Unit 8: In the Clouds

Cloud Computing, Security & Encryption

Learning Objectives

- 1: The student can use computing tools and techniques to create artifacts.
- 4: The student can use programming as a creative tool.
- 5: The student can describe the combination of abstractions used to represent data.
- 9: The student can use models and simulations to raise and answer questions

Readings/Lectures

- Reading 8.01: What is Cloud Computing? (/bjc-course/curriculum/08-cloud-computing/readings/01-what-is-cloud-computing)
- Worksheet 8.02: Hand Biometrics (/bjc-course/curriculum/08-cloud-computing/readings/02-hand-biometrics-worksheet)

External Resources

- The History of Encryption (http://visual.ly/history-encryption)
- The Enigma War, 1939-1942 (http://www.turing.org.uk/scrapbook/ww2.html)
- Who was Alan Turing? (http://www.cs4fn.org/magazine/magazine14.php)
- Locking a Dead Man’s Chest (http://www.cs4fn.org/binary/lock/)
- How to control a computer with a banana (http://www.cnn.com/2013/04/05/tech/innovation/jay-silver-makey/index.html)

Labs/Exercises

- Lab 8.01: Encryption and Decryption (/bjc-course/curriculum/08-cloud-computing/labs/01-encryption-decryption)
- Project 8.02: Encryption Project (/bjc-course/curriculum/08-cloud-computing/labs/02-encryption-project)

What is Cloud Computing?

Much of our work this semester will be supported by software that is provided as a *service* rather than as a *product*. This is example of cloud computing (http://en.wikipedia.org/wiki/Cloud_computing).

For example, the software you used to create your portfolio is an example of cloud computing. Setting up the portfolio used software that was provided as a free service by Google. Your portfolio lives on the cloud, as the Internet is popularly called. Basically, you don't know exactly where your portfolio page is stored, as you would if it were a product (like Microsoft Word) on your laptop.

Cloud Computing Paper

Look up up cloud computing on Wikipedia (http://en.wikipedia.org/wiki/Cloud_computing) and read enough of that article to get a sense of cloud computing and to be able the questions below.

In your summary answer the following questions about cloud computing:

- Cloud computing can involve various services, including computation, data storage, and data access. Which of these services are provided in the case of your portfolio? Explain.
- What are one or two of the main benefits of cloud computing?
- What are one or two of the possible drawbacks of cloud computing?

Material from Dr. Ralph Morelli, Trinity College

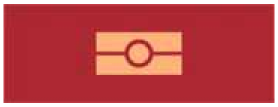
Hand Biometrics Technology

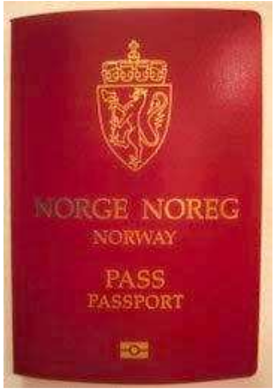
Student Worksheet:

Biometrics (ancient Greek: bios ="life", metron ="measure") is the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In information technology, "biometric authentication" refers to technologies that measure and analyze human physical and behavioral characteristics for authentication purposes. Examples of physical (or physiological or biometric) characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while examples of mostly behavioral characteristics include signature, gait and typing patterns.

Sample Applications

1. Since the beginning of the 20th century, Brazilian citizens have used ID cards that incorporate fingerprint-based biometrics.
2. Microsoft has introduced a fingerprint reader that prevents computers from being used by unauthorized people.
3. Some countries have implemented biometric passports that combine paper and electronic identity -- using biometrics to authenticate the citizenship of travelers. The passport's critical information is stored on a tiny RFID computer chip. The icon is incorporated onto most biometric passports to indicate the technology.





Hand Geometry Biometrics

Hand geometry is a biometric that identifies users by the shape of their hands. Hand geometry readers measure a user's hand along many dimensions and compare those measurements to measurements stored in a file.

Viable hand geometry devices have been manufactured since the early 1980s, making hand geometry the first biometric to find widespread computerized use. It remains popular; common applications include access control and time-and attendance operations.

Since hand geometry is not thought to be as unique as fingerprints or retinas, fingerprinting and retina scanning remain the preferred technology for high-security applications. Hand geometry is very reliable when combined with other forms of identification, such as identification cards or personal identification numbers. In large populations, hand geometry is not suitable for so-called one-to-many applications, in which a user is identified from his biometric without any other identification.

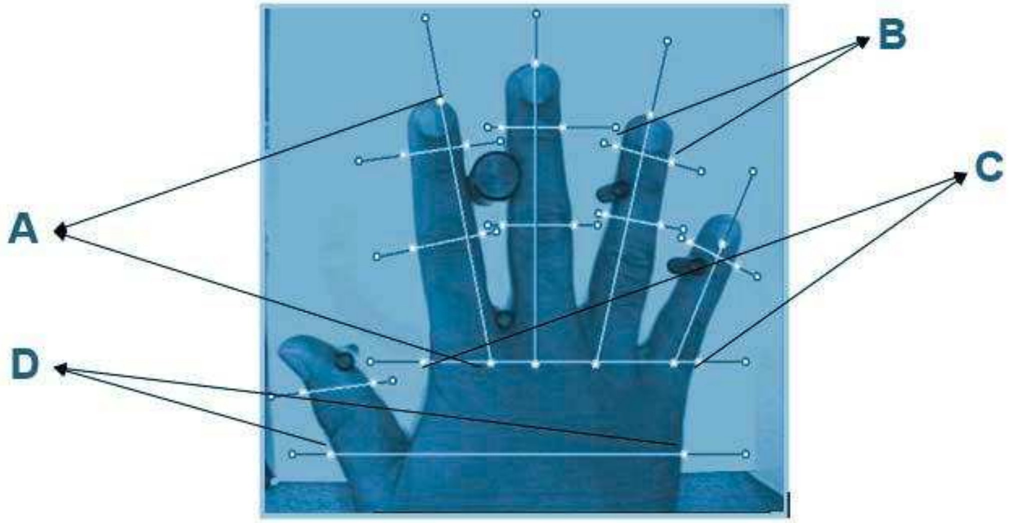
Hand Biometrics Technology

Student Worksheet:

Biometric templates contain information extracted from biometric traits. The resulting codes can be used for identification in a variety of situations. In this activity, you'll determine your own personal hand geometry code.

Step One:

1. Trace your right hand on a piece of paper, keeping the pencil as close to your skin as possible.
2. Using a ruler, measure the following in centimeters (see diagram below):
    a. Distance from index fingertip to bottom knuckle ________cm
    b. Width of ring finger, measured across the top knuckle _______cm
    c. Width of palm across 4 bottom knuckles ________cm
    d. Width of palm from middle knuckle of thumb across hand _______cm



3. Record the 4 numbers in A, B, C, D order, which is your personal hand geometry code:
    ____ _____ _____ _____

Step Two:

Have someone else in your class trace your right hand, and repeat the measurements above. Record the 4 numbers in A, B, C, D order…are there any differences?

____ _____ _____ _____

(Note: Biometric information on this page is provided by and used with the permission of The National Biometric Security Project (NBSP). Duplication is permitted for educational purposes only.)

Hand Biometrics Technology

Student Worksheet:

You are a team of computer engineers meeting to determine whether personal hand geometry templates or numbers would be unique enough to serve as an element in a new security system for a museum.

Evaluation Phase

As a team (if working with a partner), examine the geometry templates you have received. These will represent the codes of staff that need to access the museum during evening hours to check on the security of a group of priceless paintings. Discuss and answer the following questions to help form your plan for incorporating biometrics into the museum's new security system.

1. How similar were the geometry template codes you examined? What did you observe that was most similar? What did your team determine to be different in the group?

2. What problems do you envision an employee might encounter as they placed their hand in the biometric scanning device?

3. Are there any guidelines your engineering team would recommend regarding either capturing the codes from each employee, or in scanning the employee's hand at the entrance to the museum?

4. Do you think that fingerprint scans would be more effective? Why? Why Not?

Hand Biometrics Technology

Student Worksheet:

Biometrics can be applied to many situations, such as computer login security, employee recognition, time or attendance record systems, and voter identification. As a team of "engineers" describe three other situations where you think engineers should consider incorporating biometrics technology to solve problems.

Please indicate whether any of these situations might warrant at two-level system, where hand biometrics is one of the two levels of verification:

1.

2.

3.

At Walt Disney World, biometric measurements are taken from the fingers of guests to ensure that the person's ticket is used by the same person from day to day. Do you have privacy concerns about this? Why? Why not? If you were part of the engineering team on this project, what would you do to ensure privacy?

The Alan Turing Internet Scrapbook

Scrapbook Index

Critical Cryptanalysis:
The Enigma War, 1939-1942

Alan Turing Home Page | Site Map | Scrapbook Index | Previous Scrapbook page | Next Scrapbook page

Alan Turing at War

The Crown Inn, where Alan Turing lodged
(my photo, 1979)

After Britain declared war on Germany on 3 September 1939, British codebreaking operations were moved from London to **Bletchley Park.** This country house was near the then small railway town of Bletchley, half-way between Oxford and Cambridge.

See this modern map for the site, close to Bletchley railway station.

Between 4 September 1939 and the summer of 1944, Alan Turing lodged at The Crown Inn, at Shenley Brook End, a village to the west of Bletchley.

The Shenley area (see this map) is now completely changed.

War did not stop Alan Turing being an individualist. In 1940 he buried some silver bars near Shenley. In 1944, 1946 and 1952 he tried to find them and failed. No-one knows what happened to his buried treasure!

Bletchley Park today

Bletchley Park Mansion

Bletchley Park can still be seen today because the wartime site was left largely unchanged after 1945.

In 1991, the site was saved from property development, and amazing work of reconstruction was done by the original curator, Tony Sale, and his collaborators.

Now the house and grounds are managed by the Bletchley Park Trust.

The late Tony Sale created a complementary website, www.codesandciphers.org.uk, which still gives extensive technical explanation and copies of original documents.

It also gives a Virtual Tour of Bletchley Park with many photographs.

See also the National Museum of Computing.

The Bletchley Park Trust website gives full details of how to visit the museum and the various events held there. It has a history section.

The nerve centre

The huts: my photo, August 1998.

Everything to do with intelligence was dominated by the technicalities of the **Enigma cipher machine,** the key to German communications.

Alan Turing's wartime life was spent mainly in the Huts erected in the grounds of Bletchley Park, where the technical work of codebreaking was done.

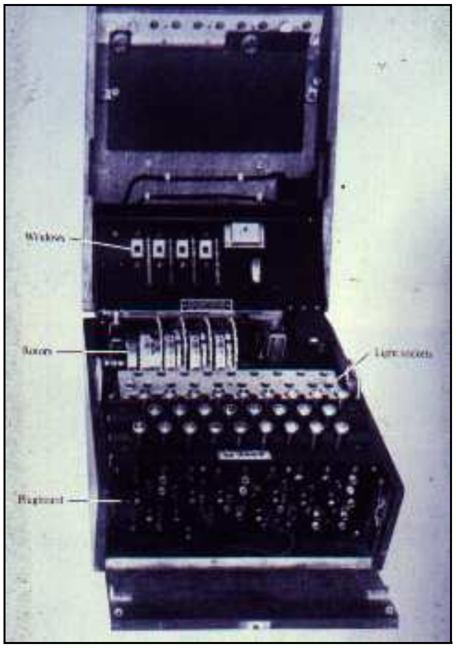
Hut Eight, where Alan Turing worked on the naval Enigma, is in the centre of the picture. To the left is Hut Six (Army and Air Force signals). To the right is Hut One. This is where, in 1940, the first Bombe, Turing's codebreaking machine, was installed.

The Enigma

Most German communications were enciphered on the Enigma cipher machine. It was based on rotors whose movement produced ever-changing alphabetic substitutions.

In its military use, the basic machine was greatly enhanced by a **plugboard**, visible on the front of the machine.

The ciphers it produced were supposed to be unbreakable even by someone in possession of the machine. Ideas of great logical ingenuity were needed to defeat it.



If you want to see an Enigma in real life, this page by David Hamer tells you some locations. If you are Bill Gates, you may like to buy one.

Cheaper: a modern replica.

Even cheaper: this on-line simulator by Dirk Rijmenants, with elegant and realistic graphical layout and a challenge.

The Enigma has become an icon and a cult object in its own way. This is explored in a book by Dominik Landwehr (in German):

Mythos Enigma.

Who broke the Enigma?

In fact, the Enigma had to be broken afresh *over and over again.* The hardware in the picture is not the whole story, and capturing it did not allow Enigma messages to be read. The German use of the Enigma depended on systems for setting the *keys* for each message transmitted, and it was these *key-systems* that had to be broken. There were many such systems, often changing, and the hardware was changed as well from time to time. The brilliant pre-war work by Polish mathematicians enabled them to read Enigma messages on the simplest key-systems. The information they gave to Britain and France in 1939 may have been crucial, but it was not sufficient for the continuation and extension of Enigma breaking over the next six years. New ideas were essential.

In 1939-40 Alan Turing and another Cambridge mathematician, Gordon Welchman, designed a new machine, the British **Bombe.** The basic property of the Bombe was that it could break any Enigma-enciphered message, provided that the hardware of the Enigma was known and that a plain-text 'crib' of about 20 letters could be guessed accurately.

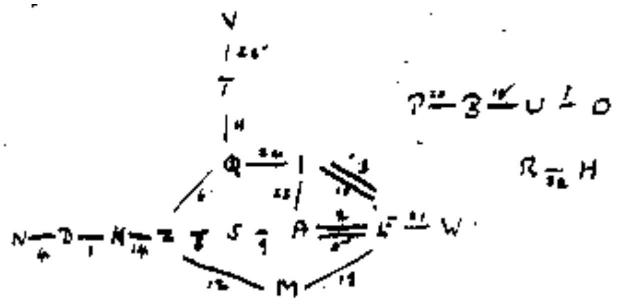
See the Enigma report of November 1939, announcing the British 'superbombe' in production

Alan Turing's mission to France, January 1940, for conference with the Polish analysts

The cottage in the stable yard of Bletchley Park, where Alan Turing worked in 1939-40.
(My photo, July 2002).

Alan Turing made a brilliant contribution to the design with an idea that he himself related to the principle in mathematical logic that 'a false proposition implies any proposition.' It was this idea that overcame the apparently insuperable complication of the plugboard attachment. But that idea was just the beginning of a continuous struggle.

The work done by Turing and his colleagues at Bletchley Park brought cryptology into the modern world. It required ingenious logic, statistical theory, the beginnings of information theory, advanced technology, and superb organisation.



See Alan Turing's own sketch of the logical principle of his Bombe.

Alan Turing's Bombe

The fullest source of on-line information on the use of the Enigma and the Bombe is on Tony Sale's site.

This gives a full technical description and explanation of the Enigma machine and its use.

It also offers a 'Virtual Bletchley Park' area with a page detailing his explanation of how Turing arrived at the idea of the Bombe, and another about the Polish breaking of the Enigma which preceded it.

It includes an on-line simulator of the Bombe, and much more historical information.

A 1944 American report gives a very clear explanation of how the Bombe was used to break Enigma messages.

Another clear explanation of the principle of the Bombe is given by Graham Ellsbury of Microvector on his Enigma pages.

The Bombes were built by British Tabulating Machinery at their factory in Letchworth, Hertfordshire.

John Harper describes the work of rebuilding a copy of Turing's Bombe, with much further information about the engineering involved.

News story on the running of the rebuilt Bombe, 6 September 2006.

Rotors on the mock-up Bombe, June 2001

Totally secret for thirty years

Everything about the breaking of the Enigma cipher systems remained secret until the mid-1970s. Partial accounts then emerged constrained by continuing secrecy about technical matters. Gordon Welchman gave the central principle of the Bombe in describing his own contribution in *The Hut Six Story,* 1983.

In the mid-1990s virtually everything was released from secrecy and now it is possible for scholars to investigate this fascinating history in considerable detail.

Notable books are:

- *Codebreakers,* eds. F. H. Hinsley and A. Stripp.
- Ralph Erskine and Michael Smith (eds.) *Action This Day*
- Stephen Budiansky *Battle of Wits: The Complete Story of Codebreaking in World War II*
- F. L. Bauer, *Decrypted Secrets,* gives a full account of the

Hut 6, Bletchley Park, where the German Air Force signals
were broken with the help of Turing's Bombes.
(My photo, 1998)

Enigma as part of a serious
work on modern cryptology.

Simon Singh's popular work *The Code Book* claims to explain 'how Turing broke the Enigma.' Unfortunately it makes the Enigma problem look much easier than it actually was, and so undervalues Turing's contribution.

Mark Baldwin offers illustrated talks and an extensive specialist book service.

Station X

The television programme series *Station X* about Bletchley Park, made for Channel Four television in the UK, was first transmitted in early 1999. The video can be bought on-line from the Bletchley Park Shop. For the United States it was reduced to a two-hour programme shown on Nova as *Decoding Nazi Secrets.* It is evocative and valuable as a archive of interviews but weak in showing that the secret of success at Bletchley Park was the application of scientific method. Michael Smith's book, *Station X,* accompanied the TV series.

Other sites on World War II cryptography

Frode Weierud's CryptoCellar.
Geoff Sullivan's CryptoMuseum

Alan Turing and the Battle of the Atlantic

The Bombe was used with success from the summer of 1940 onwards, to break messages enciphered on the simpler Enigma system used by the German Air Force. But the most important messages were those to and from the **U-boat fleet,** and these were enciphered on a much more secure Enigma system.

Alan Turing took on this problem, going against the prevailing view that it would prove unbreakable. Although he had crucial new ideas at the end of 1939, not much practical progress could be made. In 1940 they were desperate.

See the October 1940 Operation Ruthless plan devised by Ian Fleming, later the creator of 'James Bond', to capture such information for Turing's work.

The breakthrough came in February 1941, with the capture of papers from the *Krebs* off Norway.

From then on, with the help of some further captures, the U-boat communications were effectively mastered. Alan Turing continued to head the cryptanalysis of all German Naval signals in Hut Eight.

The naval Enigma was more complicated than those of the other German services, using a stock of eight rather than five rotors. For the Bombe to work in a practical time it was necessary to find ways of cutting down the number of possibilities. Alan Turing developed 'Banburismus,' a statistical and logical technique of great elegance, to find the identity of the rotors of the enciphering Enigma before using the Bombe. Turing made major developments in Bayesian statistical theory for this work, with his assistant (I. J.) Jack Good.

See this news article about recent work extending Turing's theory, with more technical web-page and downloadable pdf on 'Almost Good Turing.'

See Steve Hosgood's page on 'Banburismus' for a detailed description of the whole process.

Tony Sale's site also has a sequence of pages on Naval Enigma explaining in considerable detail what Alan Turing did and how Banburismus worked.

Books concentrating on the naval Enigma capture operations:

- Hugh Sebag-Montefiore, *Enigma: the battle for the code.* There is a summary of his story on this naval history page
- David Kahn, *Seizing the Enigma*

On 1 February 1942, the U-boats changed to an even more complicated Enigma system, involving a fourth rotor. Their communications became unbreakable until December 1942, when a brilliant trick allowed codebreaking to be restored.

Fact and Fiction

An American film, **U-571,** drew on the story of the material captured in 1941 but fictionalised it as an American achievement. You can see US Navy comment on this fictionalisation here.

Robert Harris's thriller novel *Enigma* has been adapted as a film *Enigma* with a screenplay by Tom Stoppard. It depicts the naval Enigma problem in the 1943 period. However the story is fiction, and the film does not show the actual Bletchley Park location. The film also endows the fictional lead character with allusions suggesting he is 'really' Turing himself. See my review of the film.

However, more care was taken in representing the technical background. You can see in Tony Sale's detailed pages how he scrupulously devised suitable messages and Enigma methods for this film.

The end of the beginning

At the end of 1942, Alan Turing's war experience had changed him in many ways. It gave him experience of **digital electronics.** It made him fascinated by the idea of **'intelligent machinery'.**

But first, it made him a top level liaison between **the United Kingdom and the United States.**

Continue to the next Scrapbook page.

All these developments were to come together in the post-war world of the computer, with Alan Turing at its centre. But no-one knew it was...

The beginning of the end

CONTINUE: Next Page | Previous Page | Scrapbook Index

Quick Links: Book | Short Bio | Scrapbook | Publications | Sources

Alan Turing Home Page | Search | Andrew Hodges

Curriculum (/bjc-course/curriculum) / Unit 8 (/bjc-course/curriculum/08-cloud-computing) /
Lab 1 (/bjc-course/curriculum/08-cloud-computing/labs/01-encryption-decryption) /

Encryption and Decryption

Learning Objective 27: The student can connect the concern of cybersecurity with the Internet and systems built on it.

- 27a. Identification of tradeoffs associated with the trust model of the Internet.
- 27b. Description of software, hardware, and human components involved in implementing cybersecurity.
- 27c. Explanation of how cryptography is essential to many models of cybersecurity.

Symmetric Key Cryptography

Cryptography means secret writing. **Cryptanalysis** is the study of how to break a secret message, sometimes called a **cryptogram**.

A **cipher** is system for **encrypting** and **decrypting** messages. A cipher's strength – i.e., how secure it is, how well it protects a secret message – depends on the strength and security of its key.

A *symmetric* key cipher is one in which the sender and receiver of the message share the same secret key.

Simple Substitution Cipher

A **simple substitution cipher** is a cipher that is based on a **permutation** of the alphabet. For example,

Plaintext alphabet: abcdefghijklmnopqrstuvwxyz

Cipher alphabet : **ZEBRASROCK**DFGHIJLMNPQTUVWX

There are 26! (= $4.03291461 \times 10^{26}$) ways to permute a 26-letter alphabet – i.e, 26 ways to pick the first letter times 25 ways to pick the second times 24 ways to pick the third, and so on.

In this example, the *symmetric key* is the permuted cipher alphabet. Note how we can use the *keyphrase*, "zebras rock" to construct the alphabet. This makes it easier for two parties to share a secret key.

If Alice wants to send the secret message "attack at noon" to Bob, her fellow agent, should would use the cipher alphabet to encrypt the message, replacing a with Z, t with P, and so on:

Plaintext alphabet: abcdefghijklmnopqrstuvwxyz

Cipher alphabet : ZEBRASROCKDFGHIJLMNPQTUVWX

```
                  attack at noon


                  ZPPZBD ZP HIIH
```

Upon receipt of the message, Bob would use the cipher alphabet in reverse to decrypt the message, replace Z with a, P with t, and so on:

Plaintext alphabet: abcdefghijklmnopqrstuvwxyz

Cipher alphabet : ZEBRASROCKDFGHIJLMNPQTUVWX

```
                ZPPZBD ZP HIIH

                attack at noon
```

Breaking a Cipher

Suppose Eve intercepts Alice’s message. Eve doesn’t know the key. Can she break the secret message?

Question: Would it be practical to try every one of the 26! alphabets? No, that would be **intractable**.

If Alice and Bob only sent short messages and changed their key after every message – i.e., **one-time pad** – then Eve will not be able to crack the messages.

But, if they use the key to send message of 40 or more characters, then Eve may be able to break it using **pattern analysis** and **frequency analysis**. How many English words have the pattern 1221 (noon, kook, deed, …)? If the letter “t” is the second most frequent letter in English, then its substitute, “P”, will be the second most frequent letter in the secret message.

Modern Symmetric Cipher

The Advanced Encryption Standard (AES) (http://en.wikipedia.org/wiki/Advanced_Encryption_Standard) is a modern secure electronic cipher used by businesses and the federal government.

AES is an open standard that went through a 5 year public analysis period. AES turns documents into strings of bits and then scrambles and permutes the bits in such a way that it removes all statistical patterns.

What makes AES secure is its large key size, ranging from 128, 192, or 256 bits, which make it **intractable** to use a brute-force search to find the key.

The Key Exchange Problem

How can Alice and Bob share their shared key? It’s difficult to image the modern day Internet if the **key exchange problem** had not been solved.

Public Key Cryptography

In **public key cryptography** the key exchange problem goes away because there is no secret key to be shared.

It is based on a **trap door function** or a **one way function –** i.e., a function that is easy to compute in one direction but hard (intractable) to compute in the other.

For example, its easy to multiply 2180 × 7208 = 15,713,440. But it would be relatively difficult to factor 15,713,440 into 2180 and 7208.

Simple Public Key Example

Here’s a simple example (http://www.di-mgt.com.au/rsa_alg.html#simpleexample) of the Rivest Shamir Adelman (RSA) public key algorithm. It illustrates that we can send a secret message without having to share a secret key.

- Pick two big (100 digit) prime numbers, p = 11, q = 3
- Let n = p × q = 11 × 3 = 33
- Let phi = (p - 1) × (q - 1) = 20

- Choose e=3 to be relatively prime to (p - 1) and (q - 1) – i.e., gcd(10,3) = 1 and gcd(2,3) = 1.
- Find d=7 such that phi (20) divides (3 × d) - 1 – i.e., 20 = (3 × 7) - 1
- We end up with 3 numbers, n, e, and d that can be used to form Alice's public and private keys:

  Alice's **public key**: (n, e) = (33, 3) Alice publishes this key.

Alice's **private key**: (n, d) = (33, 7) Alice keeps this key secret.

Let's suppose Bob wants to send the message "15" to Alice.

Bob encrypts the message using Alice's public key: 153 mod 33 = 3375 mod 33 = 9

Alice receives the secret message, "9".

Alice decrypts the message using her private key: 97 mod 33 = 4782969 mod 33 = 15

Alice reads Bob's message, "15".

What makes RSA secure is that it's easy to compute c = m^e mod n, but it's very difficult to compute its inverse – i.e., m = c^{-e} mod n.

Secure Transactions Across the Internet

In **secure client-server** transactions, RSA is used by the client (Alice) and server (Bob) to exchange a **secret symmetric key**.

Note the role that the **certificate** plays in authenticating the identity of the server.

Questions

- Would it be possible to have today's Internet – Amazon, online banking, etc. – without public key cryptography?
- Can you solve this simple substitution cryptogram?

Qbono kjdo vrp r lcqdbon rq Qncjcqy,

Vbkpo xrpqerhh vrp dhkdgos rq cjxcjcqy.

Kj sryp bo vkths lcqdb,

Qbo erqqonp vkths scqdb,

Pk bcqp vono rj cilkppcechcqy.

- Hint: Look at the first words in lines 1 and 3.
- Hint: That first word has a familiar pattern.
- Hint: The last word in the first line has a familiar pattern.
- Here's an online cryptogram tool (http://www.cs.trincoll.edu/~ram/cryptogrammer/) to help you solve it. Paste the cryptogram into the tool and then try substituting letters in the alphabet until you get it.

Curriculum (/bjc-course/curriculum) / Unit 8 (/bjc-course/curriculum/08-cloud-computing) /
Lab 2 (/bjc-course/curriculum/08-cloud-computing/labs/02-encryption-project) /

Encryption Project

Using the links provided and your own research on encryption methods used today, create a product about encryption past, present and/or future. You can focus on any aspect of encryption that interests you.

You should have at least 4 sources with one of those not given by me. Make sure to include a Works Cited page to submit with your product.

Work with your table partner to create a product of your choice. The product can be any of the following.

- Wiki/Blog/Web Page
- PowerPoint or Prezi presentation
- Short “Film”
- Voki
- Other by Student/Teacher discussion

TURN IN

- Create a new portfolio page called Encryption.
- Add a description of what you chose to do your project on.
- Upload your product
- Add your Works Cited as a link

SUBMIT IN MOODLE

- Screenshot of your Portfolio Page
- Works Cited document
- Your product (or link if it is on the Internet)