including sleeping, eating and relaxing are targets for IoT services. Smart home IoT technology analyzes and learns the life patterns of owners and sets the optimal lighting and temperature. It also efficiently manages energy consumption to prevent waste. Moreover, it recognizes the faces of pets and manages their weight so that they can stay healthy.

Smart lighting | Hue from Philips is a great example of LED smart lighting. Using their smartphones, users can adjust the color and brightness of lighting and even make it blink by adjusting the cycle. Smart lighting can also wake users up with a dim light in the morning and be used to turn on house lights before users arrive home. It can



With Hue, lighting developed by Philips, users can adjust the color and brightness of their lighting and also turn it on/off using smartphones.
© Philips



NEST's Thermostat is a smart temperature controller that adjust indoor temperature automatically by detecting human movement. © NEST

also be programmed to turn on and off regularly to prevent crimes when the home is empty for a long time.

Smart temperature controller | NEST's Thermostat, the representative product acquired by Google in 2014, works as a smart temperature controller. This may not seem special as temperature controllers are already attached to home boilers to operate and stop the boilers based on the preset temperature.

But, Thermostat is a smart temperature controller that learns by itself. When users first install it and set the indoor temperature they want in their daily lives, it starts to learn their patterns. Once it has learned their patterns, it sets the desired temperature on its own even if the users do not adjust the temperature every time. The more it learns, the more accurate it becomes in accommodating users' patterns. This is why it is considered a smart temperature controller.

Thermostat also detects human movement and lowers the temperature when users go out and raises the temperature according to when users set the time they will come back. As it is connected to the Internet, it can also maintain the indoor environment pleasantly by acquiring outdoor temperature and humidity information, and users can also adjust the indoor temperature from outside by using smartphones.

Preventing the leakage of personal information and invasions by thieves — security

Security is the area where IoT technology is expected to be most actively used. We may first think of information security when hearing the word security, but the physical security of preventing crimes and disasters when our homes or offices are empty is as important as information security.



TEO Lock is a lock that does not need a key. It can be open and closed with a smartphone. © form3

Smart Lock | TEO Lock is a lock that can be opened and closed with a smartphone. As one can au-

thorize another to open it only once or continuously, it is also possible to share lock access among families. Of course, it is also possible to manage the location, status and remaining battery capacity through a smartphone.

Smart video phone | Ring Video Doorbell is similar to the video phones generally installed at home entrances. When guests come and ring the doorbell, their faces appear on the screen. However, as most video phones are fixed to the wall, we need to go out to the living room to find out who is there. Also, we cannot see who comes while we are out. The best we can do is watch the recorded video when we get back home.

However, with Ring Video Doorbell, when the doorbell rings the image is transmitted to the connected smartphone. Of course, we can also talk to visitors when we are out and open the door for them.

Even at this moment, new IoT services are being developed based on fresh ideas in diverse areas. Which area is the most interesting to you? Write down what services are needed.



With Ring Video Doorbell, when a visitor rings the door bell, the image is transmitted to a smartphone and users can see who is there anytime, anywhere. © ring.com

Area	Name of IoT service	Description or image

Activity ③

Make a smart bulb

Let's make a smart bulb like Philips' Hue that we saw above. By attaching communication equipment to a common bulb and connecting it with a smartphone and Bluetooth, we can make diverse and convenient services. Let's experience how a common object can be changed through adding a network and software.

What to prepare Scientific calculator or computer connected to the Internet

Activity

1 Imagine how familiar objects we use can become smart.

Objects	Function

2 Find out about the smart bulb project algorithm

① Let's devise a smartphone app that can control smart bulbs from a users' perspective. First, design the screen of the smart bulb app.

② Devise an algorithm: Let's find out and write down how an LED bulb shows diverse colors.

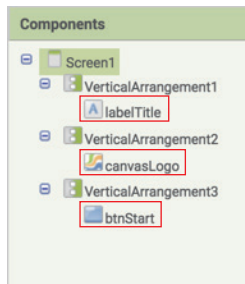
3 Programming

Make the 1st screen layout (Designer mode)

- ① This is the first screen of the smart bulb project. Make the title “Smart Bulb” and select and open the image bulb.png for the image in the center of the app. Add the text “Start” to the button.

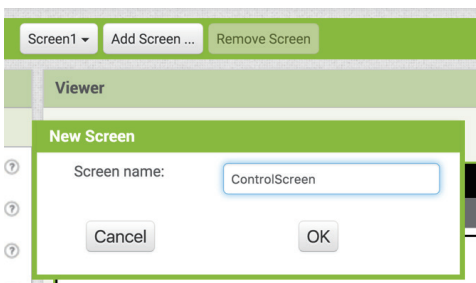


- ② Put three arrangement layouts in the main screen and add a label to insert the title, canvas to insert the bulb image and the Start button. Change the component names to “labelTitle”, “canvasLogo” and “btnStart”.



Reference) you can maintain a consistent layout regardless of the smartphone’s resolution if you set the height of arrangement layout in percentage.

- ③ Click <Add Screen...> to add a new screen named “ControlScreen”.

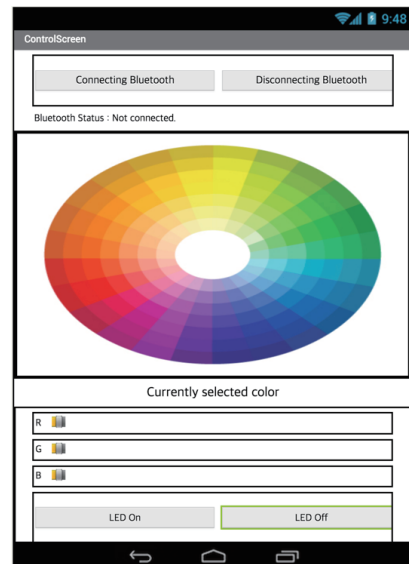


- ④ Ensure that a new window for “ControlScreen” opens when clicking the Start button after opening Blocks mode.



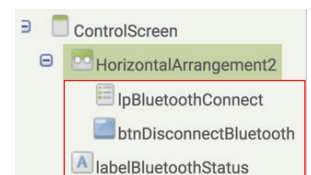
Make the 2nd screen layout (Designer mode)

- ⑤ This is the second screen that appears when touching the Start button.

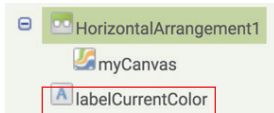


- ⑥ Design the part for Bluetooth connection on the top.

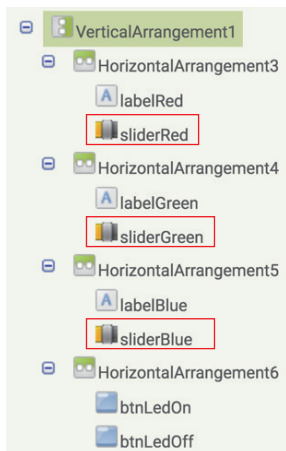
Add “ListPicker” and a button in the HorizontalArrangement layout and change the name to “IpBluetoothConnect” and “btnDisconnectBluetooth”, respectively. Put a label showing the Bluetooth status at the bottom and write the text that will appear first as in the following. Change the name to “labelBluetoothStatus”.



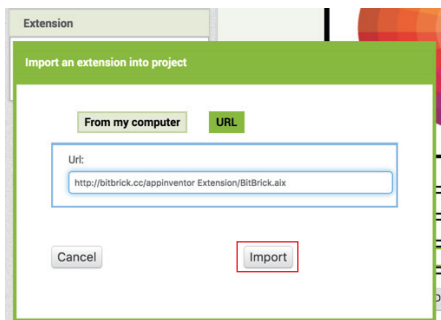
- ⑦ Use the canvas component to add color images. Apply colorwheel.jpg to this canvas. Add a label on the bottom so that the selected color can be seen immediately and change the name to “labelCurrentColor”.



- ⑧ Add Slider so that users can easily see the RGB value of the selected color. Set the max value at 255 and min value at 0, and clear the ThumbEnabled option so that users cannot change the RGB value by using Slider. Add 2 buttons so that the LED can be turned on/off at the bottom and change the names to “btnLedOn” and “btnLedOff”.



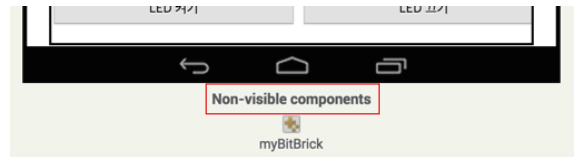
- ⑨ Import the BitBrick extension.
To easily use BitBrick in App Inventor, import the BitBrick extension. Select Extension from



the left palette, click URL and add the following address and click the Import button.

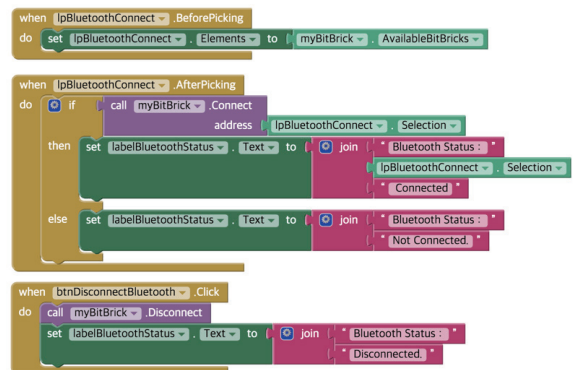
<http://bitbrick.cc/appinventorExtension/BitBrick.aix>

- ⑩ When the import is complete, the BitBrick component appears as above in the Non-visible components area. By using this, you can more easily control BitBrick in App Inventor.

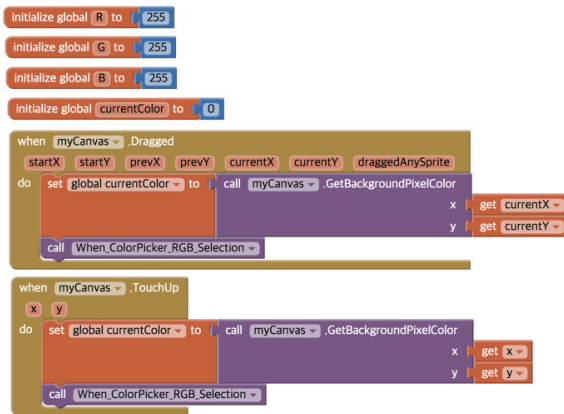


Adding screen codes in the 2nd screen (Blocks mode)

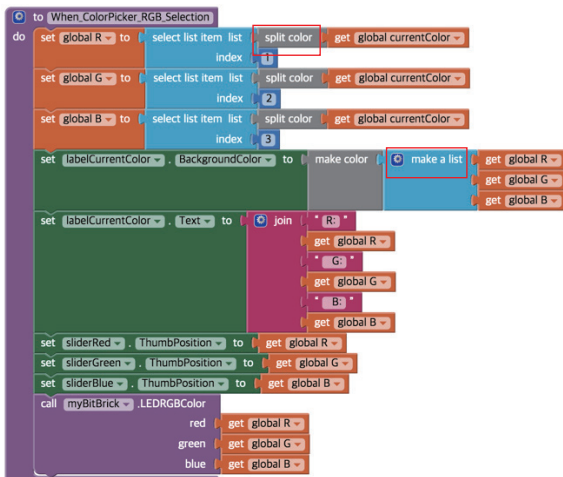
- ⑪ Use the following codes to connect BitBrick and smartphones through Bluetooth. Put the BitBrick list available for connection in the list before IpBluetoothConnect, which is shown when ListPicekr is clicked. When the user clicks IpBluetoothConnect, it connects with the Bluetooth of the selected BitBrick's Bluetooth, and if normally connected, make sure that the normal connection message appears on labelBluetoothStatus. When not connected well, make sure that the connection failed message appears. Make that the message that the connection with BitBrick has stopped and is disconnected is on the btnDisconnectBluetooth button.



- ⑫ Declare the current Color variable to save the background color of the color wheel. To convert the background color into RGB values, create R, G and B variables and put 255 as the initial value. The selected colors as such will change the LED of BitBrick through the function WhenColorPickerRGBSelection that will be defined below.



- ⑬ Create the function WhenColorPickerRGBSelection. As this is the part that repeats the same task when the user drags or touches the canvas, the user does not need to do the same task many times if this function is made. First, divide the colors in the currentColor variable in each of R, G and B variables in to R, G, B and Alpha values through the split color function. Then, put this into the corresponding variable using the list function.



Make sure that users can easily check the color they selected by changing the background color of labelCurrentColor to the selected color. Moreover, make sure that the accurate values of R, G and B are visible. Once the values of R, G and B are decided, move the Slider position based on the respective value and put it in the RGB value of BitBrick LED's RGB.

- ⑭ Add the block to turn the LED on/off by using the button. Put the current R, G and B values as the red, green and blue value in BitBrick for the LED On button so that it is turned on. For the LED Off button, use the LEDOff command block provided by BitBrick to turn it off.



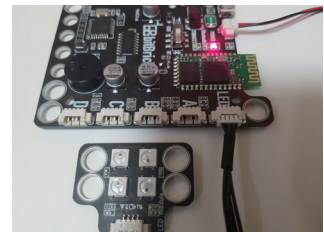
Reference

1. App installation

- ① In the settings of the Android mobile phone allow the installation of "app from unknown sources".
- ② Download the installation files. (Refer to Class Instruction Guidelines for the location of the installation files.)

2. Connect with BitBrick

Connect the LED module to the LED output jack after connecting the battery power outlet to BitBrick. Push the BitBrick connection setting switch to the far right to select Bluetooth.





IoT developer

Today is the era of objects, instead of humans, using the Internet. The idea of IoT is nothing new, but it is becoming further realized with the development of super high-speed communications networks, the availability of smart electronic products, sensors, Big Data and the development of security technology, etc. When IoT becomes universal, electronic devices will operate based on users' life patterns without needing commands. In the near future, it is expected that occupations related to the base technologies of IoT and that make diverse services based on IoT will increase.

What do they do?

- Make sensors, artificial brains and communication functions where IoT is possible and design and manufacture electronic products with such functions
- Make equipment for building super high-speed internet communications networks and manage the communications networks
- Plan and create services that are useful in our daily lives and industries, including smart home, disaster preparation and energy saving by using IoT

Occupations related to artificial intelligence

Electronic payment	Security experts, NFC program developer, computer system design analyst
Communications equipment	Communications engineer, communications device engineer, communications equipment engineer, communications technology developer, communications network operation engineer
IoT service	IoT service planner, IoT product planner, service developer, smart home designer, electronic product planner

Related majors

Diverse technology areas are needed to realize IoT including sensors, processors, super high-speed communications, Big Data and security, etc. As smart services can-

Computer
engineering

electric
engineering

electronic
engineering

architecture
studies

urban studies

not be realized with only one or two devices available for IoT, it seems that it will take some time to establish a robust foundation across many areas. However, after this foundation is prepared, a wide range of services will be provided. In the age of IoT, architecture departments and urban studies departments that teach building design or urban facility planning will also teach IoT.

Required aptitude

- A basic understanding of communications networks is required. One should be well aware of the background and methods of using super high-speed communications network to develop IoT services.
- The ability to observe surrounding objects and situations and find the required elements will be helpful in planning and realizing services utilizing IoT.
- The attitude to acquire and explore knowledge is required as this is an area where new technology develops rapidly.
- As there are many cases where one needs to work in cooperation with other engineers or experts, good interpersonal skills and clear communication ability are required.

Expert interview

My division makes equipment needed for networks like LTE. I get excited to work when I see the people around me conveniently using the products developed here. It means that I am contributing to the development of communications technology, and one step further, to the advancement of society. I feel proud when I see people's lives becoming more enriched and fun.



Yeon-jeong Lim / Graduated from Information and Communications (currently Electric Engineering) Department, Ewha Womans University, Development Fellow, Network Division, Samsung Electronics



Make an IoT parking system



Written by
Min-chul Shin (Singil Middle School teacher)



Product overview

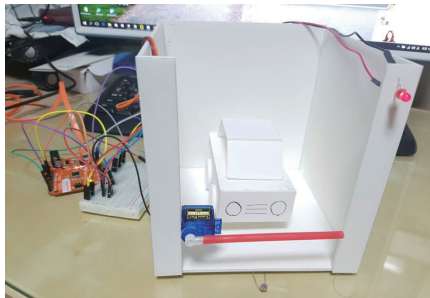
■ Product function

A simple garage model and an IoT parking system using S4A and Arduino programming

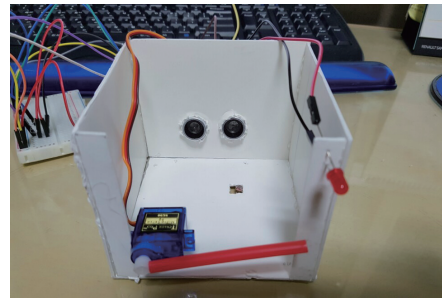
■ How it works

Arduino programming using IoT (controlling actuator by using sensor value)

■ Product picture

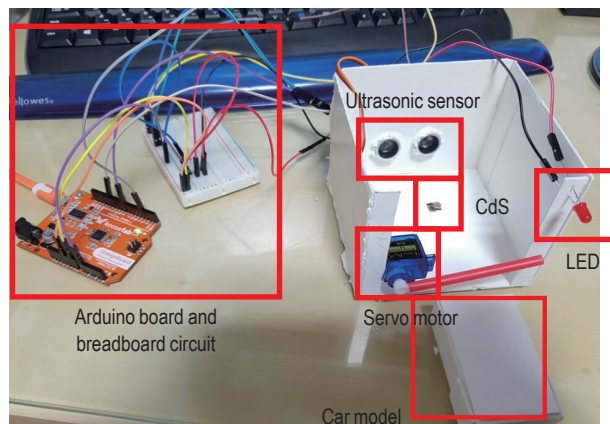


Garage system that automatically opens when a car arrives



Lighting that automatically turns on when a car arrives

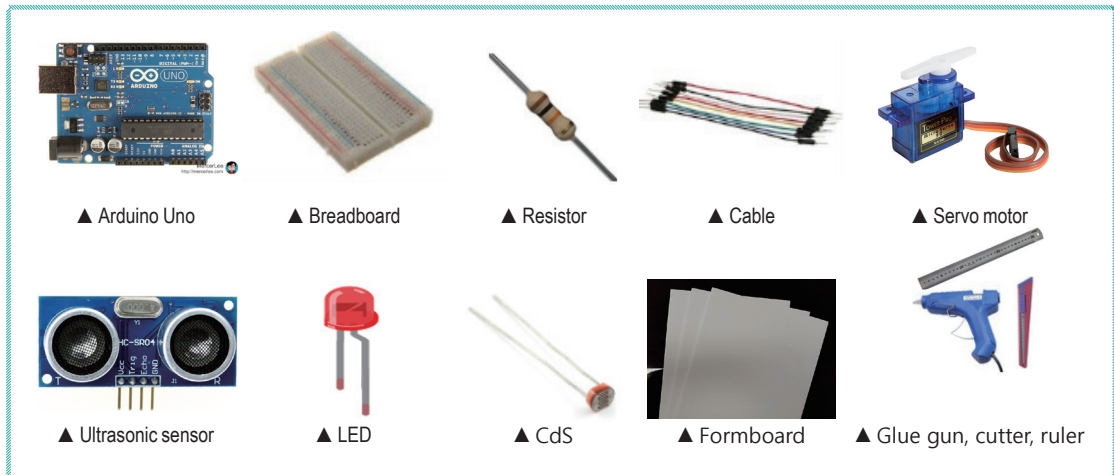
■ Product structure





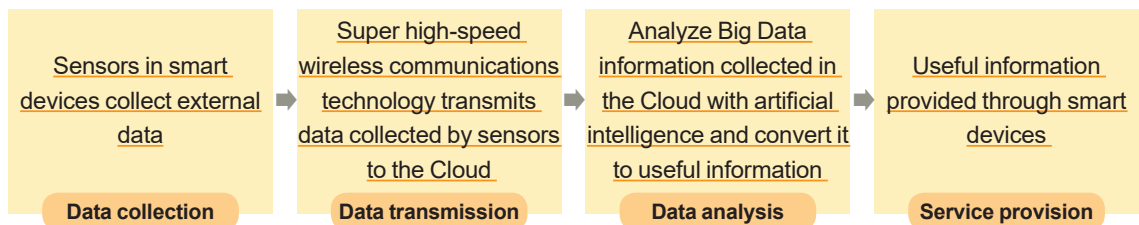
Production overview

- **Production time** : around 10 hours
- **Needed materials and tools**



■ Key production principles

How IoT works



■ What requires attention in production

- 1 Learn simple ways of using Arduino and S4A.
- 2 Make a garage model to express only a simple structure.
- 3 Be careful of safety accidents while using the cutter.

■ Required knowledge and functions

- 1 How to link Arduino and S4A
- 2 How to connect diverse sensors and the actuator with Arduino
- 3 How IoT is implemented

SW Education Module Textbook

❶ Artificial Intelligence

❷ Driverless Vehicles

❸ IoT(Internet of Things)

❹ Virtual Reality

❺ CRISPR

❻ Space Launch Vehicles

❼ Natural Disasters

❽ Smart Medicine

❾ Game Engines

❿ Sports Statistics

SW Education Module Textbook ❸ IoT

Our Life Changed by IoT

Issued on February 23, 2017

Issued by Ministry of Science and ICT, Korea Foundation for the Advancement of Science and Creativity

Written by Jin-tae Lee

Planned by Ji-young Park, Jong-geol Son, Hye-ja Kim (MSIP)
Yun-jeong Kim, Se-man Park, Ok-su Hong, Jae-min Han, Hye-ran Go (KOFAC)

Edited by Tae-won Seo, Byeong-rae Han

Reviewed by Seong-hoon Kim

Published by Doo-hui Kim

Publisher Dongascience Inc.

Responsible editor Kyeong-ae Chang

Inquiries Software Education Center, Korea Foundation for the Advancement of Science and Creativity

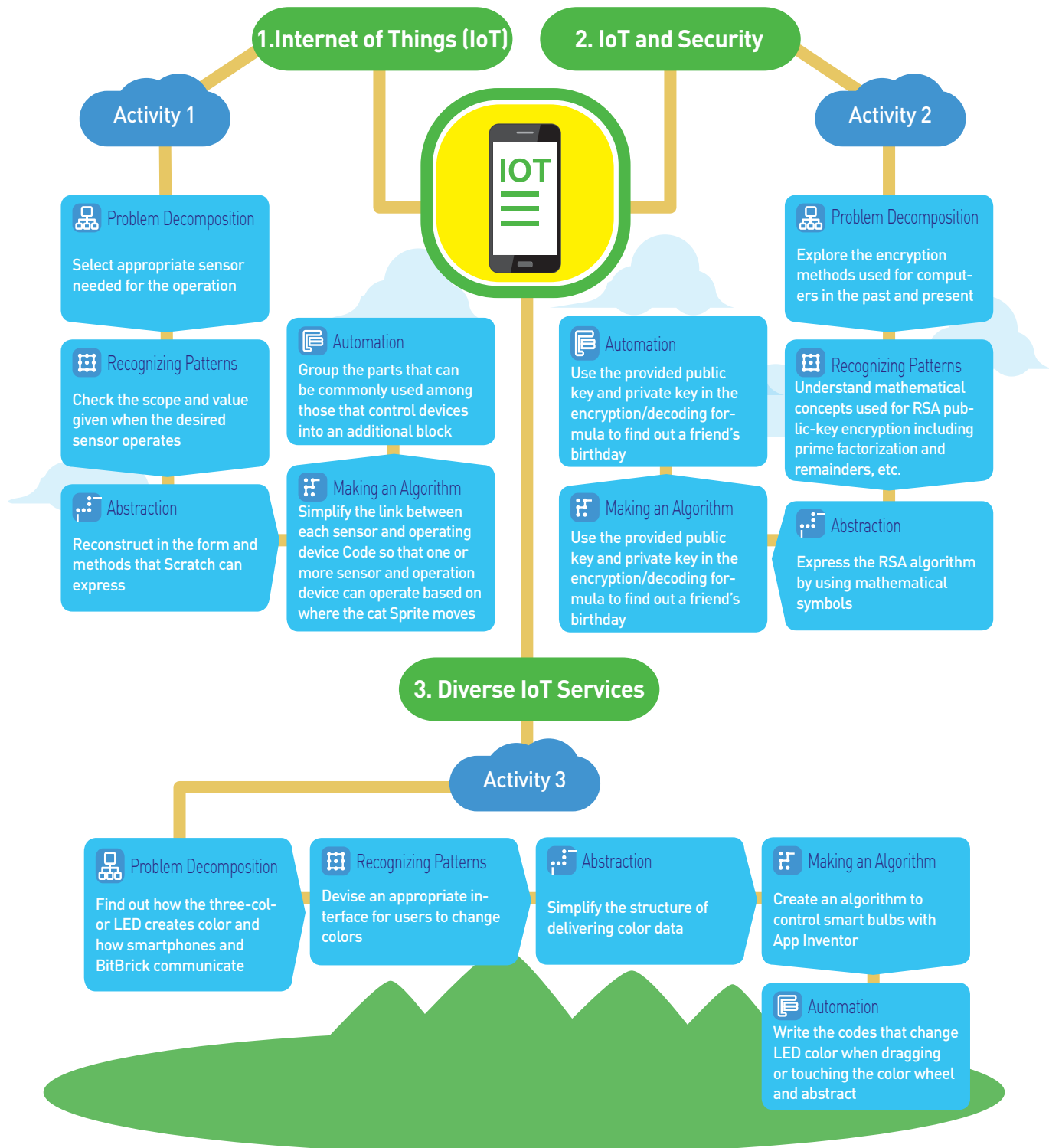
Email swedu@kofac.re.kr

Phone (02)559-3841~9

Address (135-867) 602 Seolleung-ro, Gangnam-gu, Seoul (Samreung Building, Samseong-dong)

Homepage www.kofac.re.kr

Computational Thinking Map



software

education module



Ministry of Science and ICT



KOFAC
Korea Foundation for
the Advancement of Science & Creativity
한국과학창의재단