PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Networks and Cybersecurity Essentials (ACCA4024)

Lab 9: The art of ensuring Integrity

(Digital Signatures)

Cisco | Networking Academy®
Mind Wide Open™

Objectives

Using open source password cracking tool to recover the password.

Use of Digital Signatures.

Tasks

1. Use John the ripper tool to recover the passwords of Alice, Bob, Eve and Eric
2. Create digital Signatures to validate the document

Required Resources

- PC with Ubuntu 16.0.4 LTS installed in a VirtualBox or VMware virtual machine. (*Alternatively,* Any Linux Platform)
- Internet Connection to refer the outcomes
- References:
  - John the Ripper: http://www.openwall.com/john/
  - Digital Signatures: http://nmichaels.org/rsa.py

Task 1

➔ Login as User Cisco.
➔ Go to Terminal and Type the following commands and examine
➔ Run John the Ripper *(Hint: Change your directory to Downloads/ John-1.8.0/run)*

- cisco@ubuntu:~/Downloads/john-1.8.0/run$ sudo ./unshadow /etc/passwd /etc/shadow > mypasswd

- *This command will combine the /etc/passwd file where user accounts are stored, with the /etc/shadow file where user passwords are stored, into a new file called "mypasswd".*

- Recover Passwords: Type the following command in terminal:
  - cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd

There are no cracked passwords at this point. Why?

Maybe its due to the passwords being encrypted.

- Type the following command in terminal:
  - cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --wordlist=password.lst --rules mypasswd --format=crypt

- *The program, John the Ripper, uses a predefined dictionary called password.lst with a standard set of predefined "rules" for handling the dictionary and retrieves all password hashes of both md5crypt and crypt type.*
- The results should display the passwords for each account. To check the passwords and evidence them, open the file you have created to see the passwords cracked

There are cracked passwords. List the outcome.

```
password1  (Eric)
12345  (Bob)
123456  (Alice)
password (cisco)
password (Eve)
```

Task 2

Using Digital Signatures

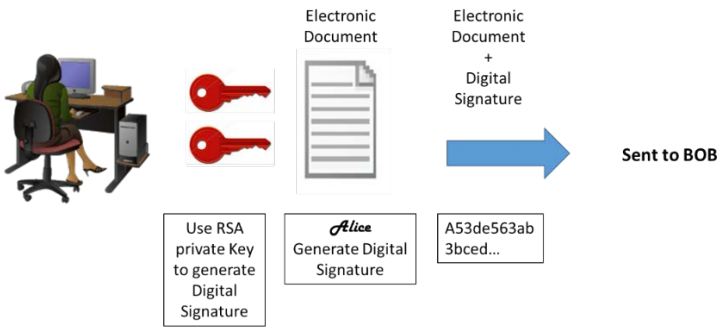
In this part, you will use a website to verify a document signature between Alice and Bob. Alice and Bob share a pair of private and public RSA keys. Each of them uses their private key to sign a legal document. They then send the documents to each other. Both Alice and Bob can verify each other's signature with the public key. They must also agree on a shared public exponent for calculation.

Table 1 - RSA Public and Private Keys

Public RSA Key	d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d79252f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24beb9c825b73ebf549
Private RSA Key	47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352df58848adad11a1
Public Exponent	10001

Sign the Document.

Alice signs a legal document and send it to Bob using the RSA public and private keys shown in the table above. Now Bob will have to verify Alice's digital signature in order to trust the authenticity of the electronic document.



Verify Digital Signature.

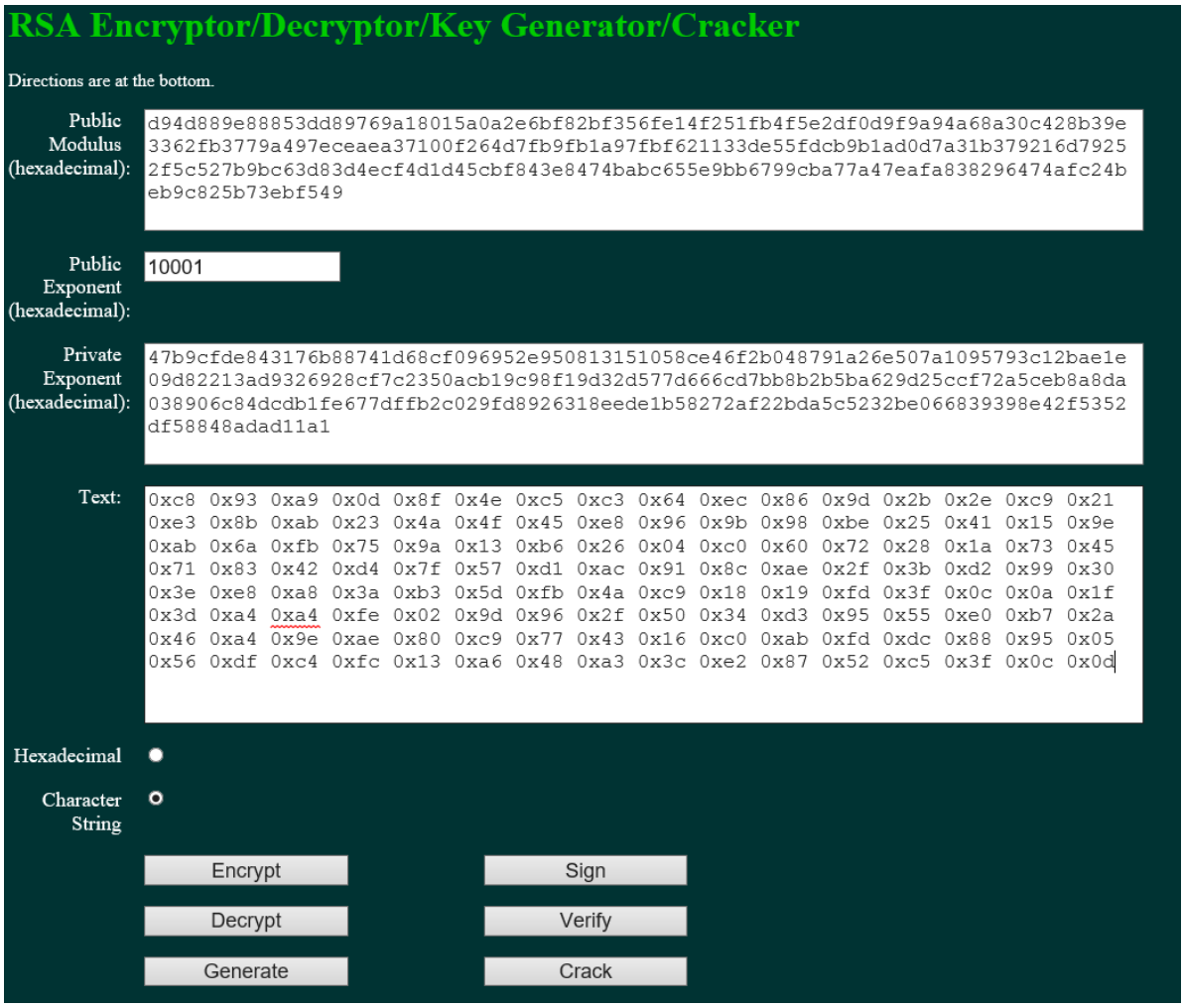
Bob receives the document with a digital signature shown in the table below.

Table 2 - Alice's Digital Signature

Alice's Digital Signature
0xc8 0x93 0xa9 0x0d 0x8f 0x4e 0xc5 0xc3 0x64 0xec 0x86 0x9d 0x2b 0x2e 0xc9 0x21 0xe3 0x8b 0xab 0x23 0x4a 0x4f 0x45 0xe8 0x96 0x9b 0x98 0xbe 0x25 0x41 0x15 0x9e 0xab 0x6a 0xfb 0x75 0x9a 0x13 0xb6 0x26 0x04 0xc0 0x60 0x72 0x28 0x1a 0x73 0x45 0x71 0x83 0x42 0xd4 0x7f 0x57 0xd1 0xac 0x91 0x8c 0xae 0x2f 0x3b 0xd2 0x99 0x30 0x3e 0xe8 0xa8 0x3a 0xb3 0x5d 0xfb 0x4a 0xc9 0x18 0x19 0xfd 0x3f 0x0c 0x0a 0x1f 0x3d 0xa4 0xa4 0xfe 0x02 0x9d 0x96 0x2f 0x50 0x34 0xd3 0x95 0x55 0xe0 0xb7 0x2a 0x46 0xa4 0x9e 0xae 0x80 0xc9 0x77 0x43 0x16 0xc0 0xab 0xfd 0xdc 0x88 0x95 0x05 0x56 0xdf 0xc4 0xfc 0x13 0xa6 0x48 0xa3 0x3c 0xe2 0x87 0x52 0xc5 0x3f 0x0c 0x0d

Click http://nmichaels.org/rsa.py to use the online RSA tool to verify the authenticity of Alice's digital signature.

Table 3 - Online Digital Signature Tool



Copy and paste the **public** and **private** keys from Table 1 above into the **Public Modulus** and **Private Exponent** boxes on the website as shown in the picture above.

Make sure the Public Exponent is 10001.

Paste Alice's digital signature from Table 2 in the box labeled text on the website as shown above.

Now BOB can verify the digital signature by clicking the **Verify** button near the bottom center of the website.

Whose signature is identified?

Alice's

Generate a Response Signature.

Bob receives and verifies Alice's electronic document and digital signature. Now Bob creates an electronic document and generates his own digital signature using the private RSA Key in Table 1 (Note: Bob's name is in all capital letters).

Table 4 - BOB Digital Signature

BOB's Digital Signature
0x6c 0x99 0xd6 0xa8 0x42 0x53 0xee 0xb5 0x2d 0x7f 0x0b 0x27 0x17 0xf1 0x1b 0x62 0x92 0x7f 0x92 0x6d 0x42 0xbd 0xc6 0xd5 0x3e 0x5c 0xe9 0xb5 0xd2 0x96 0xad 0x22 0x5d 0x18 0x64 0xf3 0x89 0x52 0x08 0x62 0xe2 0xa2 0x91 0x47 0x94 0xe8 0x75 0xce 0x02 0xf8 0xe9 0xf8 0x49 0x72 0x20 0x12 0xe2 0xac 0x99 0x25 0x9a 0x27 0xe0 0x99 0x38 0x54 0x54 0x93 0x06 0x97 0x71 0x69 0xb1 0xb6 0x24 0xed 0x1c 0x89 0x62 0x3d 0xd2 0xdf 0xda 0x7a 0x0b 0xd3 0x36 0x37 0xa3 0xcb 0x32 0xbb 0x1d 0x5e 0x13 0xbc 0xca 0x78 0x3e 0xe6 0xfc 0x5a 0x81 0x66 0x4e 0xa0 0x66 0xce 0xb3 0x1b 0x93 0x32 0x2c 0x91 0x4c 0x58 0xbf 0xff 0xd8 0x97 0x2f 0xa8 0x57 0xd7 0x49 0x93 0xb1 0x62

Bob sends the electronic document and digital signature to Alice.

Verify Digital Signature.

Copy and paste the **public** and **private** keys from Table 1 above into the **Public Modulus** and **Private Exponent** boxes on the website as shown in the picture above.

Make sure the Public Exponent is 10001.

Paste Bob's digital signature from Table 4 in the box labeled text on the website as shown above.

Now Alice can verify the digital signature by clicking the **Verify** button near the bottom center of the website.

Whose signature is identified?

Bob's

Verify this Digital Signature

Table 5 – Your lecturer's Digital Signature

Public RSA Key	d639edcb90b508fba5005ed5f6e2b06f885e7a2ad5f6babbde7b0481e8b7af73f4a821951757f797 6e2b8a925b6940e930a4bab189ccb93a9e81f74829140e767ec2ef3acad7afecb3d1a114498524cd 084f9ae54a7ffd1f35c50ebdb24abb95dd5d8dfcd3ee7dd06630c831877bee8549a1c2b615e53098 8f5cee0255a75f71
Private RSA Key	63cf1d91885c30513e310bfe584689b98d29a775a9b6888ddb3c297f75338f9550d9bcbbbfe28642 915bcbf6208ccb6759f885db0dbeca561b5fa61c82b70b7d2337c28ce1934fc7ad035c87367a089a 24d2eca2583822fd5a7505bb76a7c3fd8486989ef8876617488a07330cae414fce708b1c7278151d e92a994a639b85b9
Public Exponent	10001
Text	0x8d 0x2d 0xcc 0x0c 0x12 0xdf 0xa2 0xbe 0x16 0x51 0x6e 0x5a 0x6a 0xf3 0x02 0xb9 0xf4 0x26 0x90 0xbe 0xfb 0x8f 0x3e 0x42 0xf4 0x59 0x60 0x6c 0xb5 0x44 0xbb 0x89 0xe1 0x8e 0x34 0x7f 0xa4 0x00 0xcf 0x30 0x12 0x89 0xb8 0x44 0x7f 0xde 0x23 0x70 0xad 0x92 0xdb 0xf9 0x77 0x87 0xf4 0x8e 0xe9 0xd2 0xd0 0xcc 0xa0 0x85 0x43 0x21 0xd1 0xcf 0x9b 0x51 0x11 0x39 0xe7 0xd2 0x6f 0xa3 0x1a 0x32 0xa6 0xed 0xe4 0x2d 0xbc 0x98 0xe9 0x69 0xaf 0xb7 0x4b 0x21 0xfe 0x62 0x38 0x10 0xfd 0x3e 0x79 0x90 0x75 0x08 0x14 0x0f 0x43 0x9b 0xb2 0xa5 0xe1 0x72 0xee 0x41 0xee 0x0d 0x2c 0xfb 0x2c 0x36 0x28 0x32 0xed 0xac 0x19 0x60 0x23 0x88 0x1d 0xd8 0x74 0xee 0x47 0xa0

Whose signature is identified?

Nitheesh's

Create Your Own Digital Signature

Now that you see how digital signatures work, you can create your own digital signature.

Generate a New Pair of RSA Keys.

Go to the website tool and generate a new set of RSA public and private keys.

Delete the contents of the boxes labeled **Public Modulus**, **Private Modulus** and **Text**. Just use your mouse to highlight the text and press the delete key on your keyboard.

Make sure the “Public Exponent” box has **10001**.

Why should you have the Public Exponent as 10001? Research and document your reflections here.

Generate a new set of RSA keys by clicking the **Generate** button near the bottom right of the website.

Copy the new keys in Table 6.

Table 6 - New RSA Keys

Public Key	A string of 256 hexadecimal characters will be displayed for both the public and private keys. The keys will be different from one another. b1635937ccaebad1031fa304ec84981b4acdf8d722e61e734cf62ef02266335e550d111d3a48e52a cb99cbf60ab433e7c94566d2793692c2faff4c7118acebf29b5483bedec54f198e5ce2dd3fc63954 c68f667d24d5423ea796334dd73761a4b96e5483e78799284506a29af86a1f20d7f6555b4f41d3ba feea4c74f002c6a7
Private key	A string of 256 hexadecimal characters will be displayed for both the public and private keys. The keys will be different from one another. 747eea78dad3659d1e90085f937500efeb90997bb04fb06fc87b65180f7f4efd049e303f21a7fdd8 bd1da3f551d246c4524a61dc97fe5f23edf2fc20ca33c63fd5fca5a886c8b34f2b690964357f77a3 b2299c2de0ca49ca0a7c463a9a7741409849b63e127e57c9d11fd96abafaf145683fb285c499160a fcc8f8374c4e7201

Now type in your full name into the box labeled **Text** and click **Sign**.

Table 7 - Personal Digital Signature

Personal Digital Signature	A string of characters with this format will be displayed. 0x23 0x90 …….

0xa3 0x42 0xb1 0xce 0x51 0xf3 0xf3 0xa1 0x30 0x39 0x11 0x79 0x51 0x94 0x37 0xb5 0x1e 0x80 0xc9 0x1d 0xf5 0x4a
0x1e 0xbc 0xa5 0x7b 0x4d 0xa7 0xfd 0xce 0xce 0x6e 0x80 0x6e 0x01 0x99 0xc1 0x7f 0x59 0xa8 0x5b 0x9b 0xb0 0x3b
0x51 0x19 0x1b 0x9a 0x20 0x59 0x5a 0x05 0x65 0x99 0x13 0x51 0x8d 0x64 0x77 0x81 0xf6 0x39 0xcd 0xa7 0x2e 0x5
0x53 0x29 0xc9 0x6f 0x3e 0xe8 0x1c 0xef 0xc3 0x07 0xd7 0x5b 0x70 0xe0 0x90 0xed 0x42 0x32 0x48 0xea 0x69 0x5a
0xd0 0x80 0xde 0x6a 0x69 0x8d 0xc8 0xa2 0xe3 0xb2 0xef 0x8b 0x23 0x11 0x86 0x66 0xcc 0xac 0x20 0xef 0x78 0xc9
0x26 0x4b 0x2d 0x13 0x7c 0xe7 0xdb 0xf0 0x2a 0x48 0xe3 0xb6 0x9a 0x06 0x87 0xb7 0x54 0xd1

Exchange and Verify Digital Signatures

Now you can use this digital signature.

Exchange your new public and private keys in Table-6 with your lab partner.

Record your lab partner's public and private RSA keys from their Table-6.

Record both keys in the table below.

Table 8- Lab Partners RSA Keys

Public key	A string of 256 hexadecimal characters will be displayed for both the public and private keys. The keys will be different from one another.
9672aaebf6182958d1630d6a085a2c69f3dbe0fd010f57cff764d572fdb15a217aac77c603578e96cd6d4d 16f4dcbb3e407183ee8f64de6ef7f4dae99ec23cf605b26852654d843c83c50c148a4b130 fad6d906a207a8e65f9ec7fc46ec991ce67e10de066e5da81fb7e41da9fdfee7489154f408c22ba7 7e53feda69b47fb9	
Private key	A string of 256 hexadecimal characters will be displayed for both the public and private keys. The keys will be different from one another.
ab49eb29138a9c2ae4bfc457beb6541f2ffe3fdd9af4d73444c6ad3baf03397d1ba159850d963086 1e3a0b35285a0f8495741f770bc0b6ab245868ca1a6c125a57a10c8bbe0fbc5e25aa20e67b1b88e3 ed6da5255d8958b0aa6d015b28f18fc62032b95fd1f6b3e94c354438748a72659bc3510b0e26085f cf5f1bf4a656c01	

Now exchange their digital signature from their Table-6. Record the digital signature in the table below.

Lab Partner's Digital Signature	A string of characters with this format will be displayed. 0x23 0x90 …….
0x01 0x26 0xfd 0x7b 0xc5 0xd1 0x11 0x16 0xb8 0x31 0x46 0xc5 0xc0 0x7a 0x25 0x1b 0x63 0x64 0x9d 0xa5 0xc9 0x8b 0xd5 0xe6 0x7b 0x96 0x3b 0xc7 0x7a 0x3c 0x27 0x62 0x73 0xac 0xd7 0x5b 0x72 0xfe 0x10 0x7c 0x26 0x04 0x22 0x83 0x47 0xbe 0x8b 0xf9 0x91 0x13 0x37 0xe1 0x3d 0x9c 0xa2 0x02 0xbd 0x83 0x51 0x5e 0x4f 0x17 0x06 0x58 0x31 0xb 0x8 0x15 0x1d 0x1 0x1 0xb4 0x36 0xde 0x21 0x2a 0xe2 0xce 0x62 0xa3 0x22 0x5b 0x2f 0x3f 0x1b 0xd1 0x63 0x71 0x3f 0x59 0x66 0xd2 0x30 0xdd 0xaf 0x40 0xac 0x39 0x68 0x8e 0xe7 0x31 0xf4 0x83 0x9f 0x0d 0x79 0xd7 0x87 0xdb 0xb0 0x8e 0x0e 0x59 0x59 0x76 0x6c 0x9a 0x6c 0x27 0x43 0x1f 0xcc 0x16 0xf3 0x23 0x0a 0x0d 0x56	

Verify Lab Partner's Digital Signature

To verify your lab partner's digital signature, paste his or her public and private keys in the appropriate boxes labeled **Public and Private modulus** on the website.

Now paste the digital signature in the box labeled **Text**.

Now verify his or her digital signature by clicking the button labeled verify.

What shows up in the Text box?

Abby's

Learnings from tutorials so far:

Part 1 (Packet Tracer, Host Machines)

- ✓ ***Build a home Network***
- ✓ ***Understand and configure IP Address***
- ✓ ***Use Ping/ Trace route Utility to check the connection status***
- ✓ ***Use ipconfig /all command to determine the MAC address of a Windows computer on an Ethernet network.***
- ✓ ***Analyze a MAC address to determine the manufacturer.***
- ✓ ***Analyze the Wired and Wireless Network connection.***
- ✓ ***Analyze Address Resolution Protocol (ARP).***
- ✓ ***Connect to a Wireless Router and configure the basic settings in a wireless router and add security features.***
- ✓ ***Use nslookup command to understand the url to ip conversion.***
- ✓ ***Configure basic connectivity settings in Intermediate devices (Switch/ Router).***
- ✓ ***Work with SBA Packet Tracer Files/ environment***
- ✓ ***Configure ftp, web, email, dns, ntp and aaa Servers***

Part 2

- ✓ ***Set up a virtual lab environment***
- ✓ ***Troubleshooting the virtual lab environment***
- ✓ ***Working with virtual machines***
- ✓ ***Authentication, Authorization and Accounting***
- ✓ ***Threats and Vulnerabilities – Using NMAP***
- ✓ ***Hide and Seek – Use Steghide to hide a data file within an image file***
- ✓ ***Password Cracking using John the Ripper***
- ✓ ***Digital Signatures – Creating and Verifying.***