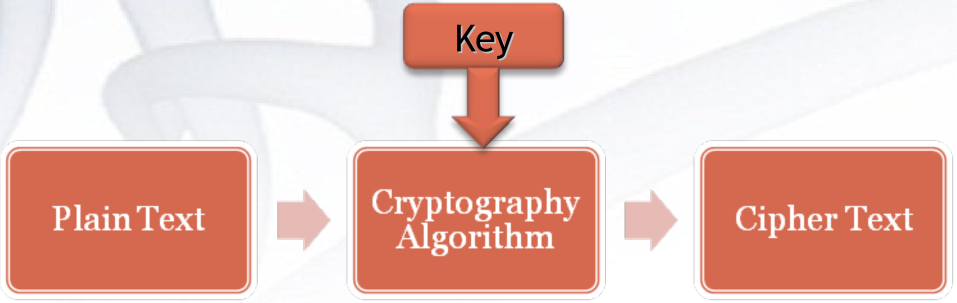
Lecture five

Cryptography

© **Dr. M. Mahfuzul Islam**
Professor, Dept. of CSE, BUET

Cryptography

Encryption

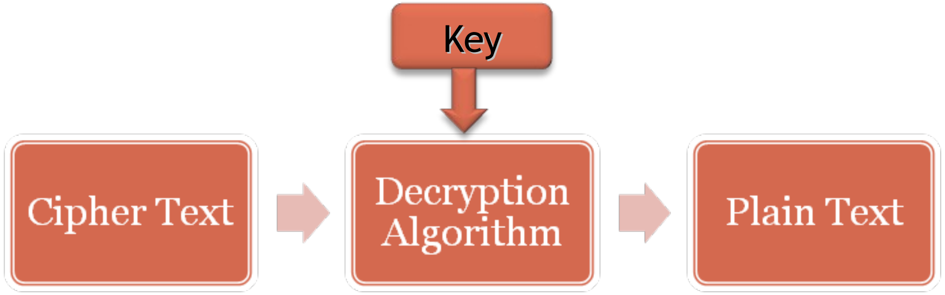

Key

Plain Text

Cryptography Algorithm

Cipher Text

Decryption


Key

Cipher Text

Decryption Algorithm

Plain Text

Objectives of Cryptography

✓ Integrity

✓ Authentication

✓ Confidentiality

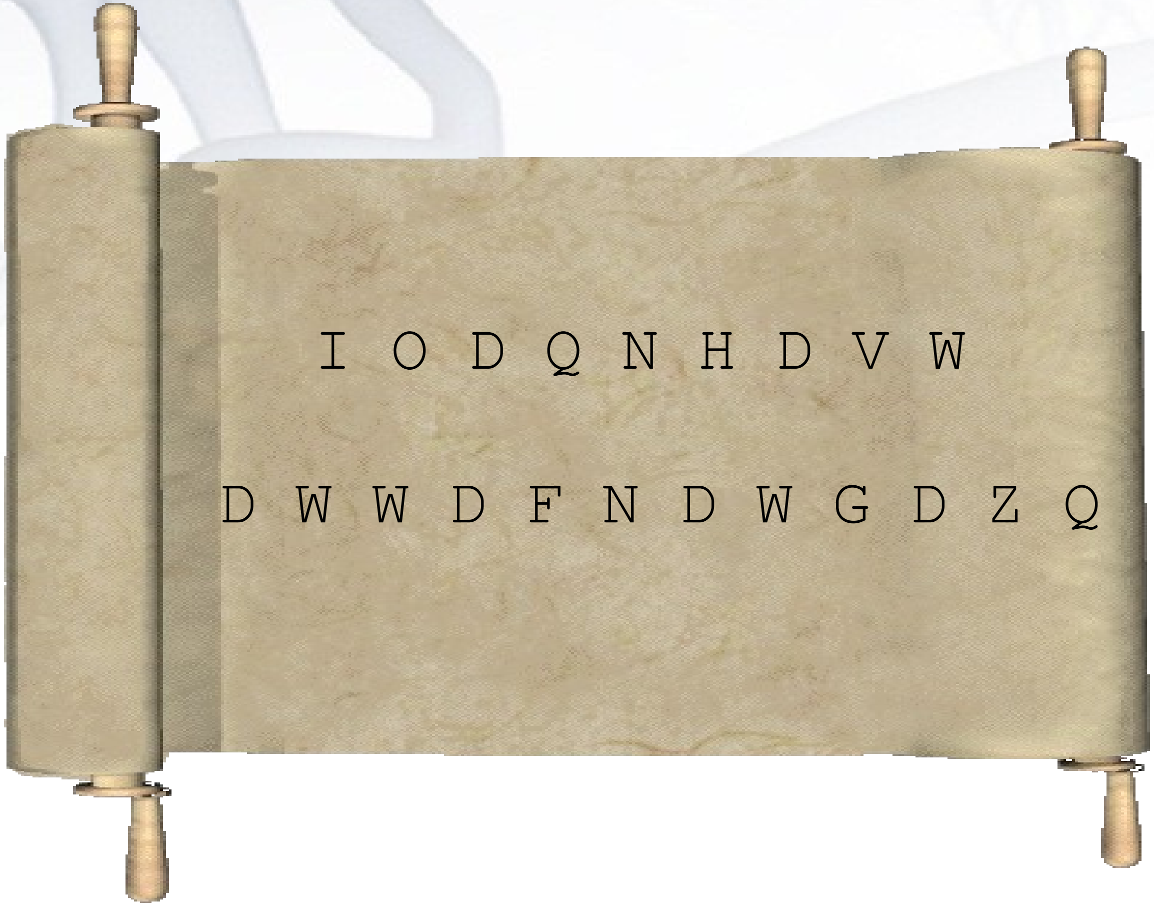
Integrity

- An unbroken wax seal on an envelop ensures integrity.
- The unique unbroken seal ensures no one has read the contents.

Authentication

- An ATM Personal Information Number (PIN) is required for authentication.
- The PIN is a shared secret between a bank account holder and the financial institution.

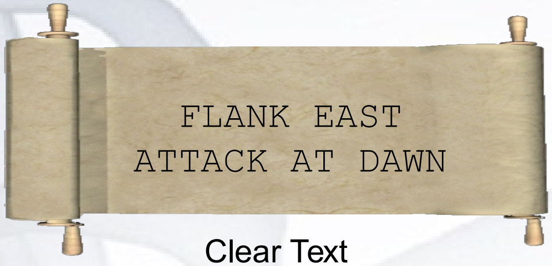
Confidentiality



- Julius Caesar would send encrypted messages to his generals in the battlefield.
- Even if intercepted, his enemies usually could not read, let alone decipher, the messages.

Transposition Ciphers

1

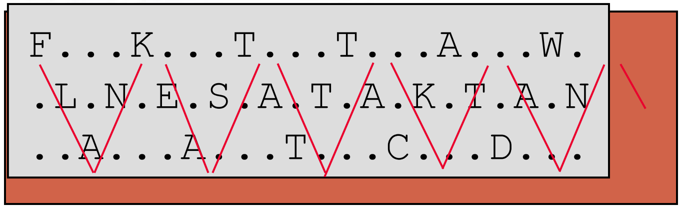


FLANK EAST
ATTACK AT DAWN

Clear Text

The clear text message would be encoded using a key of 3.

2



```
F...K...T...T...A...W.
.L.N.E.S.A.T.A.K.T.A.N
..A...A...T...C...D...
```

Use a rail fence cipher and a key of 3.

3

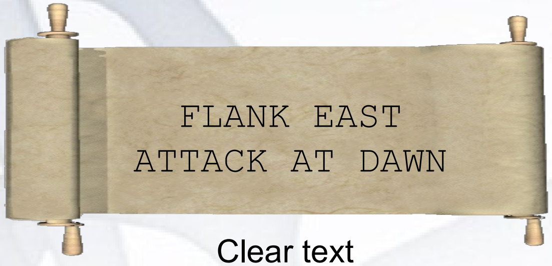
FKTTAW
LNESATAKTAN
AATCD

Ciphered Text

The clear text message would appear as follows.

Substitution Ciphers: Caesar Cipher

1

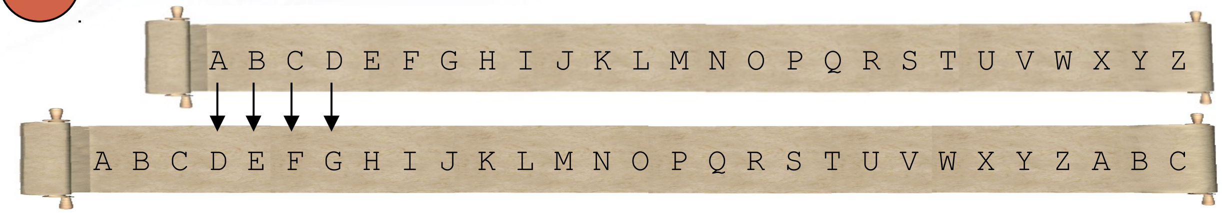


FLANK EAST
ATTACK AT DAWN

Clear text

The clear text message would be encoded using a key of 3.

2

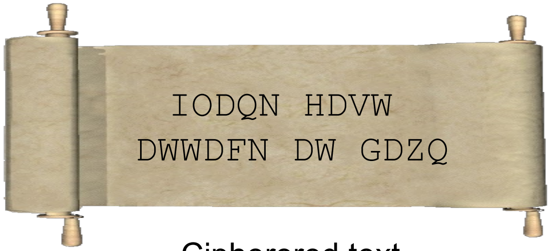


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

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 A B C

Shift the top scroll over by three characters (key of 3), an A becomes D, B becomes E, and so on.

3



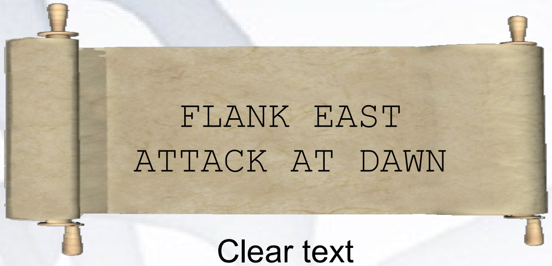
IODQN HDVW
DWWDFN DW GDZQ

Ciphered text

The clear text message would be encrypted as follows using a key of 3.

Cipher Wheel

1

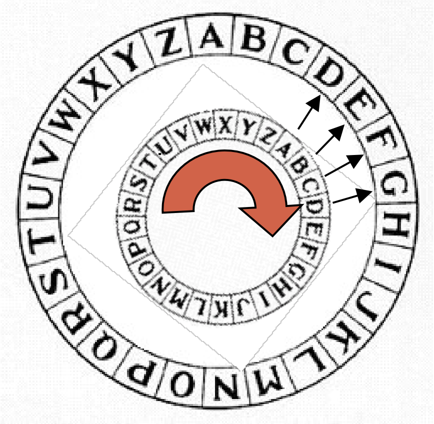


FLANK EAST
ATTACK AT DAWN

Clear text

The clear text message would be encoded using a key of 3.

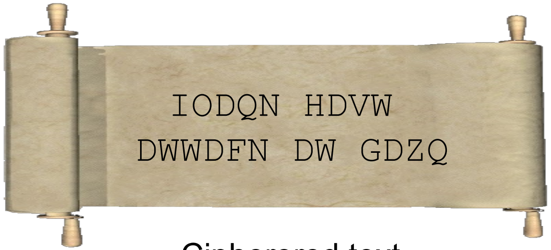
2



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
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

Shifting the inner wheel by 3, then the A becomes D, B becomes E, and so on.

3



IODQN HDVW
DWWDFN DW GDZQ

Ciphered text

The clear text message would appear as follows using a key of 3.

Vigenère Table

	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
A	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
B	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	a
C	c	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
D	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
E	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	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	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

Stream Ciphers

- Invented by the Norwegian Army Signal Corps in 1950, the ETCRRM machine uses the Vernam stream cipher method.
- It was used by the US and Russian governments to exchange information.
- Plain text message is eXclusively OR'ed with a key tape containing a random stream of data of the same length to generate the ciphertext.
- Once a message was enciphered the key tape was destroyed.
- At the receiving end, the process was reversed using an identical key tape to decode the message.

Defining Cryptanalysis

VICTORY EXTRA!

Allies decipher secret NAZI encryption code!

CITY EDITION EXTRA

The Seattle Daily Times

TERMS SIGNED 5:41 SUNDAY, SEATTLE TIME

U. S. PLANES BAG 52 MORE JAP VESSELS

Tanks, Russ Bearing Down On Prague As Nazis Resist

GREATEST OF ALL WARS IN EUROPE ENDS

BULLETINS

SURRENDER TOLD PEOPLE OF GERMANY

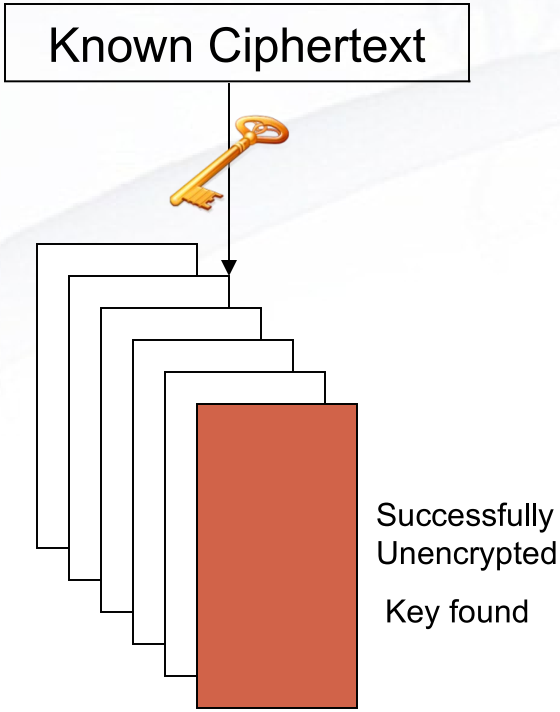
REIMS, France, May 7.—Germany surrendered unconditionally to the Western Allies and Russia at 2:41 a.m., French time, today (5:41 p.m., Sunday, Seattle time).

Cryptanalysis is from the Greek words kryptós (hidden), and analýein (to loosen or to untie). It is the practice and the study of determining the meaning of encrypted information (cracking the code), without access to the shared secret key.

Some Cryptanalysis Methods:

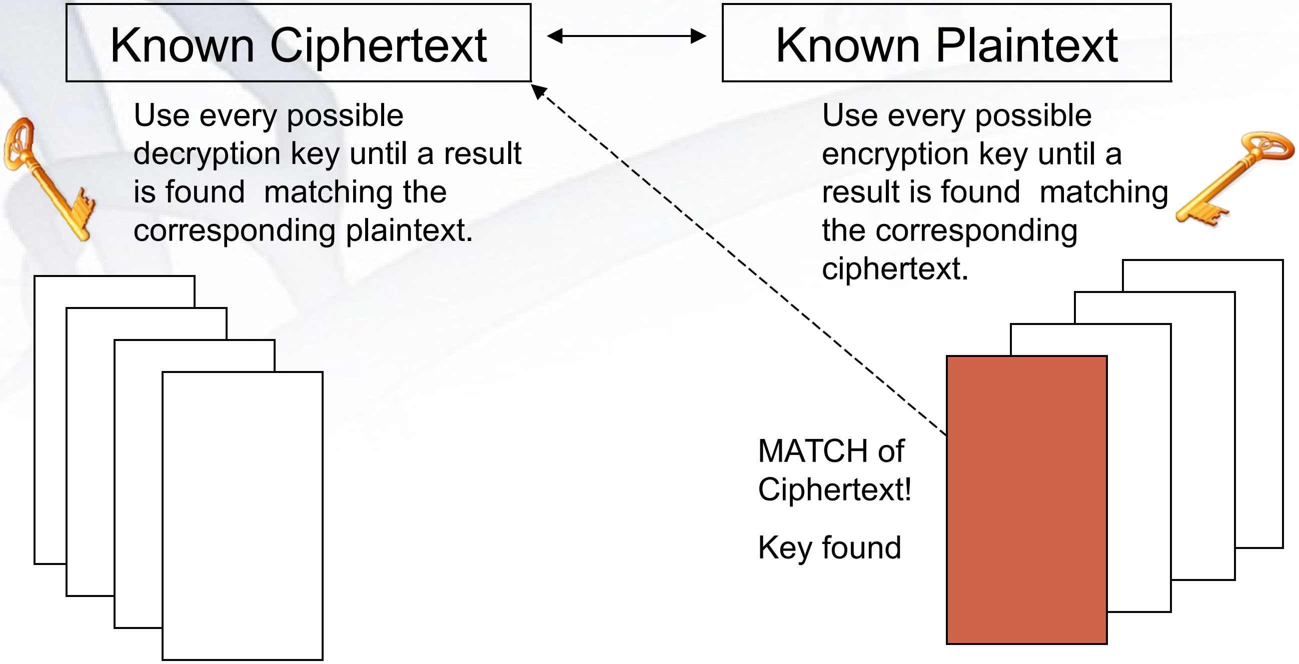
- Brute Force Attack
- Meet-in-the-Middle Attack

Brute Force Attack



With a Brute Force attack, the attacker has some portion of ciphertext. The attacker attempts to unencrypt the ciphertext with all possible keys.

Meet-in-the-Middle Attack



Known Ciphertext

Known Plaintext

Use every possible decryption key until a result is found matching the corresponding plaintext.

Use every possible encryption key until a result is found matching the corresponding ciphertext.

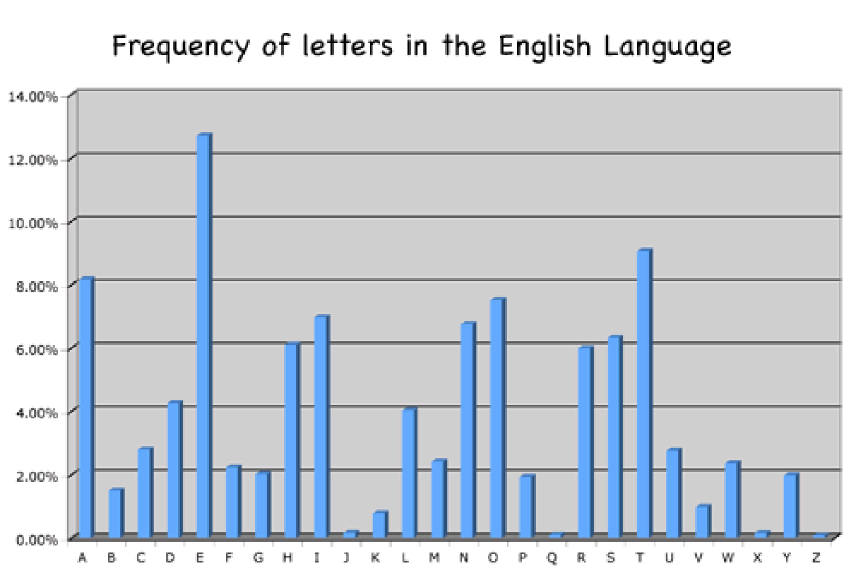
MATCH of Ciphertext!

Key found

With a Meet-in-the-Middle attack, the attacker has some portion of text in both plaintext and ciphertext. The attacker attempts to unencrypt the ciphertext with all possible keys while at the same time encrypt the plaintext with another set of possible keys until one match is found.

Choosing a Cryptanalysis Method

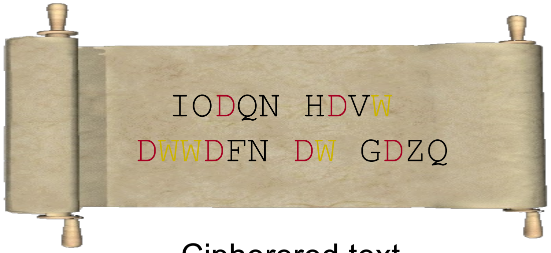
1



The graph outlines the frequency of letters in the English language.

For example, the letters E, T and A are the most popular.

2



IODQN HDVW
DWWDFN DW GDZQ

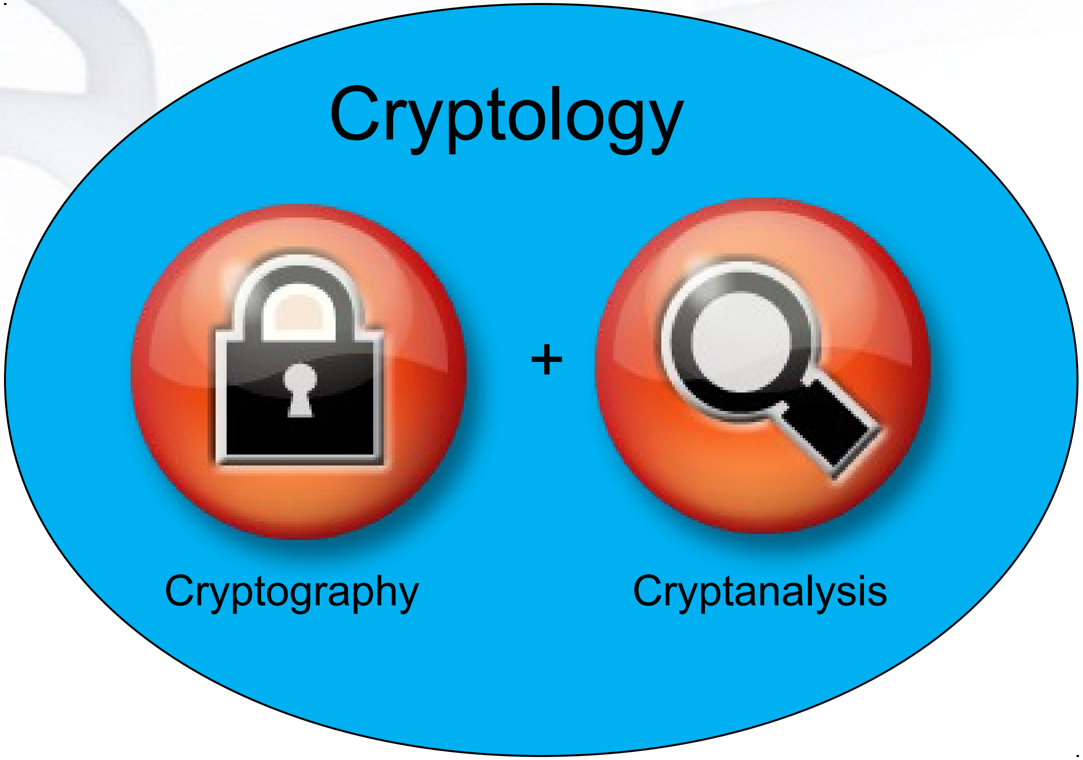
Cipherered text

There are 6 occurrences of the cipher letter D and 4 occurrences of the cipher letter W.

Replace the cipher letter D first with popular clear text letters including E, T, and finally A.

Trying A would reveal the shift pattern of 3.

Defining Cryptology



Cryptology

Cryptography + Cryptanalysis

Cryptographic Hashes, Protocols and Algorithms

Integrity	Authentication	Confidentiality
MD5 SHA	HMAC-MD5 HMAC-SHA-1 RSA and DSA	DES 3DES AES SEAL RC (RC2, RC4, RC5, and RC6)

HASH

HASH w/Key

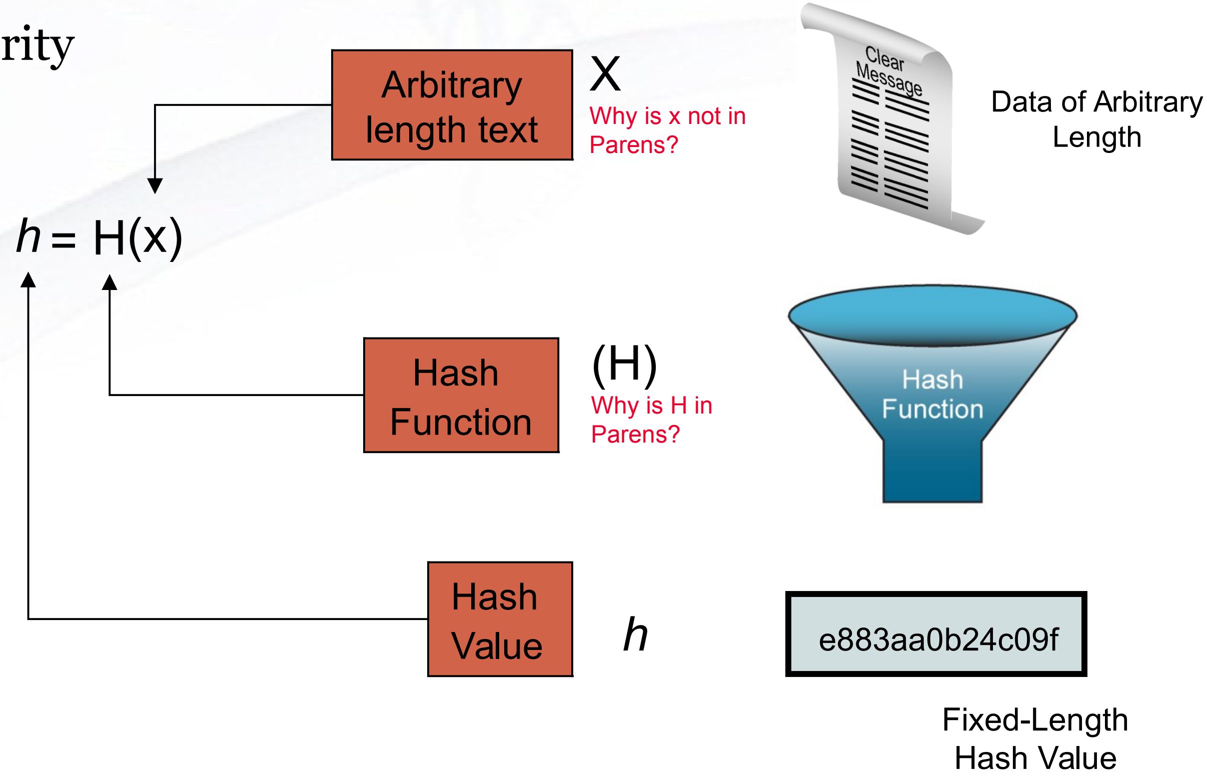
NIST

Rivest

Encryption

Hashing

- Hashes are used for integrity assurance.
- Hashes are based on one-way functions.



Arbitrary length text

X

Why is x not in Parens?

Data of Arbitrary Length

$h = H(x)$

Hash Function

(H)

Why is H in Parens?

Hash Value

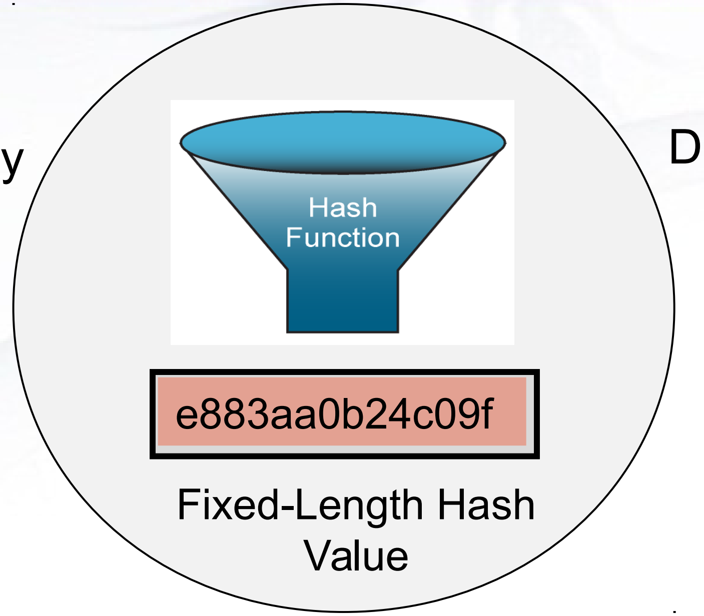
h

e883aa0b24c09f

Fixed-Length Hash Value

The hash function hashes arbitrary data into a fixed-length digest known as the hash value, message digest, digest, or fingerprint.

Using Hashing



Data Integrity

Data Authenticity

e883aa0b24c09f

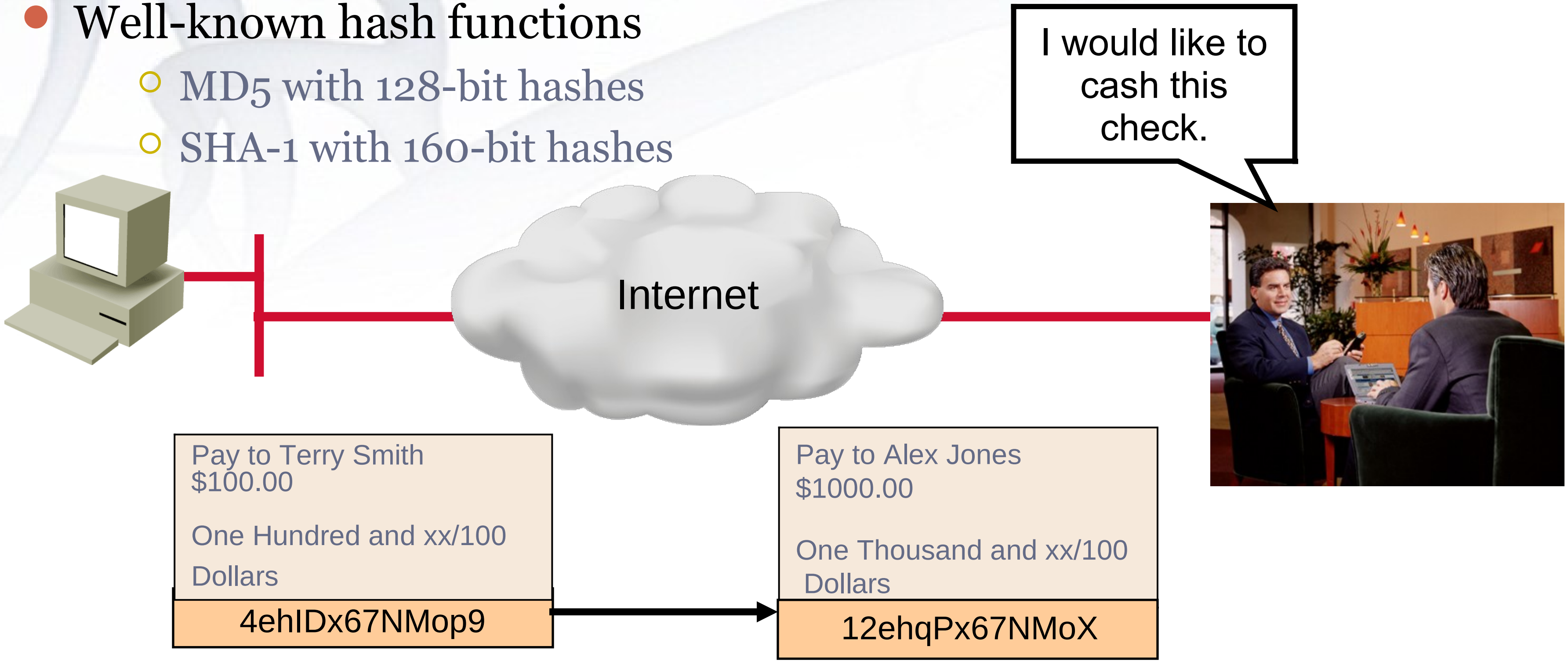
Fixed-Length Hash Value

Entity Authentication

- Routers use hashing with secret keys
- Ipsec gateways and clients use hashing algorithms
- Software images downloaded from the website have checksums
- Sessions can be encrypted

Hashing in Action

- Vulnerable to man-in-the-middle attacks
  - Hashing does not provide security to transmission.
- Well-known hash functions
  - MD5 with 128-bit hashes
  - SHA-1 with 160-bit hashes



I would like to cash this check.

Pay to Terry Smith
$100.00

One Hundred and xx/100 Dollars

4ehIDx67NMop9

Pay to Alex Jones
$1000.00

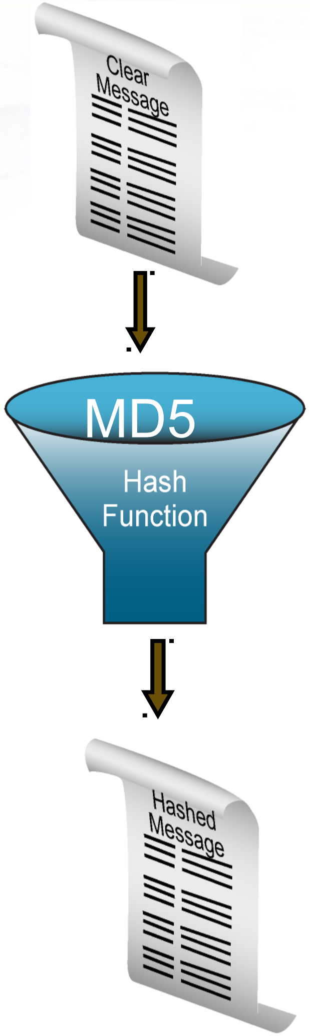
One Thousand and xx/100 Dollars

12ehqPx67NMoX

Match = No changes
No match = Alterations

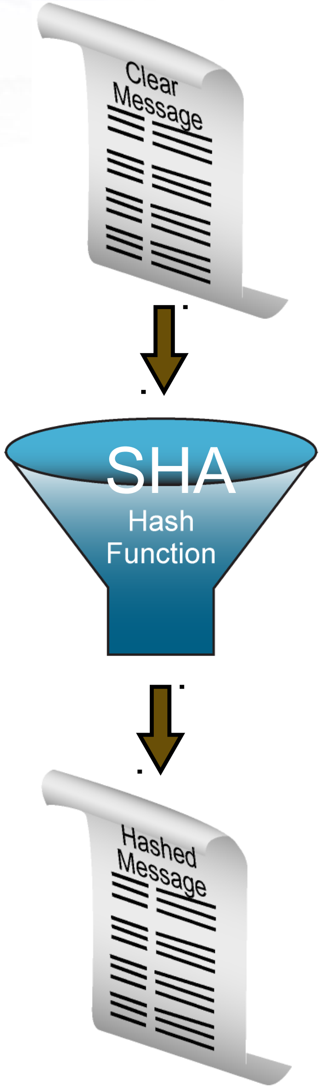
MD5

- MD5 is a ubiquitous hashing algorithm
- Hashing properties
  - One-way function—easy to compute hash and infeasible to compute data given a hash
  - Complex sequence of simple binary operations (XORs, rotations, etc.) which finally produces a 128-bit hash.



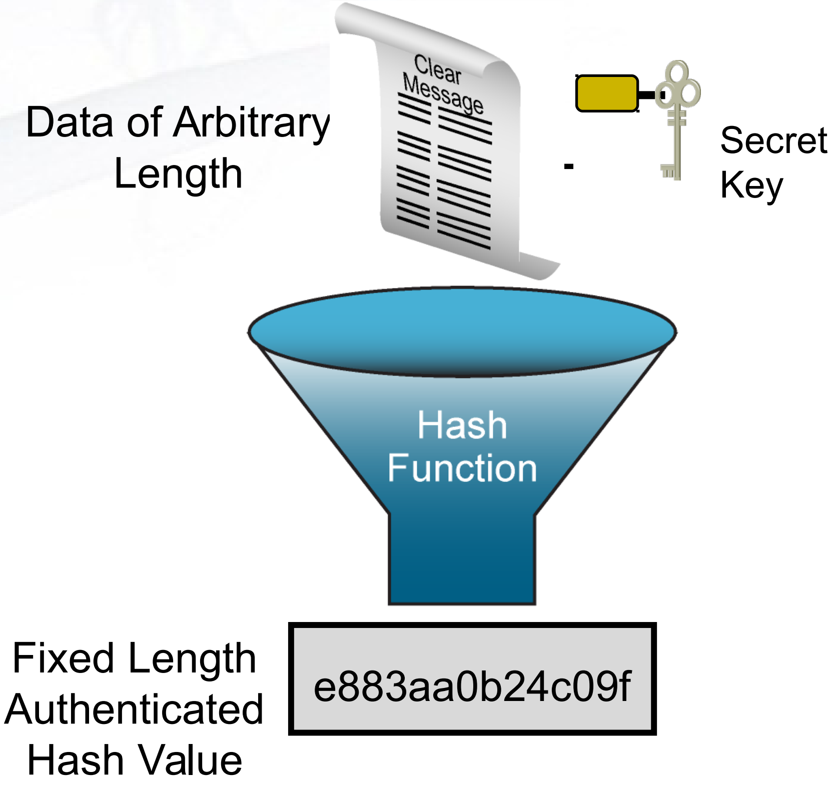
SHA

- SHA is similar in design to the MD4 and MD5 family of hash functions
  - Takes an input message of no more than 2^{64} bits
  - Produces a 160-bit message digest
- The algorithm is slightly slower than MD5.
- SHA-1 is a revision that corrected an unpublished flaw in the original SHA.
- SHA-224, SHA-256, SHA-384, and SHA-512 are newer and more secure versions of SHA and are collectively known as SHA-2.



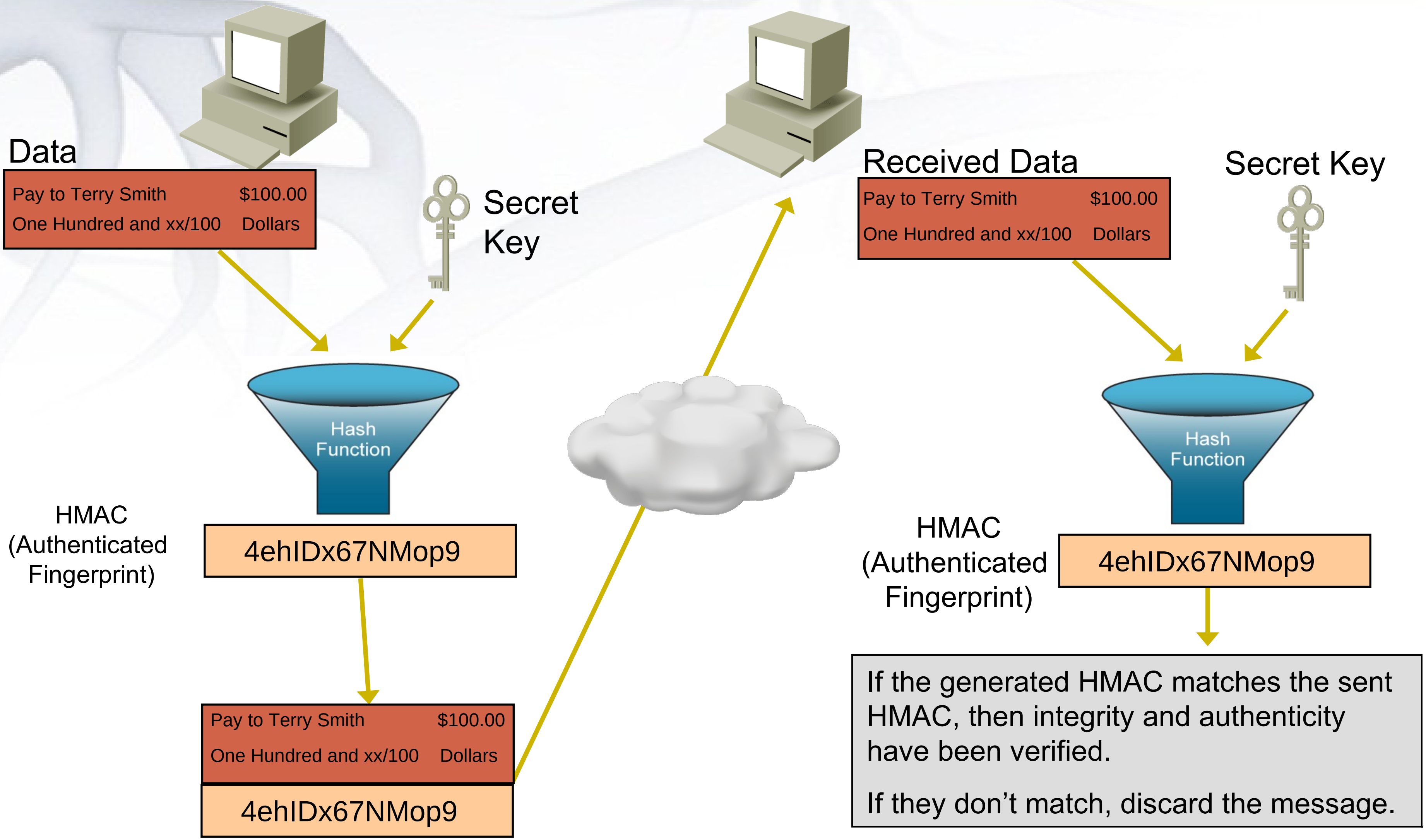
HMAC

- Uses an additional secret key as input to the hash function
- The secret key is known to the sender and receiver
  - Adds authentication to integrity assurance
  - Defeats man-in-the-middle attacks
- Based on existing hash functions, such as MD5 and SHA-1.



The same procedure is used for generation and verification of secure fingerprints

HMAC Example



Data
Pay to Terry Smith $100.00
One Hundred and xx/100 Dollars
Secret Key
Hash Function
HMAC (Authenticated Fingerprint)
4ehIDx67NMop9
Pay to Terry Smith $100.00
One Hundred and xx/100 Dollars
4ehIDx67NMop9
Received Data
Pay to Terry Smith $100.00
One Hundred and xx/100 Dollars
Secret Key
Hash Function
HMAC (Authenticated Fingerprint)
4ehIDx67NMop9

If the generated HMAC matches the sent HMAC, then integrity and authenticity have been verified.

If they don't match, discard the message.