## [3413ICT Network Security](file:///C:\\Documents%20and%20Settings\\s995689\\My%20Documents\\Teaching\\Courses_2013\\Courses_2003\\6216INT_03\\6216inthome.html)

### **Workshop:3A**

**Part 1 – Reviewing the lectures 2A and 2B, answer the following questions**

1. Compare private-key cryptography and public-key cryptography in terms of key distribution. Explain why public-key cryptography is viewed as asymmetric cryptography.

Private Key Cryptography: Also known as symmetric key encryption because the sender and receiver both use the same key for encrypting/decrypting.

### Public Key Cryptography: also known as asymmetric key encryption. The sender encrypts a message with a public key and the message is decrypted using a private key. Public key encryption is asymmetric because one key is made available publicly and the other is a secret private key for decryption.

1. Briefly explain the three broad categories of applications of public-key cryptography.   
   * **Encryption/decryption** (for confidentiality)
   * **Digital signatures** (for authentication)
   * **Key exchange** (of session keys)
2. Explain how a user, say, B, can deliver a **secret session key K** to a user A on a public channel by using a public-key scheme, with the session key inaccessible to any unauthorized party.

A generates a temporary pair of public/private keys

A sends B public key and identity

B generates session key and sends it back to A using the public key encryption.

A decrypts the session key using the private key generated in step 1

1. Explain why RSA cipher is secure, even if a hacker knows the encryption algorithm and the public key.

The RSA cipher is secure because it uses both a public and private key. If an attacker knows the encryption algorithm and public key they must also have access to the private key in order to decrypt the message.

1. Given an asymmetric key cipher. What are the roles of the public and private keys, in data encryption and digital signature, respectively?

Public keys and private keys play different roles in asymmetric encryption. Public keys are generated and made available publicly for people to encrypt messages (confidentiality). A private key allows someone to sign a message using a digital signature which provides authentication (the user is who they claim they are). The digital signature can be checked against the public key so those who do not have access to the public key can verify digital signatures.

1. RSA algorithm is very useful in data encryption and decryption for commercial systems. Would you think RSA will replace AES? Why or why not? Differentiate between AES and RSA.

RSA could potentially replace AES. It depends on the situation which is most applicable. For example if you are encrypting files locally on your computer AES should could be sufficient for encrypting/decrypting.   
  
If communicating with many different people RSA would be a better mechanism to use because it only requires a single generated public/private key. While AES on the other hand would require a symmetric key generated for every communication channel which could get computationally expensive if dealing with a large number of people.

AES is more secure because only a single individual/entity has access to the private key. In symmetric encryption there are 2 possible places where the key could potentially be stolen – from the sender AND the receiver. Trusting the receiver to have the same security in place as the sender may be a naive assumption and potential security risk.

1. Reviewthe lecture notes on Diffie-Hellman Key Exchange, and answer the following question.

Use a prime, say,*q*=23, and primitive root α=3 to exchange a shared secret session key. For an example you canassume that Users A and B have selected their secret keys 10 and 11, respectively. In this example, what is the final secret session key shared by A and B?

Compute Public Keys:

YA =310mod (23)  
YA= 8  
  
YB= 811 mod 23  
YB= 1

Compute Shared Session Keys:  
KAB= YBXA mod (23)  
KAB= 110 mod (23)  
KAB= 1KAB= YAXB mod (23)  
KAB= 811 mod (23)  
KAB= 1

**Part 2 – Challenge Exercises**

Perform encryption and decryption using RAS algorithm, (as showed in Lecture 3 Slides), for the following:

1. p=3, q=13, e=5, and suppose the plaintext is M=10

n = pq  
n = (3)(13)  
n= (39)  
  
ø(n) = (p-1)(q-1)  
ø(n) = (3-1)(13-1)  
ø(n) = 24  
  
d = (d \* e) % ø(n) = 1  
d = (d \* 5) % 24 = 1  
d = 5  
  
C = Memod(n)  
C = 105mod 39  
C = 4  
  
D = Cd mod (n)  
D = 45 mod 39  
D = 10

1. p=5, q=7, e=7, and suppose the plaintext is M=12

n = pq  
n = (5)(7)  
n= (35)  
  
ø(n) = (p-1)(q-1)  
ø(n) = (5-1)(7-1)  
ø(n) = 24  
  
d = (d \* e) % ø(n) = 1  
d = (d \* 7) % 24 = 1  
d = 31  
  
C = Me mod(n)  
C = 127 mod 35  
C = 33  
  
D = Cd mod (n)  
D = 337 mod 35  
D = 12

1. p=7, q=13, e=5, and suppose the plaintext is M=8

n = pq  
n = (7)(13)  
n= (91)  
  
ø(n) = (p-1)(q-1)  
ø(n) = (7-1)(13-1)  
ø(n) = 72  
  
d = (d \* e) % ø(n) = 1  
d = (d \* 5) % 72 = 1  
d = 29  
  
C = Me mod(n)  
C = 85mod 91  
C = 8  
  
D = Cd mod ø(n)  
D = 829 mod 91  
D = 8

1. p=11, q=7, e=11, and suppose the plaintext is M=7.

n = pq  
n = (11)(7)  
n= (77)  
  
ø(n) = (p-1)(q-1)  
ø(n) = (11-1)(7-1)  
ø(n) = 60  
  
d = (d \* e) % ø(n) = 1  
d = (d \* 11) % 60 = 1  
d = 11  
  
C = Me mod (n)  
C = 811 mod 77  
C = 7  
  
D = Cd mod ø(n)  
D = 711 mod 77  
D = 7

**Part 3 – Exercises via CrypTool**

Using the CrypTool do the following:

1. Go: *Digital Signatures/PKI*⇨*PKI*⇨*Key Generation*. Generate a pair of RSA keys. The bit length of your key should be **512**. The PIN for your key pair can be: **3413ict**
2. Using the RSA cipher and your key encrypt the following article. Keep the ciphertext for the next step.
3. Decrypt the ciphertext. Check whether the decrypted message is exactly the original message.

The decrypted ciphertext is the same as the original message. The only difference is that the paragraphs are separated by the hex values ‘20 OD 0A’.

A flurry of events in 1995 demonstrated that issues related to electronic commerce and information security are of deep concern to the public, businesses, government, researchers, and users of the rapidly expanding Internet. The sometimes heated and wide ranging debate concerning cryptographic policy, content controls, commerce, and interoperability on the Internet tends to divert attention away from the need for a reasoned assessment and understanding of the true dynamics of nurturing a diverse global marketplace on the Internet. Lost in the contentious debate is a principle we feel is particularly important given the nature of information technology: that a policy consistent with user requirements and market acceptance provides economic benefits. In some cases, the 'economic pie' can be expanded--or shrunk--by corporate or government actions, inevitably affecting all.

We argue that information security is compromised if federal policies and corporate initiatives ignore user requirements and the basic principles of Internet conomics.This in turn may limit market acceptance of new research, services, applications, and technologies. For example, unintended results from ill-formed federal laws may severely limit economic benefits gained from billions of dollars of federally sponsored research that created and sustained the Internet. Furthermore, in the guise of enhanced security and advanced features, proprietary systems and partitioned markets lead to a lack of interoperability that further compromises prospects for society to realize the aforementioned benefits. Many of these problems can be avoided by an open policymaking process that is informed by collaborative research and development activities.

It would be ironic indeed if the set of federal policies that founded and sustained the precursors of the evolving electronic marketplace centered on the Internet forced those new opportunities offshore. Aside from affecting the balance of trade, jobs andopportunities for further innovation will possibly be lost to overseas competitors. Specifically, the information security policies of the Cold War era, which provided much of the motivation for the critical federal research and development support of the Internet and its predecessors, the NSFnet and ARPANET, threaten to cripple the development of commercially acceptable levels of security for electronic marketplace transactions.

These issues are discussed in this paper, by drawing on recent events and the Commerce and Information Security session of March 9-10, 1995; part of an NSF and ARPA- sponsored workshop on Internet Economics held at MIT. An intensified dialog among industry, academia, government, and the public on information security and electronic commerce issues is clearly needed. Our research shows that these issues are critical to establishing and maintaining U.S. leadership in the Age of Information.

[By Lee McKnight, Richard Jay Solomon, BrankoGerovac, David Carver, Clark Johnson, David Gingold and Joe Reagle, March 1995]