

A Brief Introduction to Cryptography

Parshuram Budhathoki
Assistant Professor
Cameron University

Topics

- Cryptography (Crypto)
- Crypto Services
- Crypto Primitives for security services
- Certificate Authority
- Application: Everyday Cryptography

Cryptography

- Κρυπτός (Hidden or Secrete) and γράφω (writing)
- Practice and study of techniques for secure communication in the presence of third parties called adversaries.

Why do we need security services?

- ✓ Confidentiality
- ✓ Data Integrity
- ✓ Data Origin Authentication
- ✓ Non- Repudiation
- ✓ Entity Authentication

Why do we need security services?

✓ Confidentiality



hello



Why do we need security services?

✓ Data Integrity



Why do we need security services?

✓ Data Origin Authentication



hello



Why do we need security services?

✓ Non Repudiation



I want to buy 1000 watches



Amazon.com,
Inc.
Electronic commerce company



Why do we need security services?

✓ Entity Authentication



I want 280 bags as well.



Amazon.com,
Inc.
Electronic commerce company



(Some) Terms Used in Crypto World!

- ✓ Cryptography
- ✓ Cryptography primitives
- ✓ Cryptography algorithm
- ✓ Cryptographic protocol
- ✓ Cryptosystem

(Some) Terms Used in Crypto World!

- ✓ **Cryptography**: design and analysis of mechanism based on mathematical techniques
- ✓ **Cryptography primitives**: process that provides number of specified services.
- ✓ **Cryptography algorithm**: the particular specification of cryptographic primitives
- ✓ **Cryptographic protocol**: sequence of message exchange and operation between one or more parties
- ✓ **Cryptosystem**: implementation of some cryptographic primitives and their infrastructure

Cryptographic Primitives for Security Services

- ✓ Encryption and Decryption
- ✓ MAC (Message Authentication Code)
- ✓ Digital Signature
- ✓ Hash Function(One Way Function)

Cryptographic Primitives for Security Services

✓ Encryption and Decryption



hello



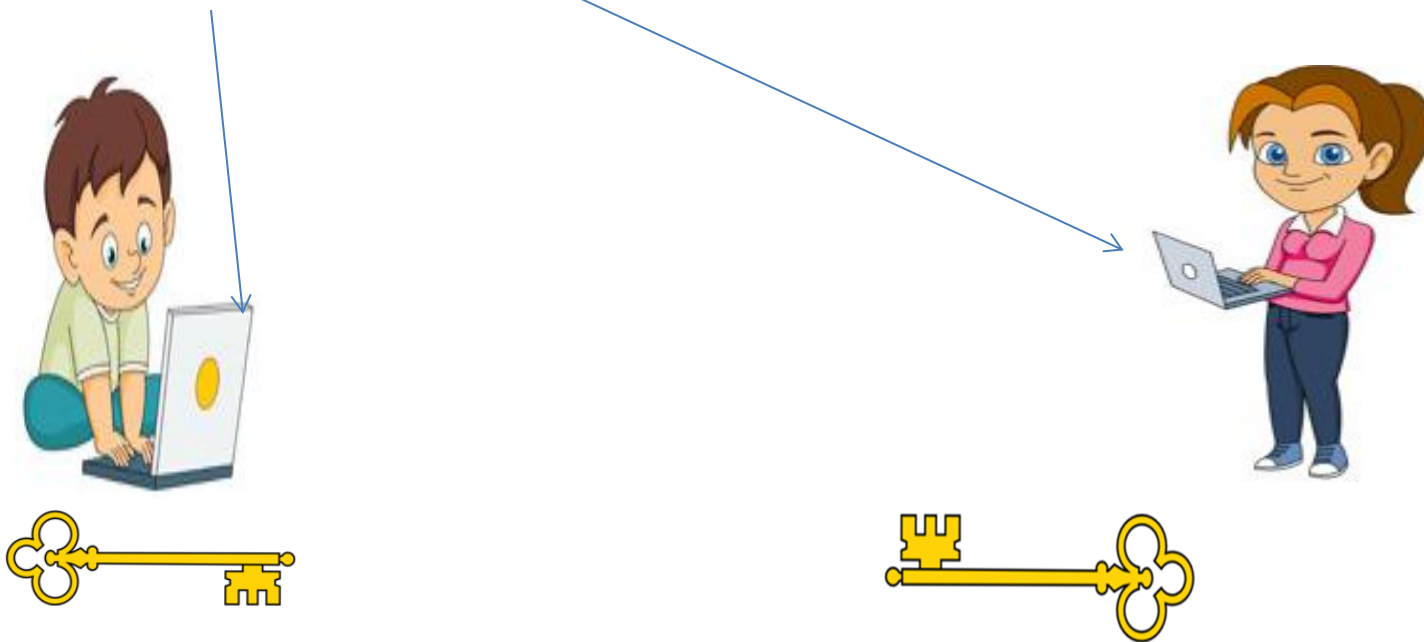
Cryptographic Primitives for Security Services

✓ Encryption and Decryption



Cryptographic Primitives for Security Services

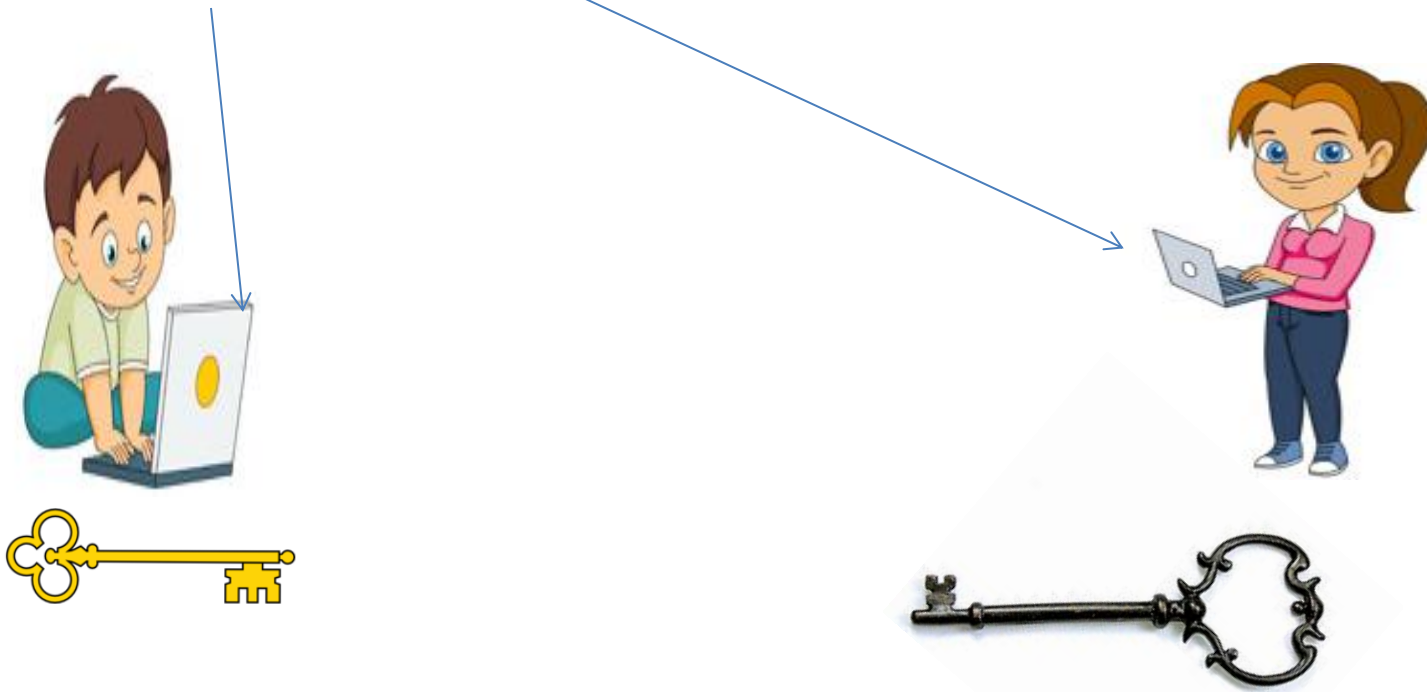
✓ Encryption and Decryption



Private (Symmetric) Key Cryptosystem

Cryptographic Primitives for Security Services

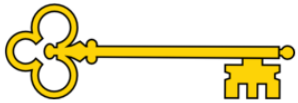
✓ Encryption and Decryption



Public (asymmetric) Key Cryptosystem

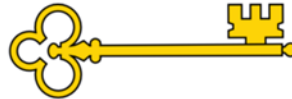
Cryptographic Primitives for Security Services

✓ Encryption and Decryption



Cryptographic Primitives for Security Services

✓ Encryption and Decryption

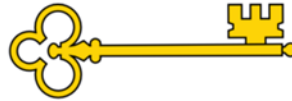


DES(Data Encryption Standard)

3DES, 2DES

Cryptographic Primitives for Security Services

✓ Encryption and Decryption



AES (Advance Encryption Standards)

AES 128, AES 192, AES 256

Cryptographic Primitives for Security Services

✓ Encryption and Decryption



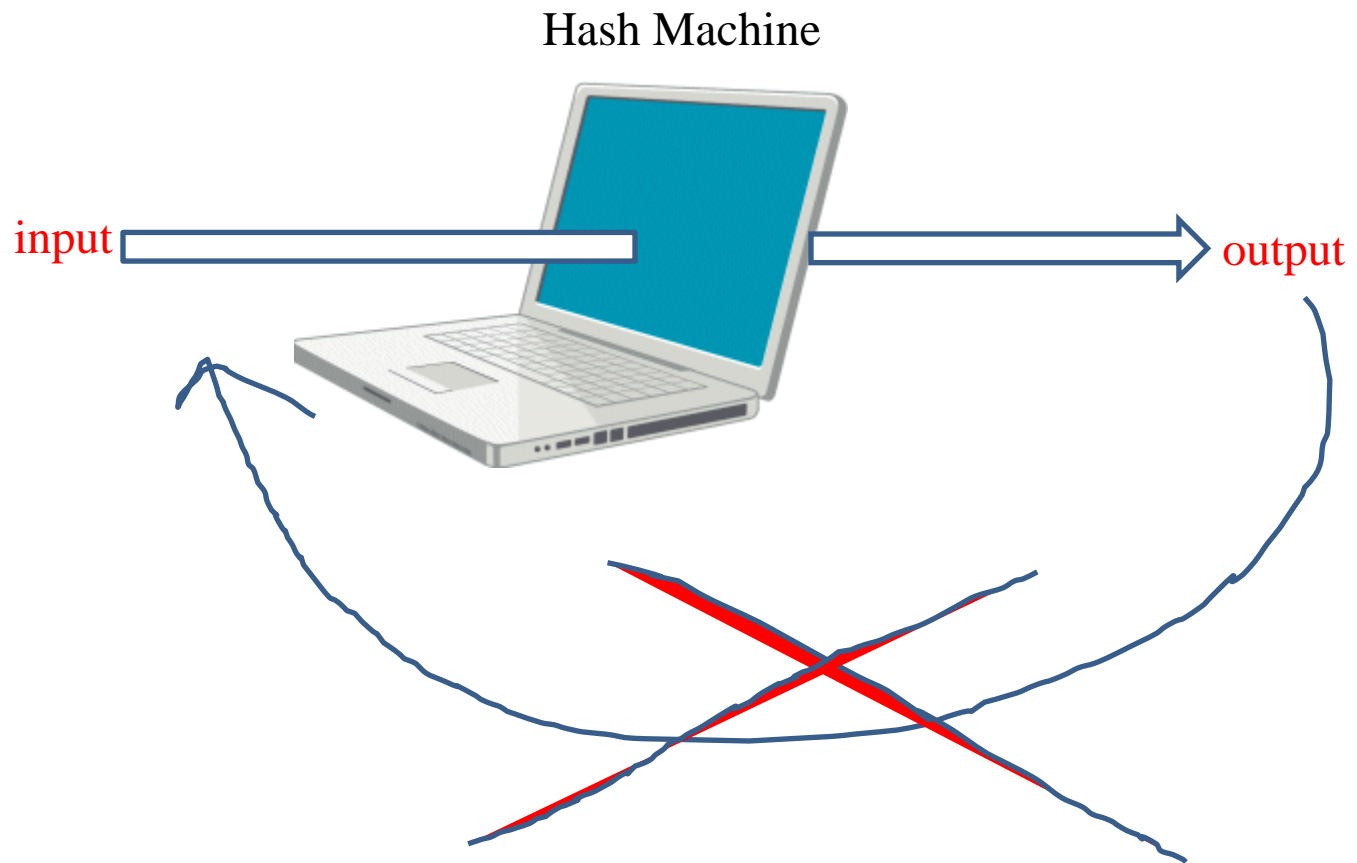
RSA

ElGamal

Elliptic-Curve variants

Cryptographic Primitives for Security Services

✓ Hash Function



Cryptographic Primitives for Security Services

✓ Hash Function

MD5

SHA-1

SHA-2 family: SHA-224, SHA-256, SHA-384 and SHA-512

SHA-3

RIPEMD

Whirlpool

Cryptographic Primitives for Security Services

✓ Hash Function

MD5

SHA-1

SHA-2 family: SHA-224, SHA-256, SHA-384 and SHA-512

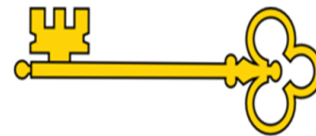
SHA-3

RIPEMD

Whirlpool

Cryptographic Primitives for Security Services

- ✓ MAC (Message Authentication Code)



MAC

HMAC

Cryptographic Primitives for Security Services

✓ Digital Signature



I want to buy 1000 watches



Amazon.com,
Inc.
Electronic commerce company



Cryptographic Primitives for Security Services

✓ Digital Signature

RSA based

DSA (ECDSA) based

Summary: Crypto Primitives and Services

	Confidentiality	Data integrity	Data origin auth.	Non-repudiation	Entity authentication
Encryption	✓				
Hash Function		✓			
MAC		✓	✓	✓	
Digital Signature		✓	✓	✓	

✓ Yes

✓ Sometime

Certificate Provider: Certificate Authority

- VeriSign
- GeoTrust
- Comodo
- Digicert
- Thawte
- GoDaddy
- Network Solutions

Everyday Cryptography



CAMERON UNIVERSITY

[FUTURE STUDENTS](#)

[CURRENT STUDENTS](#)

[ACADEMICS](#)

[FACULTY &](#)

CAMERON UNIVERSITY DEPARTMENT OF ART, MUSIC AND THEATER ARTS

- PRESENTS -

SWG!

CAMERON
CENTENNIA



- GUESTS -

www.cameron.edu

www.cameron.edu

Your connection to this site is not private. [Details](#)

Cookies

9 from this site, 3 from other sites

Permissions

- Location: Ask by default
- Camera: Ask by default
- Microphone: Ask by default
- Notifications: Ask by default
- JavaScript: Allowed by default
- Plugins: Detect important content by default
- Images: Allowed by default
- Popups: Blocked by default
- Background Sync: Allowed by default
- Automatic Downloads: Ask by default
- MIDI devices full control: Ask by default

[Site settings](#)

RON UNIVERS

STUDENTS

ACADEMICS

FACULTY &

AMERON UNIVERSITY DEPARTMENT OF ART, MUSIC AND THEATER ARTS

- PRESENTS -

CAMERON
CENTENNIA



- GUESTS -



Secure Sign-in

 Save Online ID[Security & Help](#)[Forgot ID](#)[Forgot Passcode](#)[Enroll](#)

Banking

Choose

BankAmericard Cash Rewards™



I want cash back

[Offer details >](#)

BankAmericard Travel Rewards



I want travel rewards

[Offer details >](#)

Information for:

Select a state ▼

Online Banking




Manage your accounts during a commercial break.

[Enroll now »](#)

New to Bank of America

Explore banking solutions from Bank of America® and investment services from Merrill Edge®.

[Learn more](#)

 **Bank of America Corporation**
Secure Connection

You are securely connected to this site, owned by:

Bank of America Corporation
Chicago
Illinois, US

Verified by: Symantec Corporation

[More Information](#)



Personal

Small BU



Secure Sign-in



Save Online ID

[Security & Help](#)

[Forgot ID](#)

[Forgot Passcode](#)

[Enroll](#)

Banking

Credit C

BankAmericard Cash Rewards™ credit card

1% cash back everywhere, every time

2% cash back at grocery stores **AND NOW AT WHOLESALE CLUBS**

3%

Up to \$2,500 quarter

Information for:

Select a state

[Go](#)

Save more, faster

8 tips

Help hit your savings goals sooner with these simple tips.

[Learn more >](#)

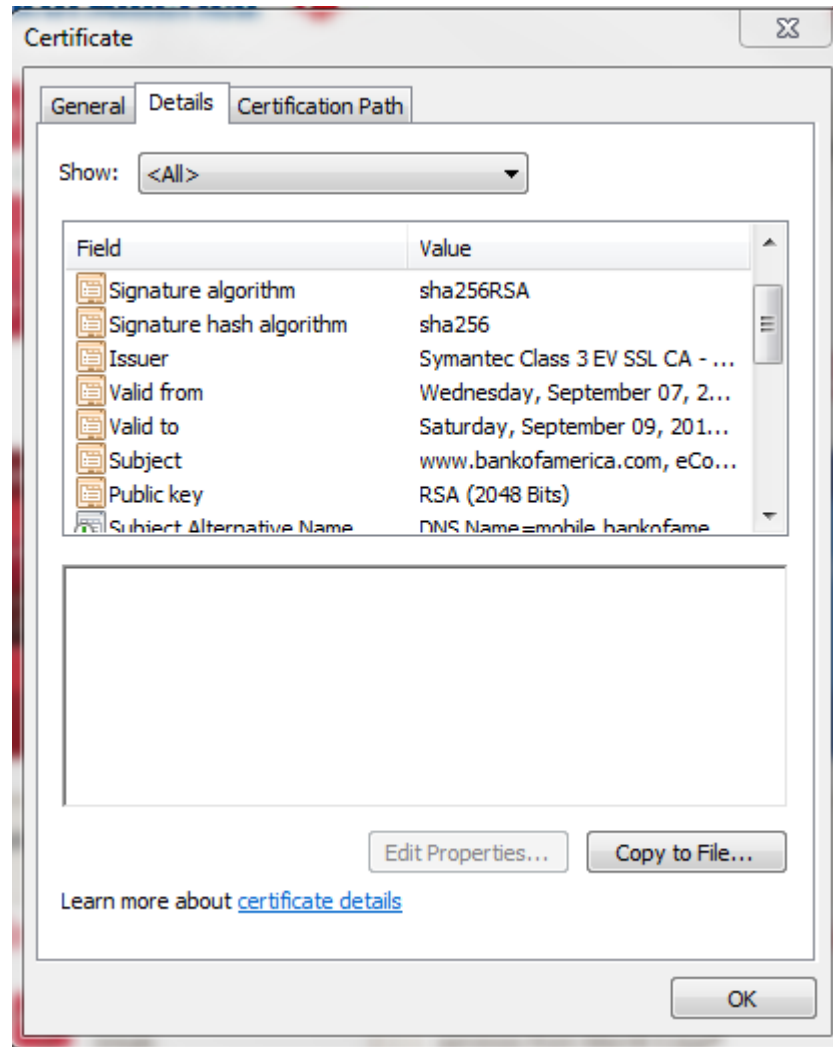
Online Bill Pay



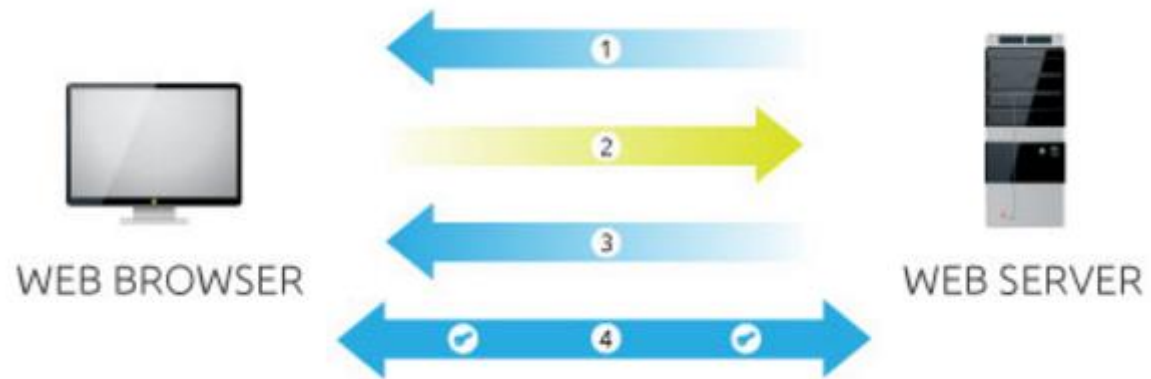
Makes bill payments easier to manage.

[Get started >](#)

Everyday Cryptography



Everyday Cryptography



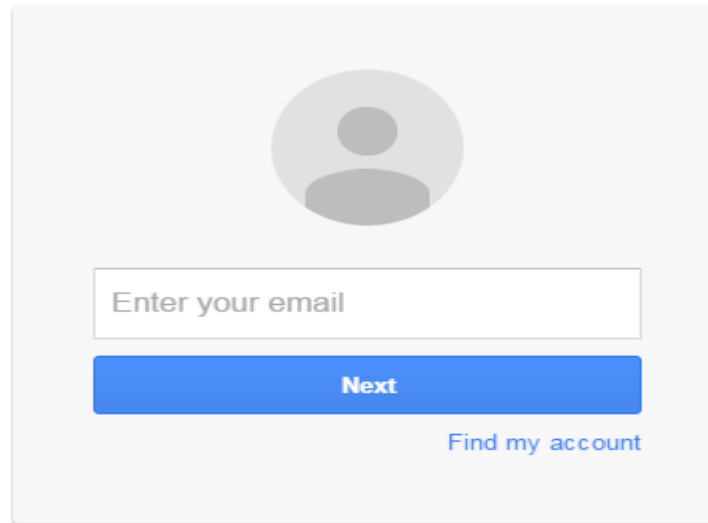
Everyday Cryptography

emails



One account. All of Google.

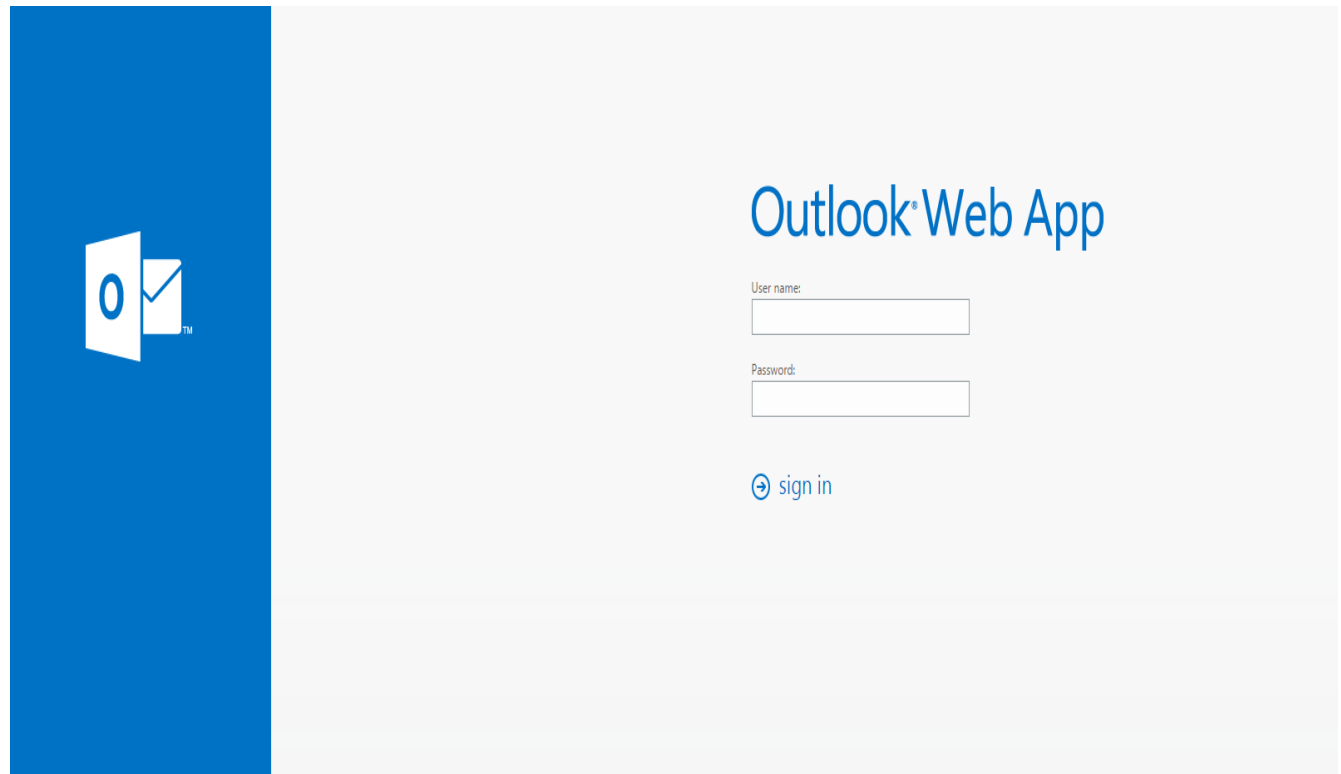
Sign in to continue to Gmail

A sign-in form with a grey background. At the top center is a grey circular icon representing a person. Below it is a white text input field with the placeholder text "Enter your email". Underneath the input field is a blue button with the text "Next" in white. To the right of the "Next" button is a blue link that says "Find my account".

[Create account](#)

Everyday Cryptography

emails



Everyday Cryptography

facebook

Email or Phone Password [Log In](#)

[Forgot account?](#)

Sign Up

It's free and always will be.

First name Last name

Mobile number or email

Re-enter mobile number or email

New password

Birthday

Month Day Year [Why do I need to provide my birthday?](#)

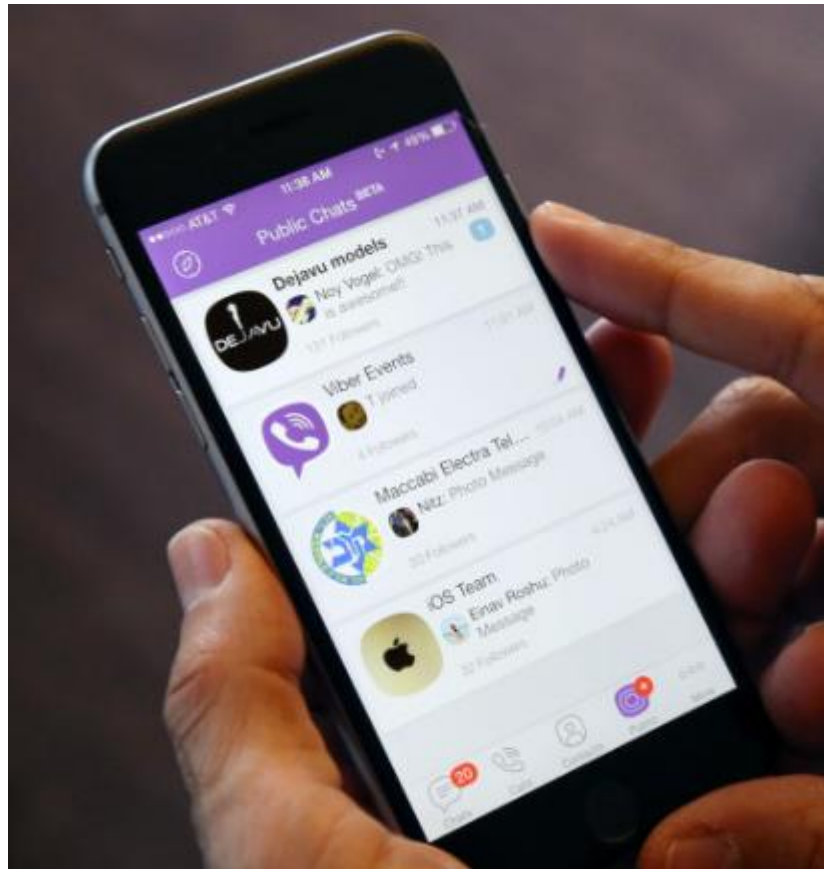
Female Male

By clicking Sign Up, you agree to our [Terms](#) and that you have read our [Data Policy](#), including our [Cookie Use](#).

[Sign Up](#)

[Create a Page](#) for a celebrity, band or business.

Everyday Cryptography



Everyday Cryptography

Password

A) /etc/passwd file

```
root:Jbw6BwE4XoUHo:0:0:root:/root:/bin/bash
carol:FM5ikbQt1K052:502:100:Carol Monaghan:/home/carol:/bin/bash
alex:LqAi7Mdyg/HcQ:503:100:Alex Insley:/home/alex:/bin/bash
gary:FkJXupRyFqY4s:501:100:Gary Kessler:/home/gary:/bin/bash
todd:edGqQUAaGv7g6:506:101:Todd Pritsky:/home/todd:/bin/bash
josh:FiH0ONcjPut1g:505:101:Joshua Kessler:/home/webroot:/bin/bash
```

B.1) /etc/passwd file (with shadow passwords)

```
root:x:0:0:root:/root:/bin/bash
carol:x:502:100:Carol Monaghan:/home/carol:/bin/bash
alex:x:503:100:Alex Insley:/home/alex:/bin/bash
gary:x:501:100:Gary Kessler:/home/gary:/bin/bash
todd:x:506:101:Todd Pritsky:/home/todd:/bin/bash
josh:x:505:101:Joshua Kessler:/home/webroot:/bin/bash
```

B.2) /etc/shadow file

```
root:AGFw$1$P4u/uhLK$12.HP35rlu65WlfcZq:11449:0:99999:7:::
carol:kjHaN%35a8xMM8a/0kMl1?fwtLAM.K&kw.:11449:0:99999:7:::
alex:1$1KKmfTy0a7#3.LL9a8H71lkwn/.hH22a:11449:0:99999:7:::
gary:9ajlknknKJHjhnu7298ypnAIJKL$Jh.hnk:11449:0:99999:7:::
todd:798P0J90uab6.k$k1PqMt%alMlprWqu6$.:11492:0:99999:7:::
josh:Awmqpsui*787pjnsnJJK%aappaMpQo07.8:11492:0:99999:7:::
```

Sample entries in Unix/Linux password files.

Everyday Cryptography

Password



Everyday Cryptography



Everyday Cryptography

The image shows a browser window displaying the login page of an ARRIS device. The browser's address bar shows the IP address 192.168.100.1. The page features a dark header with the ARRIS logo and navigation links for 'Wireless', 'HSD', and 'Logout'. The 'Wireless' link is highlighted in orange. Below the header, there is a 'Login' tab and a sidebar with two 'LOGIN' buttons. The main content area is titled 'Login' and includes a message: 'The default user name is 'admin'. Valid characters are the numbers 0 to 9, the letters a through z, and printable special characters (such as \$, !, ?, &, #, @, and others.)'. Below this message, there is a 'Login' section with two input fields: 'User Name' (containing 'admin') and 'Password'. Both fields have a question mark icon to their right. An 'Apply' button is located at the bottom of the form.

ARRIS

Wireless HSD Logout

Login

LOGIN

LOGIN

Login

The default user name is 'admin'. Valid characters are the numbers 0 to 9, the letters a through z, and printable special characters (such as \$, !, ?, &, #, @, and others.)

Login

User Name ?

Password ?

Apply

Everyday Cryptography

The screenshot shows the ARRIS router configuration interface. At the top, there is a navigation bar with the ARRIS logo and tabs for 'Wireless', 'HSD', and 'Logout'. Below this is a secondary navigation bar with tabs for 'Basic Setup', 'WAN Setup', 'LAN Setup', 'Wireless 2.4 GHz', 'Wireless 5 GHz', 'Firewall', 'MoCA', and 'Utilities'. The 'Wireless 2.4 GHz' tab is selected.

System Basic Setup

While your system has many configuration options, the options on this Basic Setup page are those required by most users. Click the tabs to access the other configuration pages to set advanced options. Hover the mouse pointer over the question mark icon next to an option to view a description of that option. For changes to take effect, you must click the Apply button.

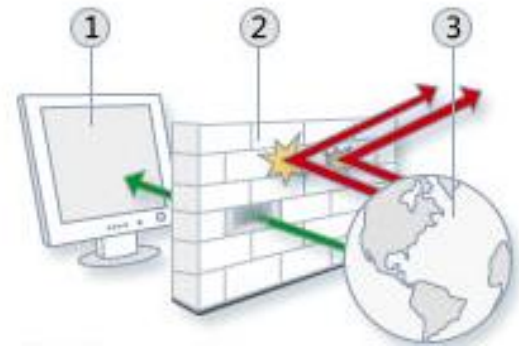
Basic Setup

- Enable Wireless: ?
- Wireless network Name (SSID): ?
- Broadcast Network Name (SSID): ?
- Tx Power Level: High ?
- Channel: Auto ?
- AP Isolation: ?
- Enable WMM: ?
- Security Mode: WPA2-PSK (AES) (Recommended) ?
- Pre-Shared Key: ?

SetupRouter.com

Everyday Cryptography

The screenshot shows a web browser interface for a router's configuration page, specifically the Firewall Settings section. The browser's address bar shows the URL 192.168.100.1. The page has a navigation menu at the top with tabs for Basic Setup, WAN Setup, LAN Setup, Wireless 2.4 GHz, Wireless 5 GHz, Firewall (selected), MoCA, and Utilities. On the left, there is a sidebar menu for the Firewall section, including options like Firewall Settings, Virtual Servers, Port Triggers, Client IP Filters, Client IPv6 Filters, DMZ, Parental Controls, and ALG. The main content area is titled "Firewall Settings" and contains a descriptive paragraph: "Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible." Below this are several toggleable settings, all of which are currently checked: "Firewall Enable/Disable", "DoS Attack Protection" (with sub-option "Enable DoS Attack Protection Firewall"), "Block Pings" (with sub-option "Enable Ping Blocking"), "IPSec Pass Through", "PPTP Pass Through", and "L2TP Pass Through". A partially visible "Block Fragmented IP Packets" option is at the bottom.



Everyday Cryptography



Everyday Cryptography



I am using the best known cryptosystem in the world. Am I secure?

Everyday Cryptography





Share / Email

National Cyber Security Awareness Month

Resources

National Cyber Security Awareness Month

October is National Cyber Security Awareness Month which is an annual campaign to raise awareness about cybersecurity. We live in a world that is more connected than ever before. The Internet touches almost all aspects of everyone's daily life, whether we realize it or not. National Cyber Security

Awareness Month (NCSAM) is designed to engage and educate public and private sector partners through events and initiatives to raise awareness about cybersecurity, provide them with tools and resources needed to stay safe online, and increase the resiliency of the Nation in the event of a cyber incident.

[Expand All Sections](#)

NCSAM 2016 Weekly Themes +

Get Involved +

Stop.Think.Connect. Toolkit +

NCSAM 2016 Resources +

NCSAM 2015 Highlights +

References:

- Everyday Cryptography Fundamental Principles & Applications by Keith M. Martin
- A Cryptography Primer by Philip N. Klein
- Introduction to Cryptography by Katz and Lindell
- Understanding Cryptography by Christof Paar and Jan Pelzl
- An Overview of Cryptography by Gary C. Kessler
<http://www.garykessler.net/library/crypto.html#trust>
- <http://www.howstuffworks.com>
- Many other online resources.

Questions ?

Thank you 😊