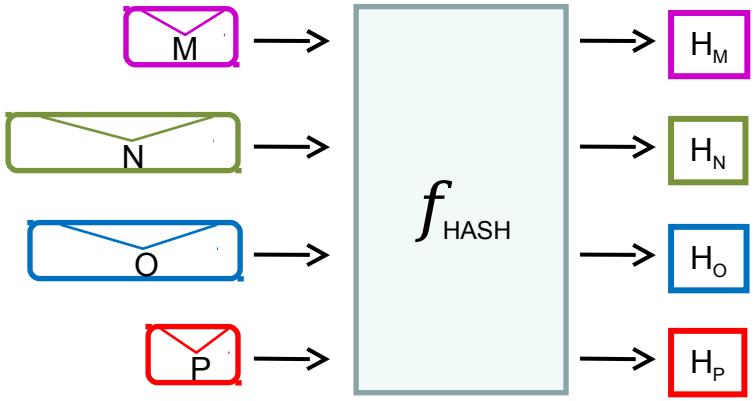
CRYPTOGRAPHY



CISSP®
Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP
diarmuid@obriain.com

History of Cryptography

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Classic Cryptography

- Non-standard hieroglyphs carved into monuments from Egypt
- Clay tablets from Mesopotamia
- Hebrew scholars made use of simple monoalphabetic substitution ciphers beginning perhaps around 500 to 600 BC.

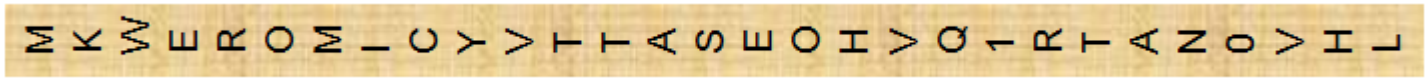
Classic Cryptography – Atbash cipher

- Atbash cipher
  - Simple substitution cipher for the Hebrew alphabet.
  - Reverse the alphabet.
  - Example using the standard English alphabet.

A | B | C | D | E | F | G | H | I | J | K | L | M
Z | Y | X | W | V | U | T | S | R | Q | P | O | N

Classic Cryptography – Scytale cipher

- Greek cipher - Spartan military.
- Scytale (baton) transposition cipher.
- Baton same size on each side.
- Easily broken.



Classic Cryptography – Polybius Square

- Greek cipher.
- Polybius Square or Chequerboard.
- Each letter is then represented by its coordinates in the grid. For example, "CISSP" becomes "13 23 41 41 34".
- Exercise: Encrypt "*Polybius was a greek crypto master*".

	1	2	3	4	5	6	
1	A	B	C	D	E	F	1
2	G	H	I	J	K	L	2
3	M	N	O	P	Q	R	3
4	S	T	U	V	W	X	4
5	Y	Z	0	1	2	3	5
6	4	5	6	7	8	9	6
	1	2	3	4	5	6	

Classic Cryptography – Caesar cipher

- Romans “Caesar’s cipher”
  - Substitution cipher
  - Each letter replaced by a letter some fixed number of positions down the alphabet.
    - Example, with a shift of 3, A would be replaced by D, B would become E, and so on.
    - ROT3 (ROTate 3) as it rotates by 3 places.
  - Exercise: Encrypt the line “Caesar was a Roman Emperor”.

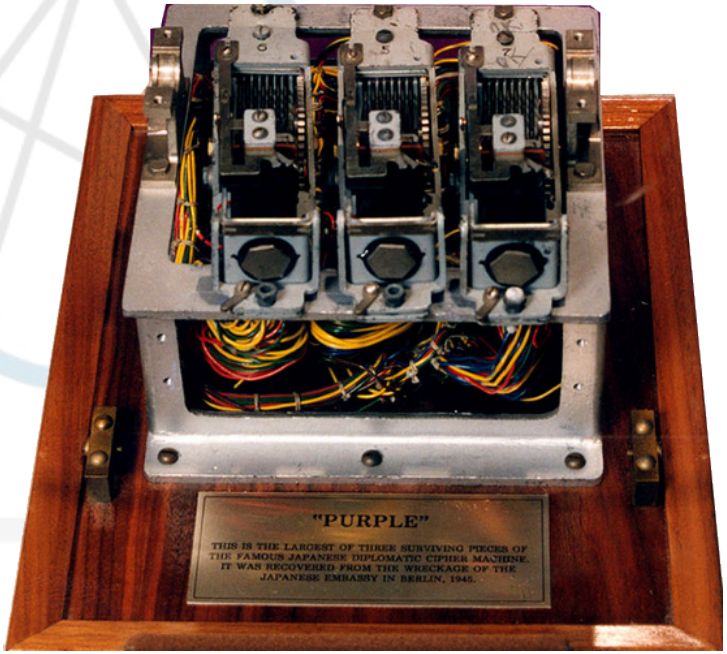
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

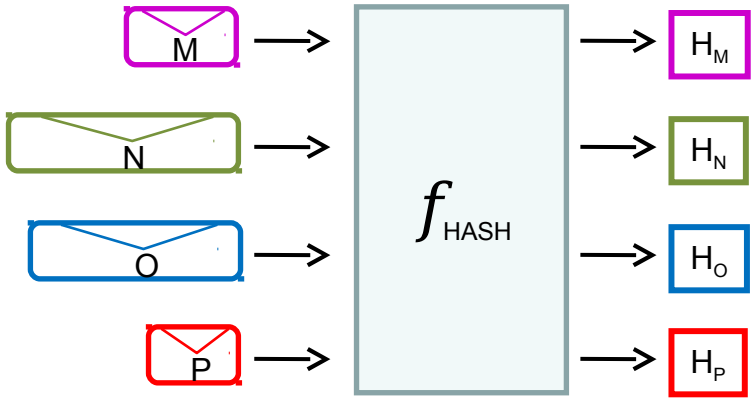
Enigma Machine

- Invented by German engineer Arthur Scherbius at the end of World War I.
- Used by Nazi Germany during World War II.
- Combination of mechanical and electrical subsystems.
  - Stepping components to turn one or more of the rotors with each key press
  - Right-hand rotor steps once with each key stroke, other rotors step occasionally.
    - Continual movement of the rotors results in a different cryptographic substitution after each key press.
- Bletchley Park project ULTRA
  - Decrypt Enigma messages.

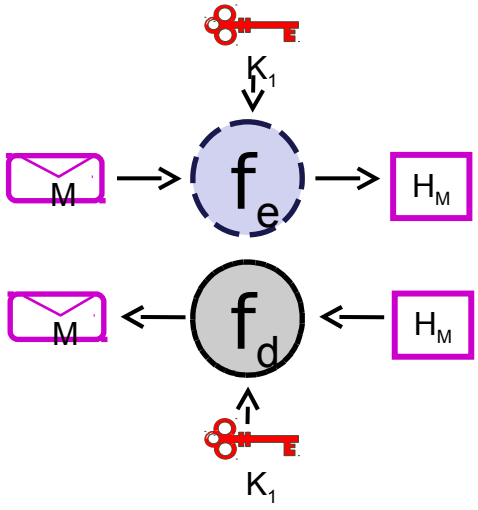
Japanese RED and PURPLE Machines

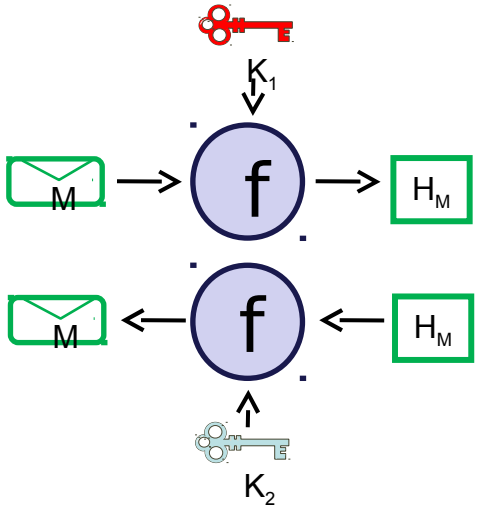
- RED Machine
  - “System 91 Printing Machine” diplomatic cryptographic machine used before and during World War II. (Type A)
  - Simple device, encryption provided through a single half-rotor.
- PURPLE Machine
  - The “System 97 Printing Machine replaced the RED Machine just before and during World War II.
  - Electromechanical stepping-switch device.
  - More secure than RED.
  - Inherited a weak point from the RED machine, namely vowel-consonant separate encryption, which was called "sixes-twenties" by the US Army Signals Intelligence Service (SIS).





Cryptography Principles





Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Goals of Cryptography

- CIA Triad
  - ***C*** onfidentiality
  - ***I*** ntegrity
  - ***A*** uthentication
  - Non-repudiation
    - A goal that is achieved by a combination of integrity and authentication.

Kerckhoffs' principle & Shannon's' maxim

- Auguste Kerckhoffs
  - Paris based Dutch linguist and cryptographer in the 19th century

- "***a cryptosystem should be secure even if everything about the system, except the key, is public knowledge***" Auguste Kerckhoffs

- Claude Shannon
  - American electronic engineer and mathematician

- "***The enemy knows the system***" Claude Shannon

Kerckhoffs' principle

1) The system must be practically, if not mathematically, indecipherable.
2) It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.
3) Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents.
4) It must be applicable to telegraphic correspondence.
5) It must be portable, and its usage and function must not require the concourse of several people.
6) Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

eXclusive OR & Modulo

- eXclusive OR

p	q	$\oplus$
F	F	F
F	T	T
T	F	T
T	T	F

- Modulo
  - Given two numbers, ***a*** (the dividend) and ***n*** (the divisor), a modulo ***n*** is the remainder, on division of ***a*** by ***n***.
  - i.e. "***7 mod 3***“ evaluates to *1*, while "***9 mod 3***" evaluates to *0*.

Other cryptographic terms

- **one-way function**
  - mathematical function that is easy to compute an output for every input but practically impossible to determine the input given the output and the function.

- **trapdoor** one-way function or trapdoor permutation
  - special kind of one-way function. Such a function is hard to invert unless some secret information, called the trapdoor, is known.

- **nonce**
  - Number used ONCE. A random or pseudo-random number issued in a security protocol to ensure that past communications cannot be reused in replay attacks.

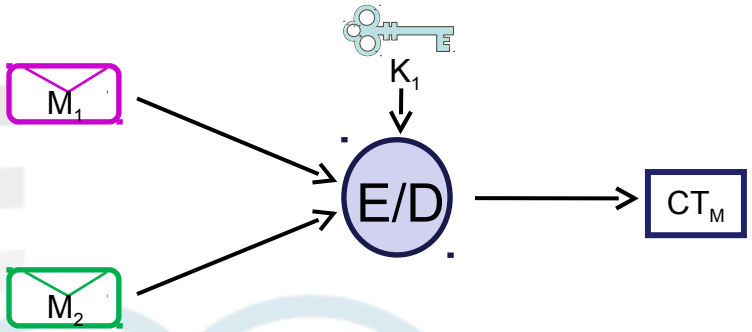
Other cryptographic terms

- **Initialisation Vector** (IV)
  - Block of bits that is required to allow a stream or block cipher to execute any of several streaming modes of operation to produce a unique stream by the same encryption key, without having to go through a re-keying process.

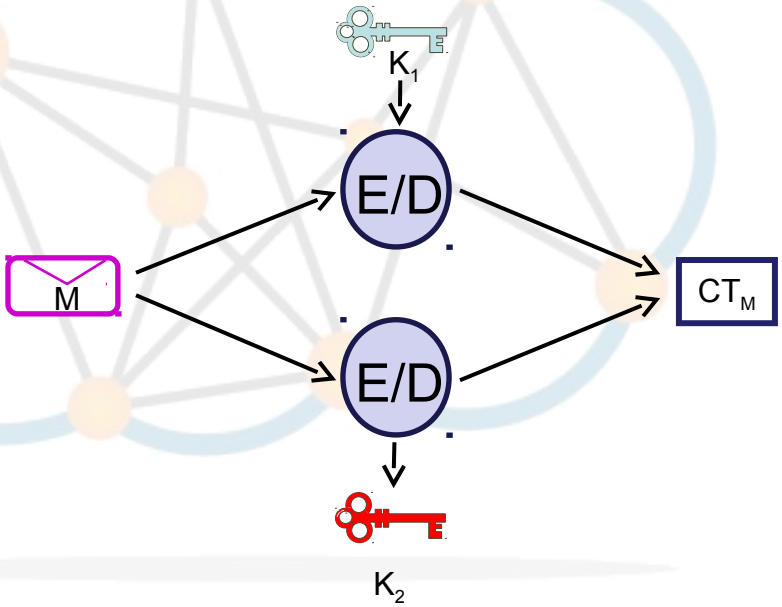
- **Work Factor**
  - Compare the cost of circumventing the mechanism with the resources of a potential attacker. The time or effort required to perform a brute force attack against a cryptosystem.

Other cryptographic terms

- **Collision**



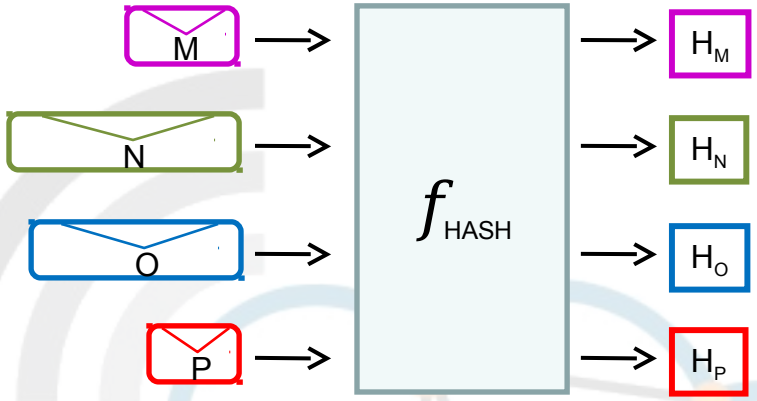
- **Key Clustering**



Other cryptographic terms

- **Codes and Ciphers**
  - A code replaces words, phrases, or sentences with groups of letters or numbers. i.e. the proword "*over*" means "*I have completed my transmission and expect a reply from you*", in this case "*over*" is a code.
  - A cipher rearranges letters or uses substitutes to disguise the message.
- **One-Time Pad (OTP)**
  - The only type of encryption that has been proven to be absolutely impossible to crack if used correctly.
  - The OTP is also known as the **Vernam Cipher** after inventor Gilbert Stanford Vernam.

Hash Function

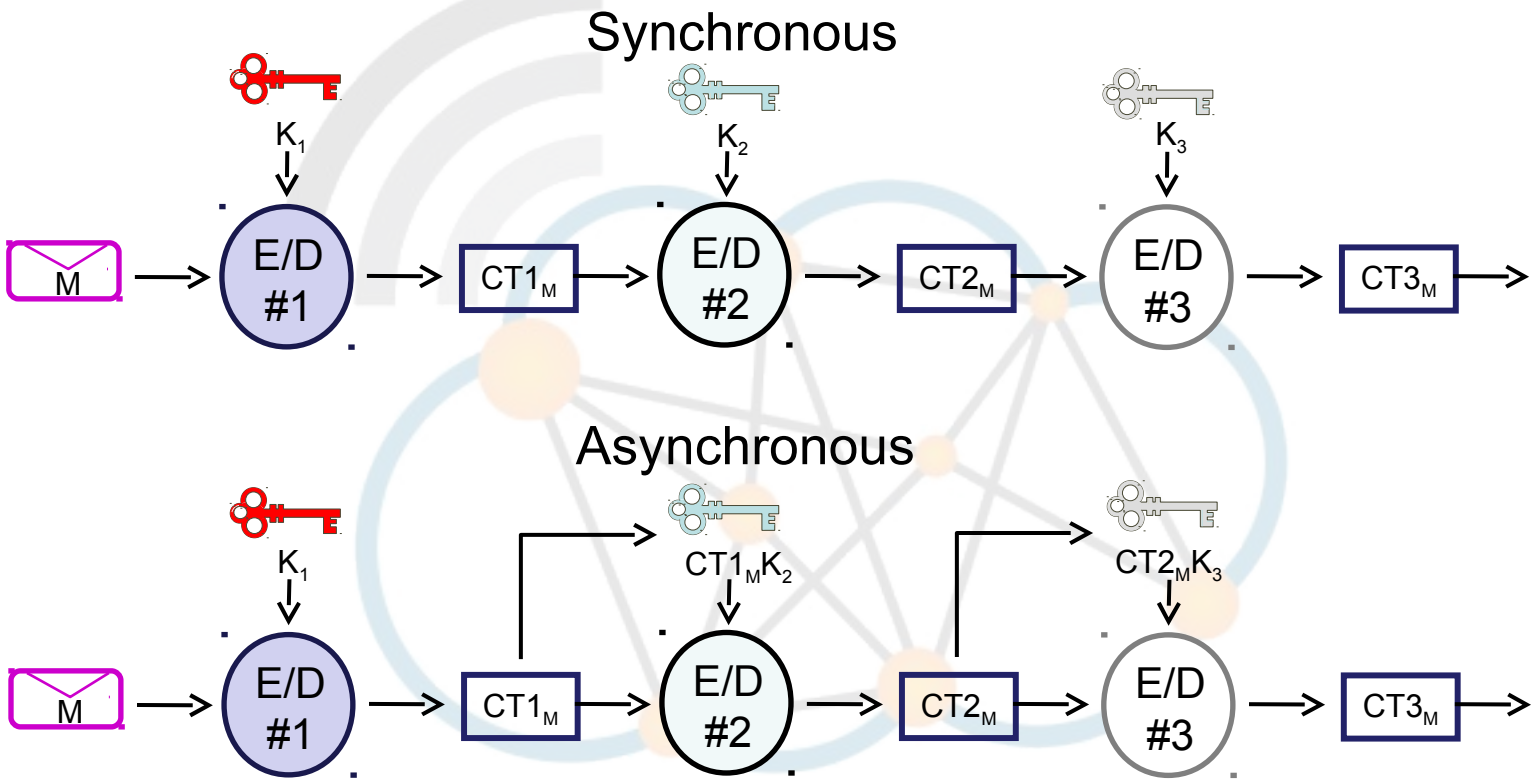


- Mathematical function that converts a large, possibly variable-sized amount of data into a small fixed size message digest (hash) that can:
  - The hash function has four properties:
    - Easy to compute the hash value for any message.
    - Infeasible to find a message that has already a given hash.
    - Infeasible to modify a message without a change to its hash.
    - Infeasible to find two different messages with the same hash.

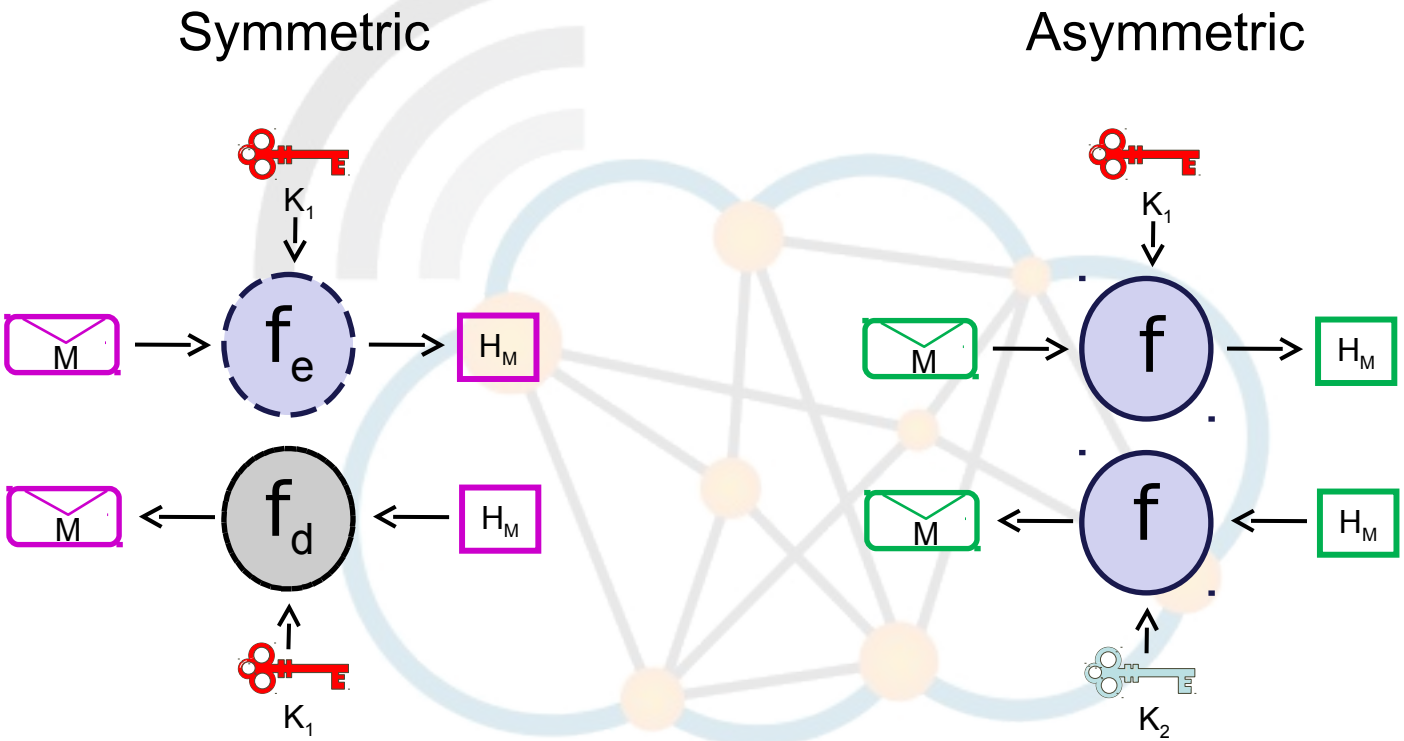
Hash Function

Algorithm	Name	Type	Block Size	Keys	Rounds	Other
SHA-1	Secure Hash Algorithm	Hash	512	160	80	160 bits output - 80 bits protection against collision
SHA-256	Secure Hash Algorithm	Hash	512	256	64	256 bits output - 128 bits protection against collision
SHA-512	Secure Hash Algorithm	Hash	Variable	512	80	512 bits output - 256 bits protection against collision
SHA3-256	Secure Hash Algorithm	Hash	576	1600	24	
SHAKE-128	eXtendable Output function	XOF	1344	1600	24	
SHAKE-256	eXtendable Output function	XOF	1088	1600	24	
MD4	Message-Digest algorithm 4	Hash	Variable	128	3	128 bits output
MD5	Message-Digest algorithm 5	Hash	Variable	128	4 (each round is composed of 16 similar operations)	128 bits output

Synchronous/Asynchronous Cryptosystem



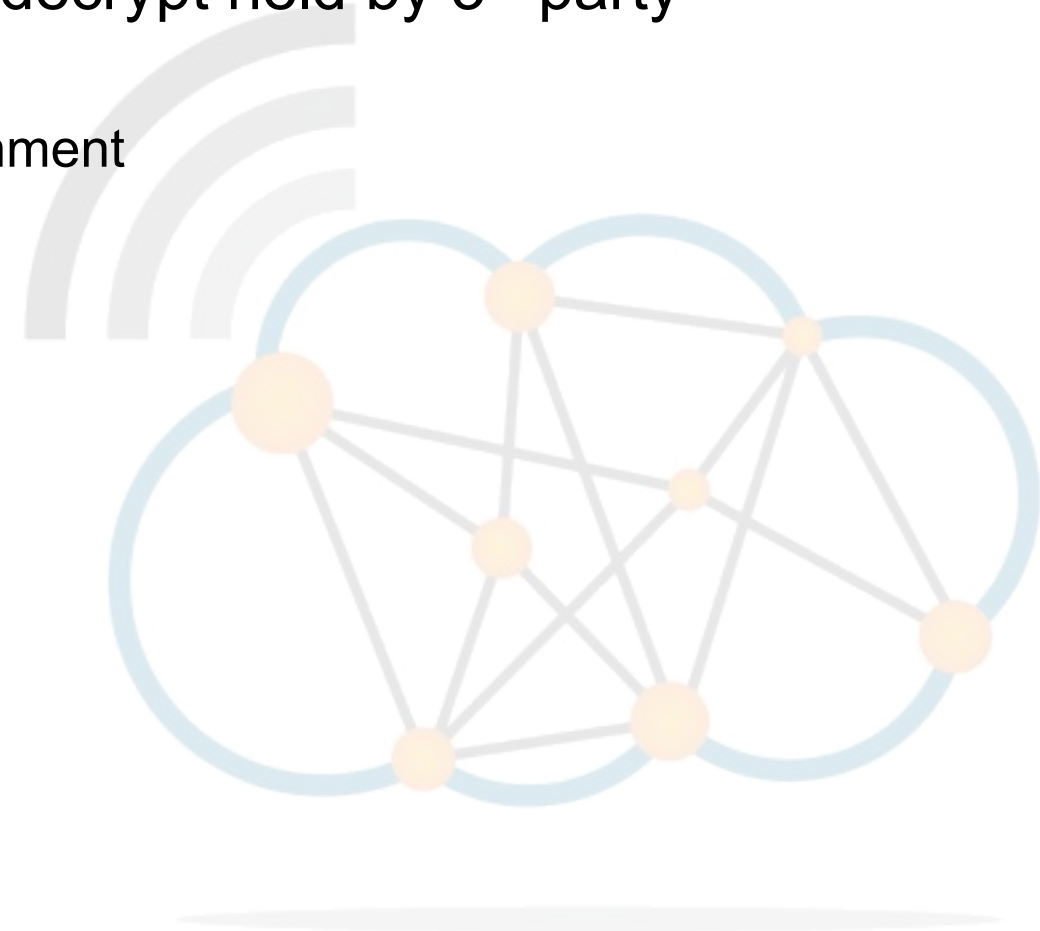
Symmetric/Asymmetric Keys



Symmetric limitation : # of keys required to link n nodes $=[n(n-1)]/2$

Key Escrow

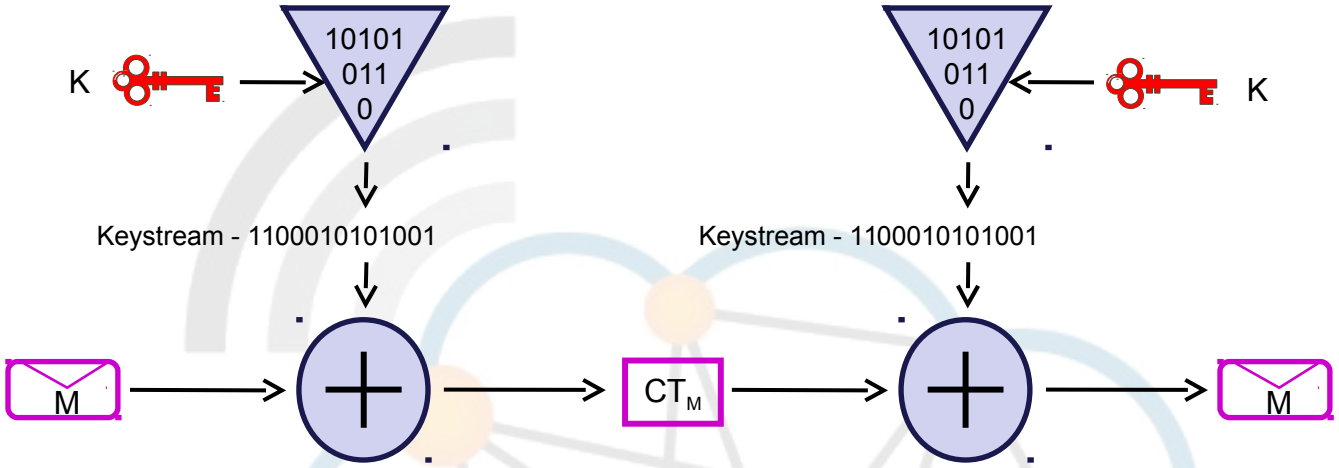
- Keys for decrypt held by 3rd party
  - Banks
  - Government



Stenography

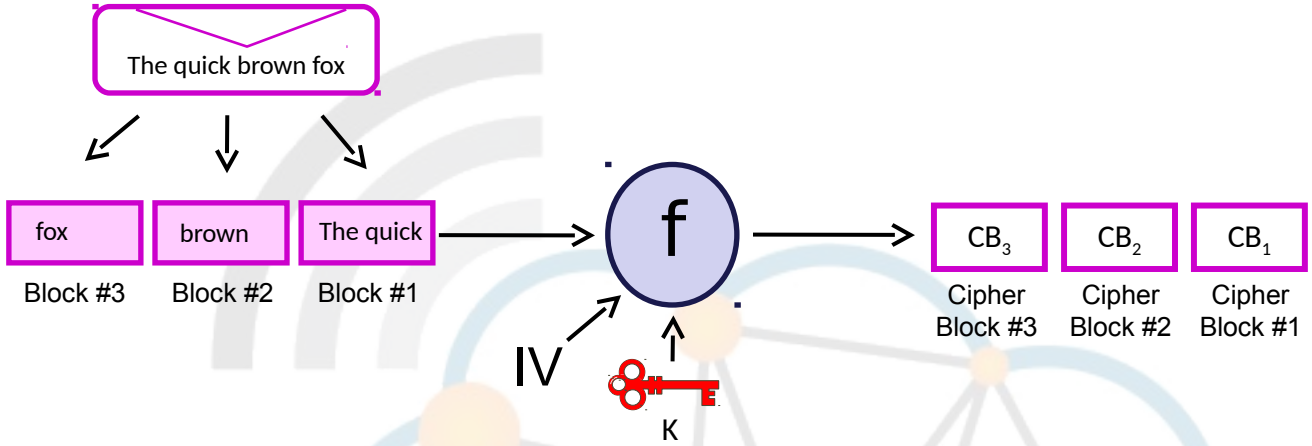
- Data hidden in plain sight

Stream Cipher



- **Rivest Cipher 4 (RC4)**
  - RC4 is a stream cipher designed by Ron Rivest of RSA Security, The Security Division of EMC Corporation in 1987.

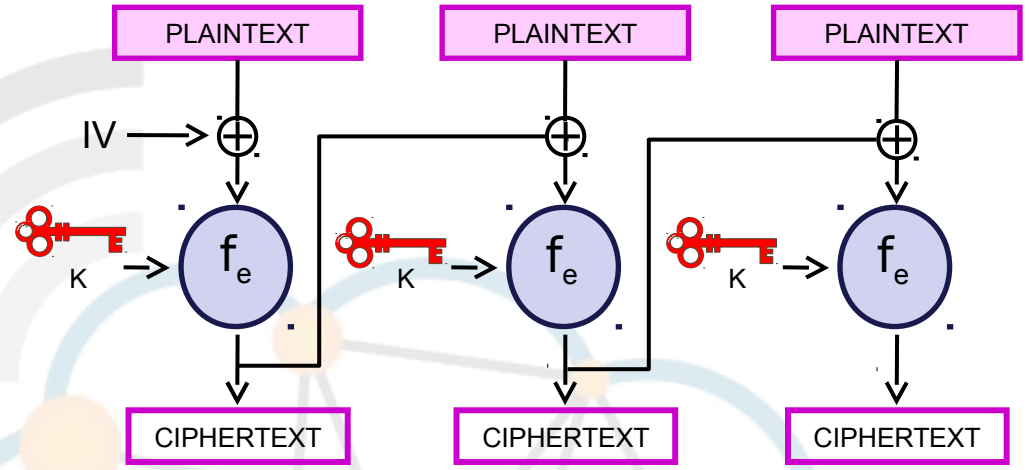
Block Cipher



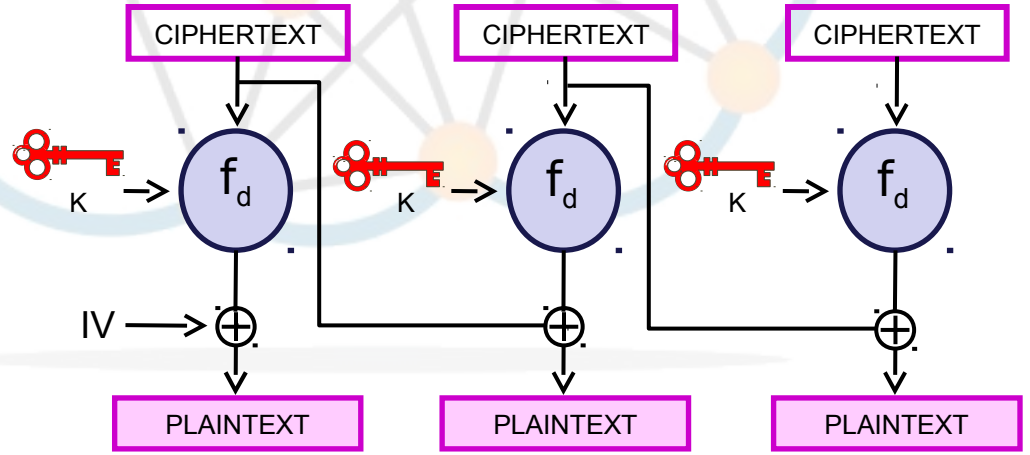
- Block Size
  - DES – 64bits
  - 3DES – 64
  - AES – 128/192/256 bits
- Key Size
  - DES – 64bits
  - 3DES – 168/112/56bit
  - AES - 128bit
- Rounds
  - DES – 16
  - 3DES - 48
  - AES - 10/12/14

Cipher-block chaining (CBC)

- CBC Encryption

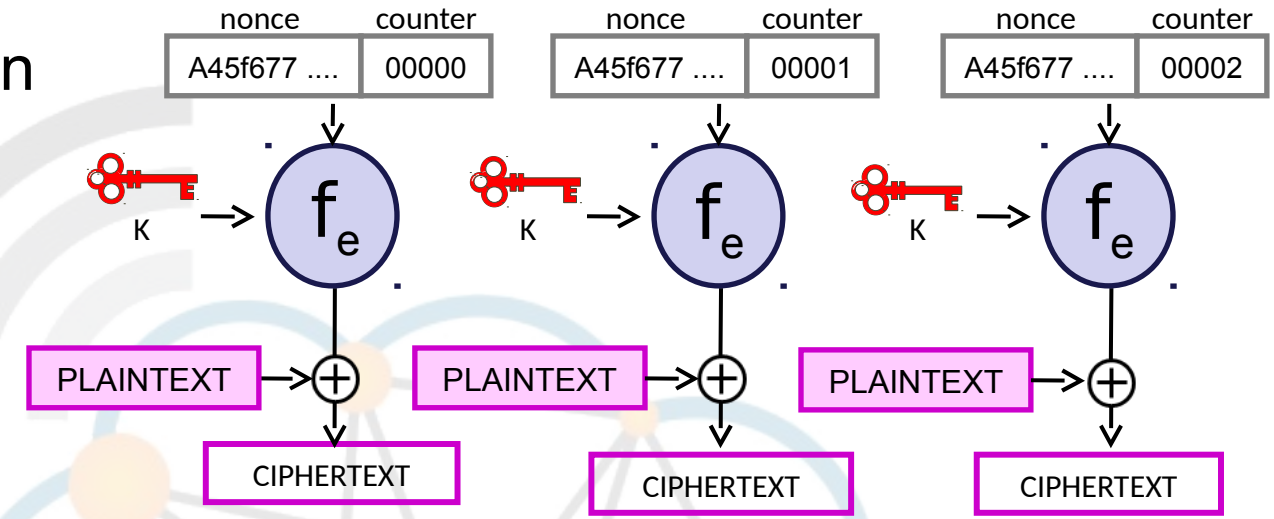


- CBC Decryption

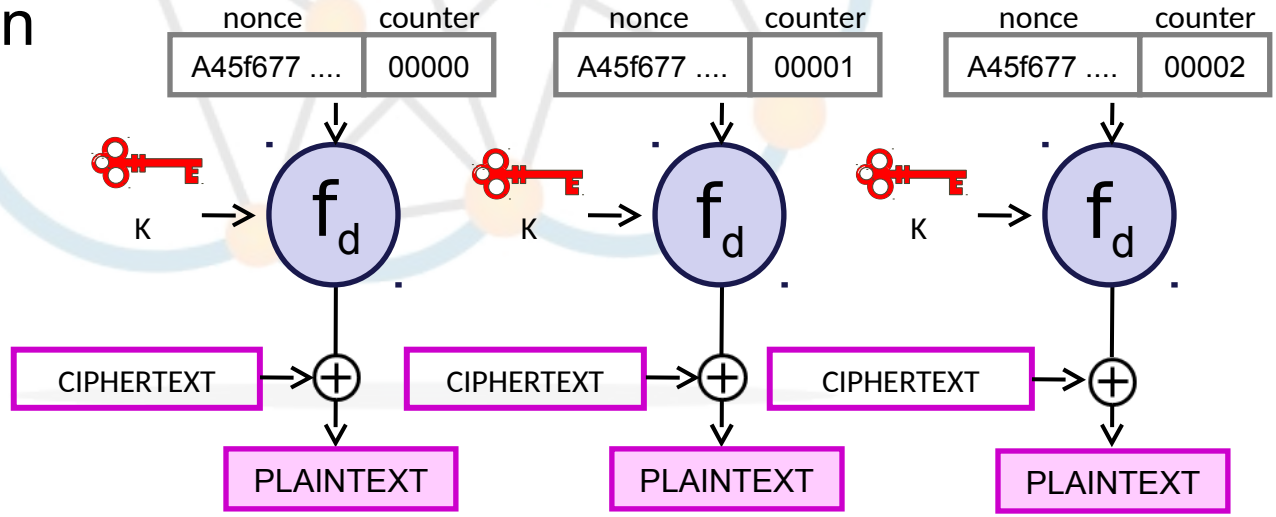


Counter (CTR)

- CTR Encryption



- CTR Decryption



CBC-MAC (CCM)

- Message Authentication Code (MAC)
  - Data block used to authenticate a message.
  - **Authenticity**
    - Confirms that message came from the stated sender.
  - **Integrity**
    - Message has not been changed in transit.
- Cipher Block Chaining - MAC (CBC-MAC).
  - Technique for constructing a MAC from a block cipher.

Counter Mode with CBC-MAC (CCM)

- CCM provides both authentication and privacy.
- Block ciphers with a block length of at least 128 bits.
- Combines CTR mode encryption with CBC-MAC mode of authentication.
- The key insight is that the same encryption key can be used for both.
- CCM is defined for AES only in RFC 3610.
  - CBC-MAC – Authentication
  - CTR – Confidentiality

Data Encryption Standard (DES)

- Block cipher selected as an official standard for the U.S. in 1976 and published it in January 1977.
- Based on a 56 bit symmetric-key algorithm.
- DES is now considered to be insecure.
- **Double DES (DDES)**
  - *ciphertext = Encrypt K_2(Encrypt K_1(plaintext))*
- **Triple DES (TDES)**
  - *ciphertext = Encrypt K_3(Decrypt K_2(Encrypt K_1(plaintext)))*
  - *plaintext = Decrypt K_1(Encrypt K_2(Decrypt K_3(ciphertext)))*
  - Keying options
    - Keying option 1: (Strongest): All three keys are independent
    - Keying option 2: K_1 and K_2 are independent, and $K_3 = K_1$
    - Keying option 3: (No better than DES): $K_1 = K_2 = K_3$.

Advanced Encryption Standard (AES)

- AES has replaced DES, DDES and TDES.
- Rijndael cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen
- Three possible block sizes
  - AES-128, AES-192 and AES-256,
  - Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively.
- AES also became the first publicly accessible and open cipher approved by the NSA for top secret information.

Rivest Cipher 5 (RC5)

- Rivest Cipher 5 (RC5)
  - Block cipher designed by Ronald Rivest in 1994 and patented by RSA, The Security Division of EMC Corporation.
  - It is notable for its simplicity.
  - It has a variable block size (32, 64 or 128 bits), key size (0 to 2040 bits) and number of rounds (0 to 255).
  - The original suggested choices of parameters were a block size of 64 bits, a 128-bit key and 12 rounds.

RSA
The Security Division of EMC

Rivest Ciphers 6 (RC6)

- Rivest Cipher 6 (RC6)
  - Symmetric key block cipher derived from RC5.
  - Designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin for the AES competition and was one of the five finalists.
  - It has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits, but, like RC5, it can be parametrised to support a wide variety of word-lengths, key sizes and number of rounds.

RSA
The Security Division of EMC

Other ciphers

- **Blowfish** was designed as a replacement for DES and it later variant **Twofish** was submitted for the AES competition. It is included in the OpenPGP standard (RFC 4880).
- Secure And Fast Encryption Routine (**SAFER**), **SAFER+** and **SAFER++** versions were submitted as candidates to the AES competition and are unpatented and available for open use.
- **CAST** is a family of block ciphers documented in RFC 2144 and RFC 2612. They are royalty and licence free basis for commercial and non-commercial use.
- **Serpent** is a symmetric key block cipher which was a finalist in the AES contest, where it came second to Rijndael. It is a free to use unpatented public domain cipher.

Asymmetric Key Cryptography

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Asymmetric/Public Key Cryptography (PKI)

- Uses Asymmetric key algorithms instead of or in addition to symmetric key algorithms.
- Unlike symmetric does not require a secure initial exchange of one or more secret keys to both sender and receiver.
- A mathematically related key pair is created, a secret private key and a public key the latter which is published.
- These keys allow protection of the **authenticity** of a message by creating a digital signature of a message using the private key, which can be validated using the public key.
- It also allows for the protection of the messages **confidentiality** and **integrity**, by public key encryption, encrypting the message using the public key, which can only be decrypted using the private key.
- Public key cryptography is employed by many cryptographic algorithms and cryptosystems.
- It is used in standards such as TLS/SSL, PGP, and GnuPG.

Key pairs

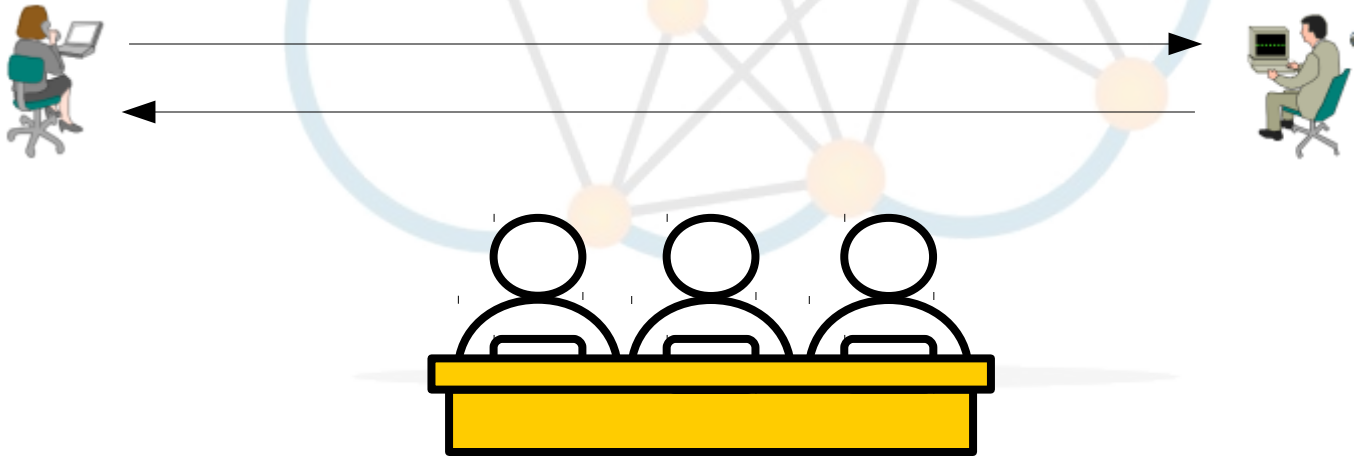
- The generation of key pairs requires the use of intractable problems called trapdoor functions which are functions that are easy to compute in one direction, yet believed to be difficult to compute in the opposite direction without special information, called the **trapdoor**.
- An intractable problem is a problem for which there is no efficient means of solving.
- The public key cryptographic intractable problems used to date are based either on factoring prime numbers or discrete logarithms.

Example, discrete logarithm problem

- Take a prime number $m = 29$ as the modulus (public key).
- Primitive roots of 29 are: 2, 3, 8, ***10,*** 11, 14, 15, 18, 19, 21, 26, 27.
- So taking as a base $b = 10$ (the trapdoor)
- Alice chooses a secret $y = 8$ (Private Key).
- Alice sends Bob $w = b^y \bmod m = 10^8 \bmod 29 = 25$
- Bob chooses a secret $z = 11$ (Private Key).
- Bob sends Alice $x = b^z \bmod m = 10^{11} \bmod 29 = 2$
- Alice computes $s = x^y \bmod m = 2^8 \bmod 29 = 24$
- Bob computes $s = w^z \bmod m = 25^{11} \bmod 29 = 24$
- Alice and Bob now share a secret, in this case 24 without it being transferred across the transmission path and without either Alice or Bob sharing their private keys.

Discrete logarithm problem

- Group Exercise
  - Public key = 41.
  - Trapdoor = 7.
  - Demonstrate how Fred and Wilma can communicate a shared value without transferring it over the system using the discrete logarithm problem.



Example, discrete logarithm problem

- The trapdoor can remain small but the public and private keys are typically over 300 digits.

- For example:

4305 0241 20D9 18FA DF8D EC2D EFD5 FD35 89C9 E069
EA95 FD20 5E35 F3B5 ED31 D4FC D6E4 4811 5D86 CD8F
CAFA 362F 922C F01C 2F40 D544 2654 D0D2 2881 D653
DA2C 4203 D266 E2D2 DC02 0301 2001

Key exchange protocols

- **Diffie-Hellman key protocol**
  - In 1976 Whitfield Diffie and Martin Hellman, who, influenced by Ralph Merkle's work on public-key distribution went down the discrete log route when developing what became known as Diffie-Hellman key exchange method.
- **El Gamal**
  - El Gamal is based on Diffie-Hellman method. It was described by Taher Elgamal in 1985.
  - It is used in the free GNU Privacy Guard software, recent versions of PGP, and other crypto-systems.

RSA

- In 1977 Ronald Rivest, Adi Shamir and Len Adleman developed an algorithm using factoring of prime numbers, known as RSA.
- Taking two large prime numbers we will call ‘B’ and ‘Q’. Multiply these numbers to generate ‘N’:
  - $N = B * Q$
- Select another number ‘*e*’ such that:
  - $e < N$
  - e and $(N - 1)(Q - 1)$ are relatively prime (no common factors except 1)
- Find a number ‘*p*’ such that:
  - $(ep - 1) \bmod (B - 1)(Q - 1) = 0$
- Distribute ‘*e*’ and ‘*N*’ as the public key and keep ‘*p*’ as the private key.
- For Alice to send an encrypted message she sends:
  - $\{CT\} = \{PT\}^e \bmod N$
- Bob receives and retrieves the message by:
  - $\{PT\} = \{CT\}^p \bmod N$

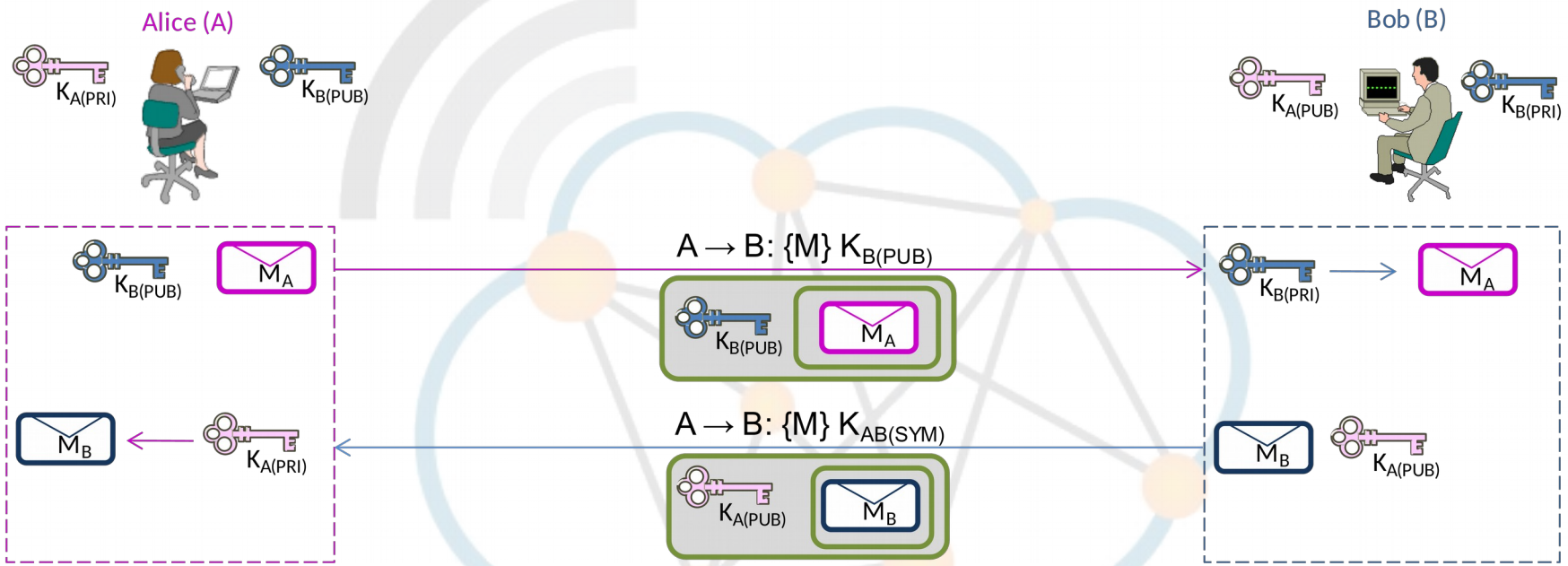
Elliptic curve cryptography (ECC)

- Another intractable problem that is used is the assumption that finding the discrete logarithm of an elliptic curve element is infeasible.
- The size of the elliptic curve determines the difficulty of the problem.
- It is believed that a smaller group can be used to obtain the same level of security as RSA-based systems.
- Using a small group reduces storage and transmission requirements.

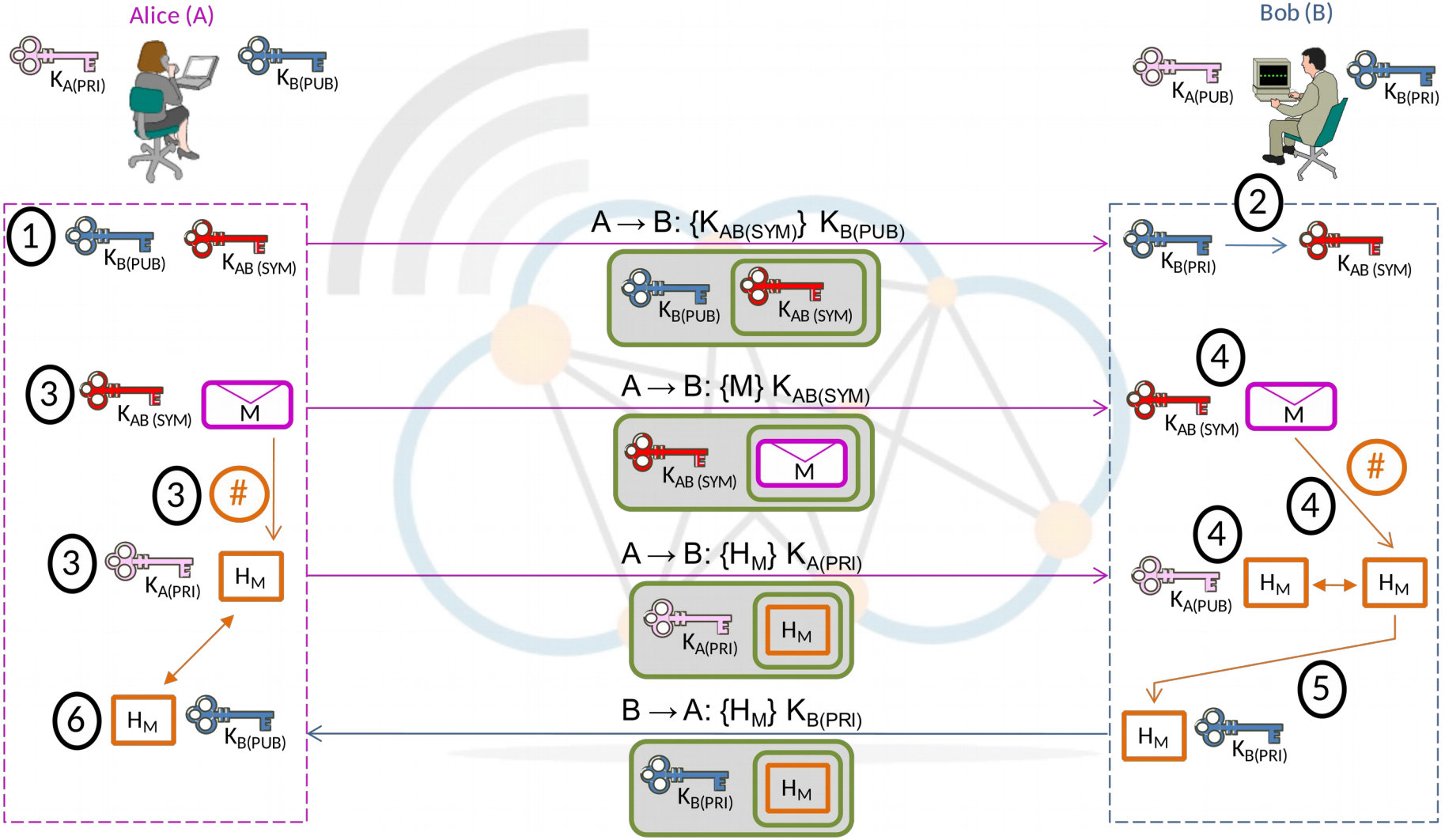
Asymmetric Key Protocol summary

Algorithm	Name	Mode	Block size	Keys	Other
RSA	Ron Rivest, Adi Shamir & Len Adleman	Factoring	Variable	1024 – 2048	
Diffie Hellamn	Whitfield Diffie & Martin Hellman	Discrete Log	Variable	Variable	Only used for key exchange
ECC	Elliptical Curve Cryptography	Discrete Log	Variable	80 → 512	160 bits key is equivalent to 1024 bits in RSA

Asymmetric Key Cryptography



The hybrid system



Key management

How to make the public keys available. For this we need a Public Key Infrastructure (PKI). This is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

VeriSign Entrust

- Certificate Authorities (CA)
  - CAs are web sites that publish the key bound to a given user.
  - This is achieved using the CA's own key, so that trust in the user key relies on one's trust in the validity of the CA's key.
  - The mechanism that binds keys to users is called the Registration Authority (RA), which might or might not be separate from the CA.
  - The key-user binding are established, depending on the level of assurance the binding has, by software or under human supervision.
  - The term trusted third party (TTP) may also be used for certificate authority (CA). Moreover, PKI is itself often used as a synonym for a CA implementation.
  - The ITU-T standard for Certificate Authority is included within the X.509 system.

Key management

- Web of Trust
  - An alternative approach to the problem of public authentication of public key information is the web of trust scheme, which uses self-signed certificates and third party attestations of those certificates.
  - PGP and GnuPG are examples of implementations of the web of trust model.
  - They allow the use of e-mail digital signatures for self-publication of public key information.
  - It is relatively easy to implement one's own Web of Trust.

Implementations

- **Privacy Enhanced Mail (PEM)**
  - PEM was an early IETF proposal for securing email using public key cryptography
  - It has never seen wide deployment as it depended on prior deployment of a hierarchical public key infrastructure (PKI) with a single root which would prove costly and was seen as not a good idea to impose central authority to e-mail.
- **Pretty Good Privacy (PGP)**
  - PGP is used for signing, encrypting and decrypting e-mails to increase the security of e-mail communications
  - PGP follows the OpenPGP standard (RFC 4880) for encrypting and decrypting data
  - The first version of this system was a web of trust, however current versions of PGP encryption include both web of trust and certificate authority options through an automated key management server
  - GnuPG is the GNU project's complete and free implementation of the OpenPGP standard.
- **Secure/Multipurpose Internet Mail Extensions (S/MIME)**
  - MIME is the standard that extends the format of e-mail to support:
  - Text in character sets other than ASCII
  - Non-text attachments
  - Message bodies with multiple parts
  - Header information in non-ASCII character sets
  - S/MIME is a standard for adding cryptographic signature and encryption services to MIME data.

Thank you

Class Test next week

A class test will be given out next class covering all the material in Lecture sets 1, 2 and 3.