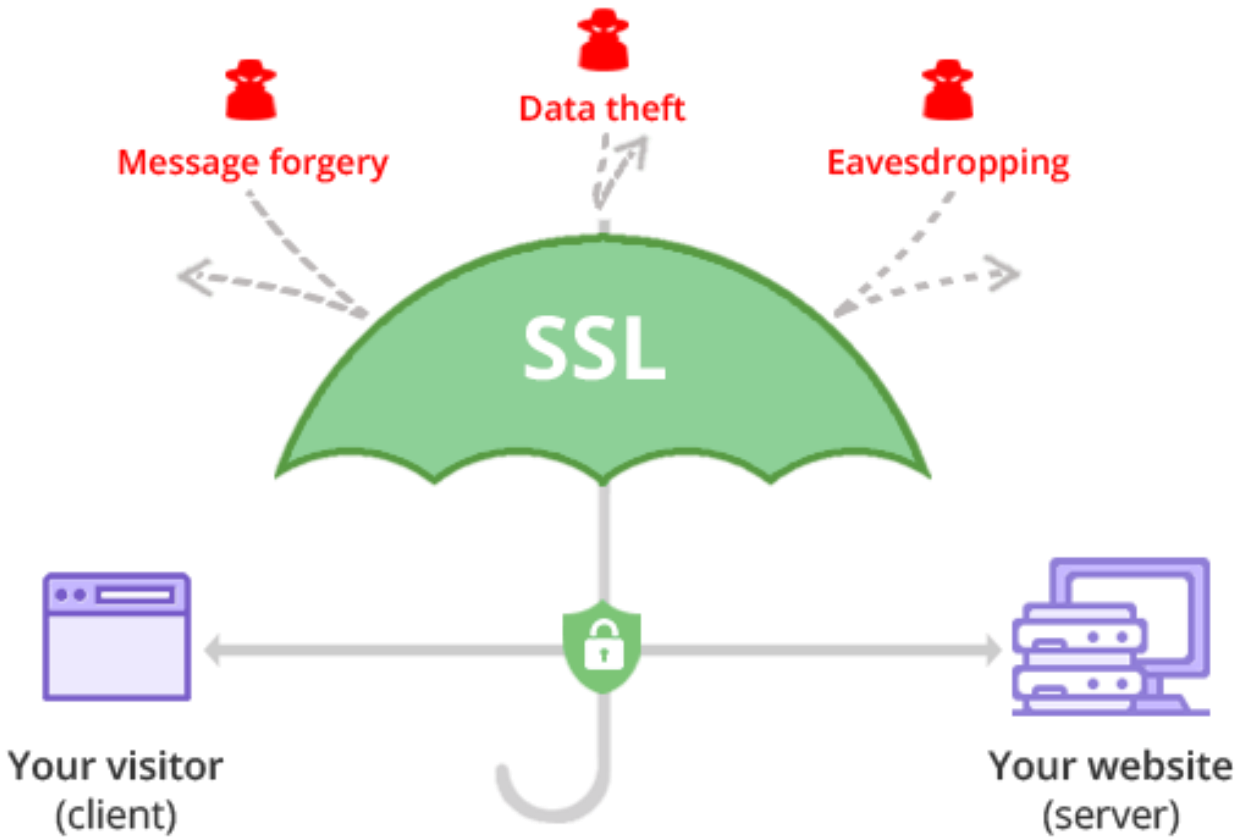
심플한 네이버톡톡 챗봇

INDEX

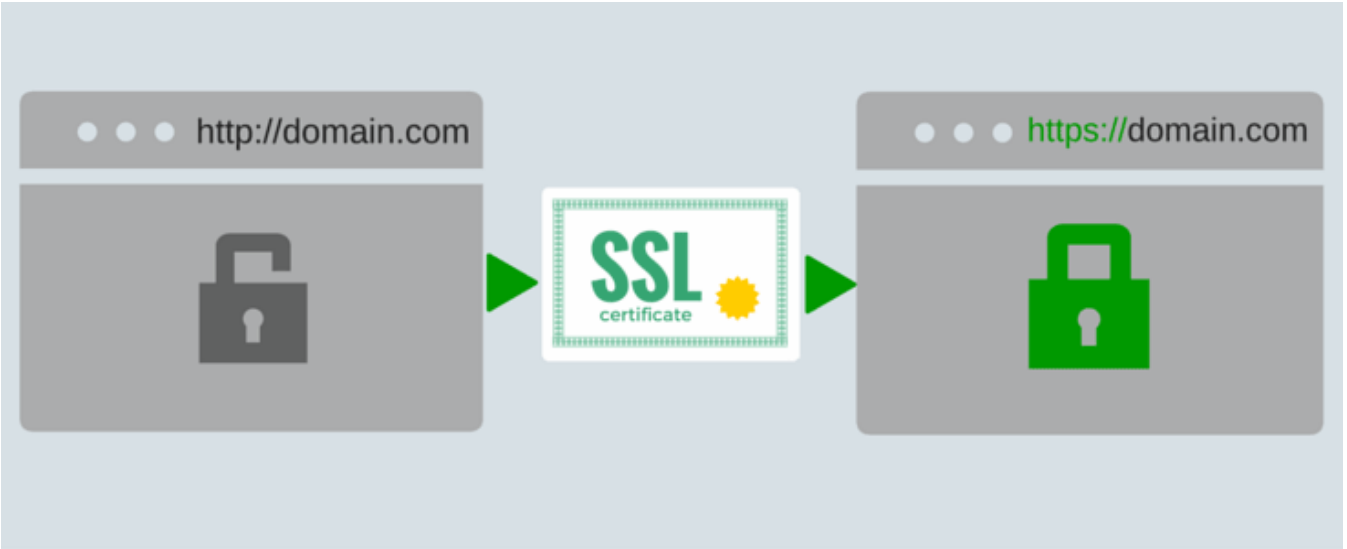
1. 개요



SSL과 웹 프레임워크를 이용한 간단한 챗봇 구현

2. 배경

- SSL이란?



Secure Socket Layer

웹 서버와 클라이언트 사이의 보안을 위해 개발

HTTPS프로토콜 통신의 기본 모델

- SSL 디지털 인증서

  - 제 3자가 통신을 보증하는 문서

  - 서버가 클라이언트에게 인증서 전달

  - 인증서 검증(인증된 기관에서 발급받았는지)

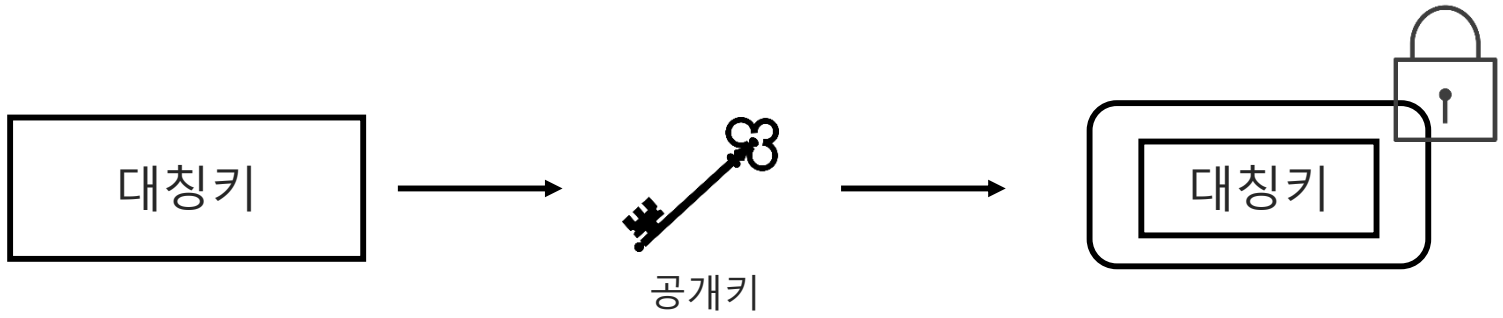
  - 인증, 기밀성, 무결성 보장

2. 배경

- SSL 암호화

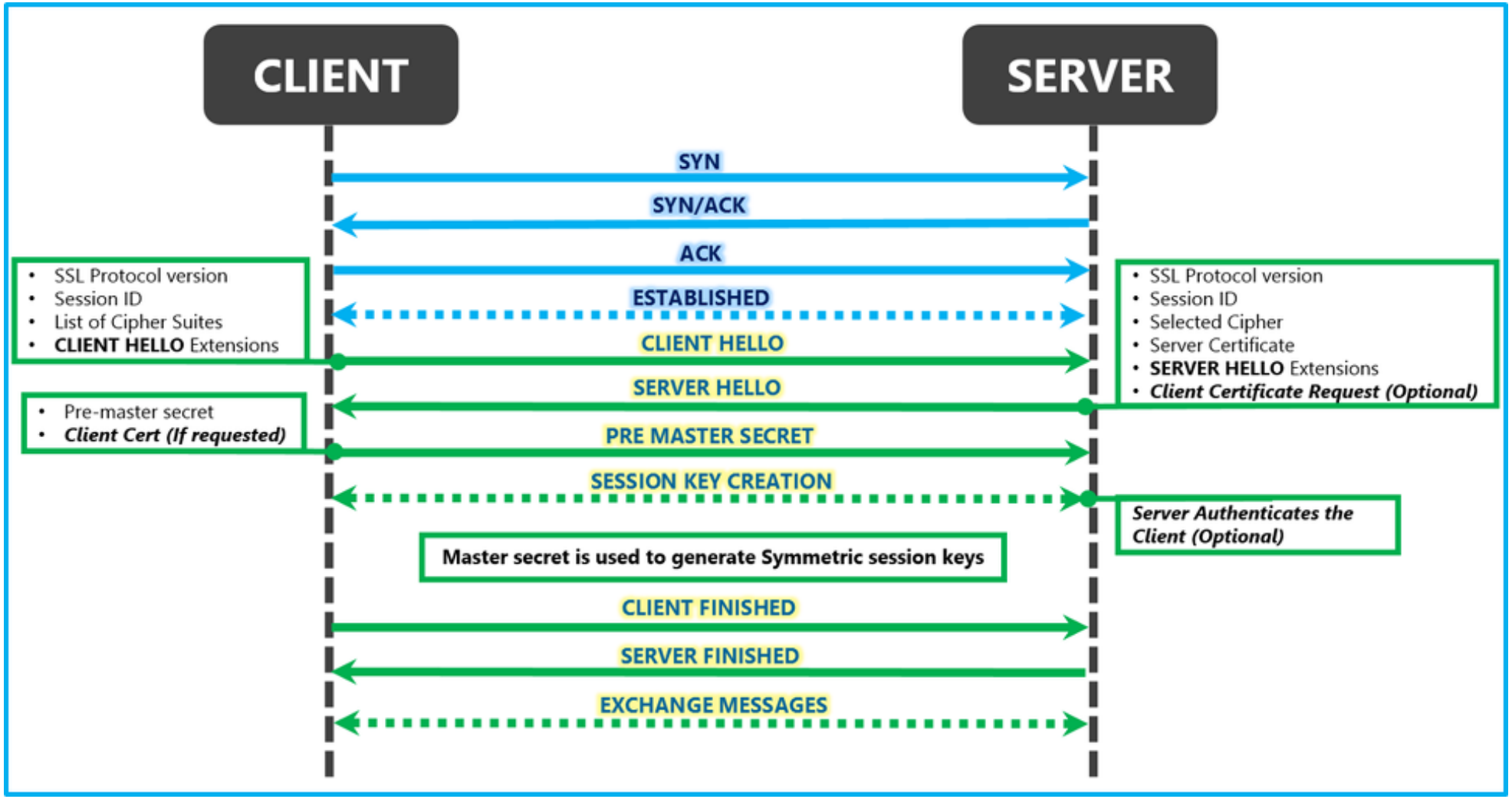
대칭키와 공개키 암호 혼용

- 대칭키 : 실제 데이터
- 공개키 : 대칭키의 키



2. 배경

- SSL 동작원리


CLIENT
SERVER
SYN
SYN/ACK
ACK
ESTABLISHED
CLIENT HELLO
SERVER HELLO
PRE MASTER SECRET
SESSION KEY CREATION
CLIENT FINISHED
SERVER FINISHED
EXCHANGE MESSAGES
• SSL Protocol version
• Session ID
• List of Cipher Suites
• CLIENT HELLO Extensions
• SSL Protocol version
• Session ID
• Selected Cipher
• Server Certificate
• SERVER HELLO Extensions
• Client Certificate Request (Optional)
• Pre-master secret
• Client Cert (If requested)
Server Authenticates the Client (Optional)
Master secret is used to generate Symmetric session keys

2. 배경

- SHA(해쉬 알고리즘)

SHA1, SHA2, SHA3, SHA5

SHA1은 SSL에서 채택 되지 않음

- 2013년 마크 스티븐스 해쉬 충돌 가능성 제시

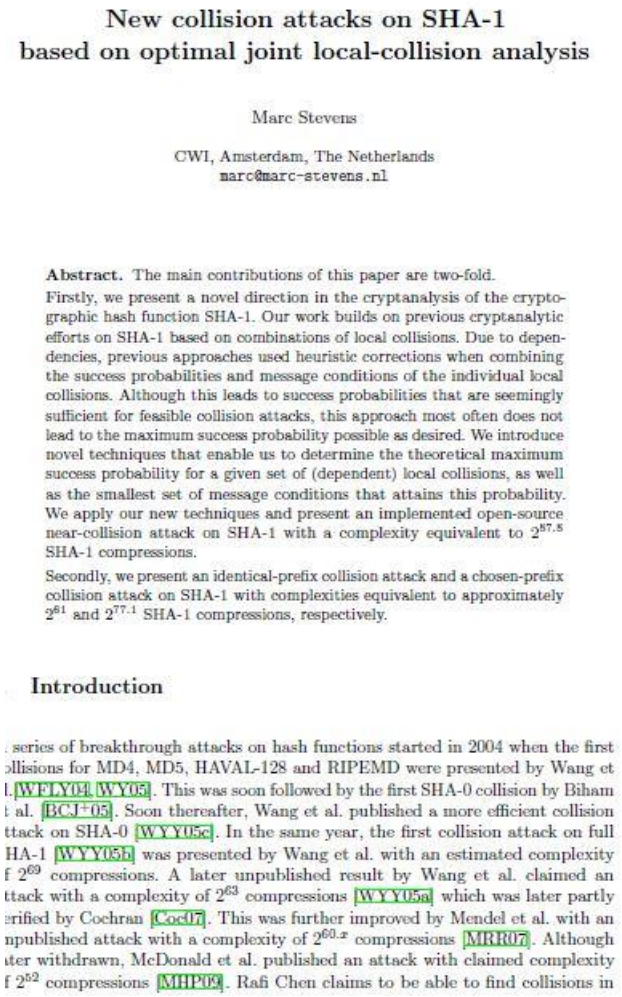
(해시 충돌: 해쉬함수가 서로 다른 두 개의 입력값에 대해 동일한 출력값을 내는 상황)

- 구글 & 네덜란드 암스테르담 국립수학전산학연구소

JPEG 이미지 데이터 영역에 충돌 블록삽입

SHA1 충돌 증명

- 실제로는 SHA256 알고리즘 사용



New collision attacks on SHA-1 based on optimal joint local-collision analysis

Marc Stevens

CWI, Amsterdam, The Netherlands
marc@marc-stevens.nl

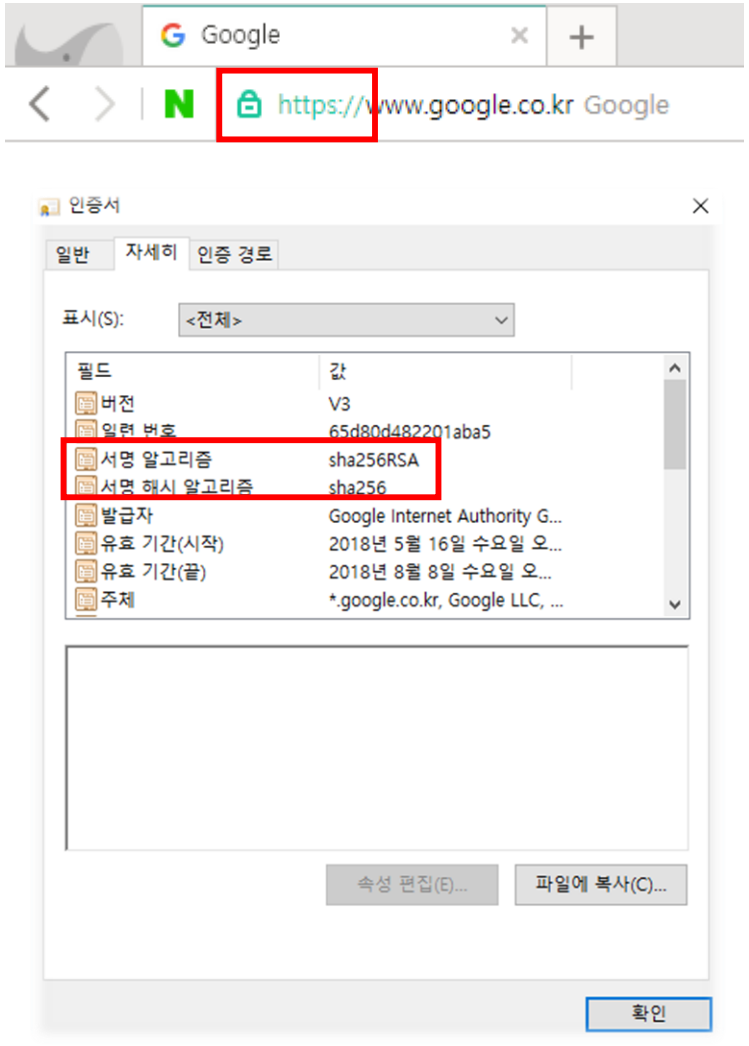
Abstract. The main contributions of this paper are two-fold.
Firstly, we present a novel direction in the cryptanalysis of the cryptographic hash function SHA-1. Our work builds on previous cryptanalytic efforts on SHA-1 based on combinations of local collisions. Due to dependencies, previous approaches used heuristic corrections when combining the success probabilities and message conditions of the individual local collisions. Although this leads to success probabilities that are seemingly sufficient for feasible collision attacks, this approach most often does not lead to the maximum success probability possible as desired. We introduce novel techniques that enable us to determine the theoretical maximum success probability for a given set of (dependent) local collisions, as well as the smallest set of message conditions that attains this probability. We apply our new techniques and present an implemented open-source near-collision attack on SHA-1 with a complexity equivalent to $2^{87.8}$ SHA-1 compressions.
Secondly, we present an identical-prefix collision attack and a chosen-prefix collision attack on SHA-1 with complexities equivalent to approximately 2^{61} and $2^{77.1}$ SHA-1 compressions, respectively.

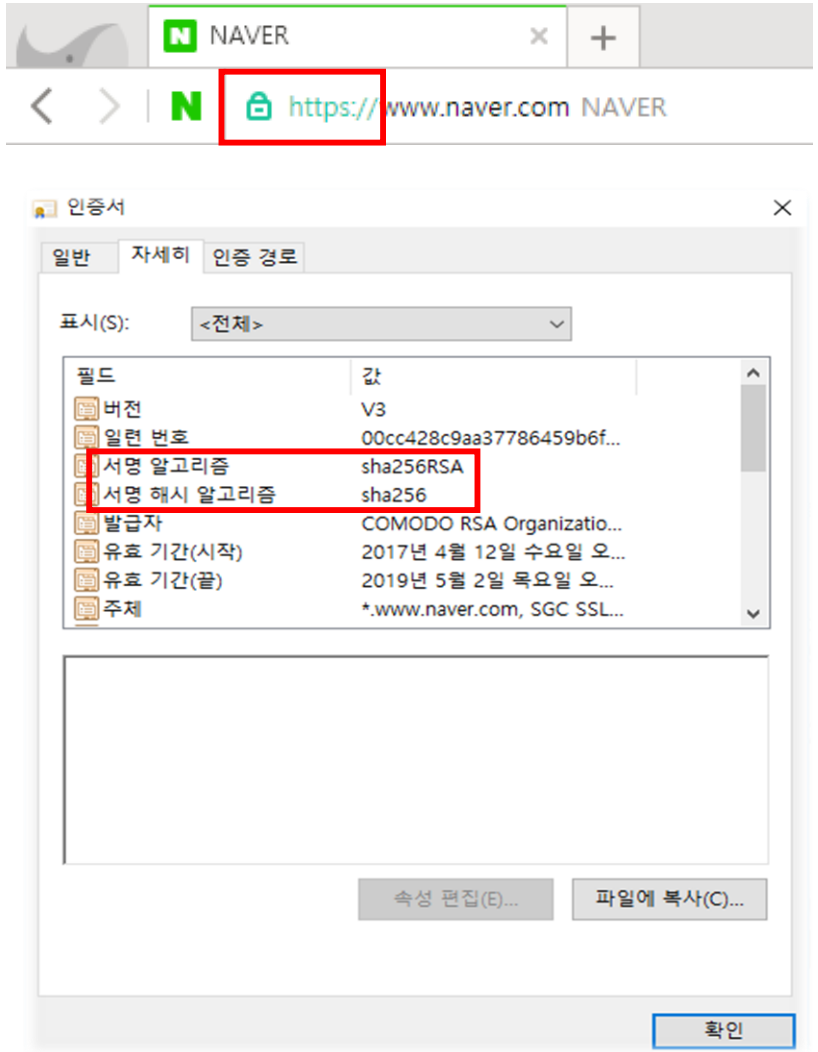
Introduction

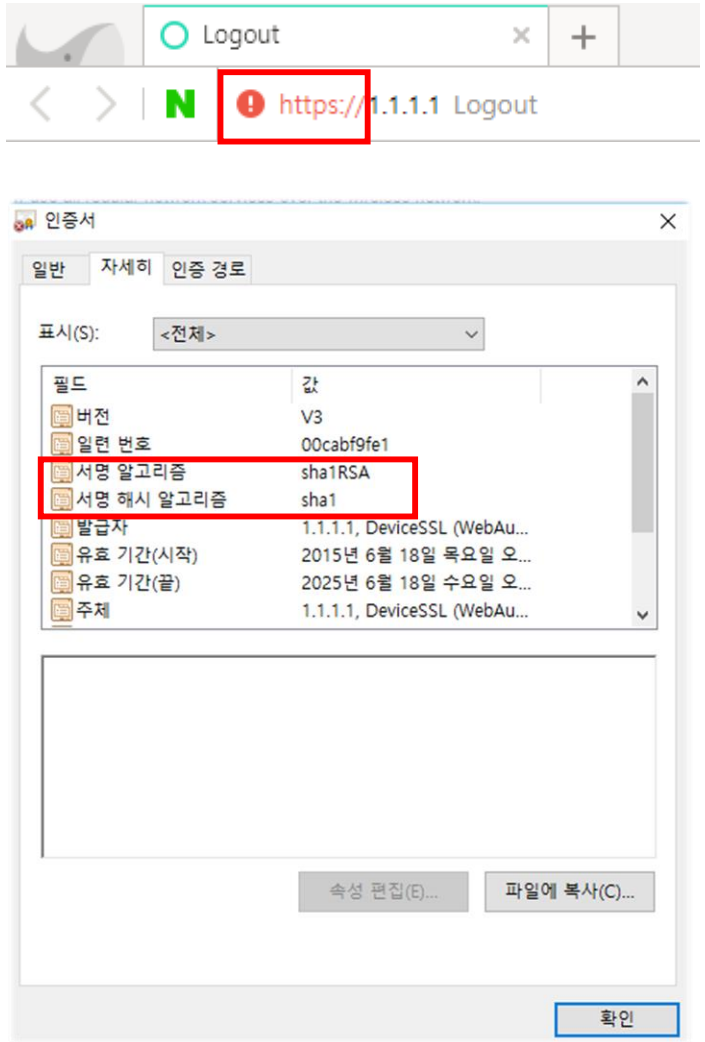
series of breakthrough attacks on hash functions started in 2004 when the first ollisions for MD4, MD5, HAVAL-128 and RIPEMD were presented by Wang et l. [WFLY04, WY05]. This was soon followed by the first SHA-0 collision by Biham t al. [BCJ+05]. Soon thereafter, Wang et al. published a more efficient collision ttack on SHA-0 [WYY05c]. In the same year, the first collision attack on full HA-1 [WYY05b] was presented by Wang et al. with an estimated complexity f 2^{69} compressions. A later unpublished result by Wang et al. claimed an ttack with a complexity of 2^{63} compressions [WYY05a] which was later partly erified by Cochran [Coc07]. This was further improved by Mendel et al. with an npublished attack with a complexity of $2^{60.x}$ compressions [MRR07]. Although ater withdrawn, McDonald et al. published an attack with claimed complexity f 2^{52} compressions [MHP09]. Rafi Chen claims to be able to find collisions in

2. 배경

- 사용 사례


Google
https://www.google.co.kr Google
인증서
일반
자세히
인증 경로
표시(S): <전체>
필드
값
버전
V3
일련 번호
65d80d482201aba5
서명 알고리즘
sha256RSA
서명 해시 알고리즘
sha256
발급자
Google Internet Authority G...
유효 기간(시작)
2018년 5월 16일 수요일 오...
유효 기간(끝)
2018년 8월 8일 수요일 오...
주체
*.google.co.kr, Google LLC, ...
속성 편집(E)...
파일에 복사(C)...
확인


NAVER
https://www.naver.com NAVER
인증서
일반
자세히
인증 경로
표시(S): <전체>
필드
값
버전
V3
일련 번호
00cc428c9aa37786459b6f...
서명 알고리즘
sha256RSA
서명 해시 알고리즘
sha256
발급자
COMODO RSA Organizatio...
유효 기간(시작)
2017년 4월 12일 수요일 오...
유효 기간(끝)
2019년 5월 2일 목요일 오...
주체
*.www.naver.com, SGC SSL...
속성 편집(E)...
파일에 복사(C)...
확인


Logout
https://1.1.1.1 Logout
인증서
일반
자세히
인증 경로
표시(S): <전체>
필드
값
버전
V3
일련 번호
00cabf9fe1
서명 알고리즘
sha1RSA
서명 해시 알고리즘
sha1
발급자
1.1.1.1, DeviceSSL (WebAu...
유효 기간(시작)
2015년 6월 18일 목요일 오...
유효 기간(끝)
2025년 6월 18일 수요일 오...
주체
1.1.1.1, DeviceSSL (WebAu...
속성 편집(E)...
파일에 복사(C)...
확인

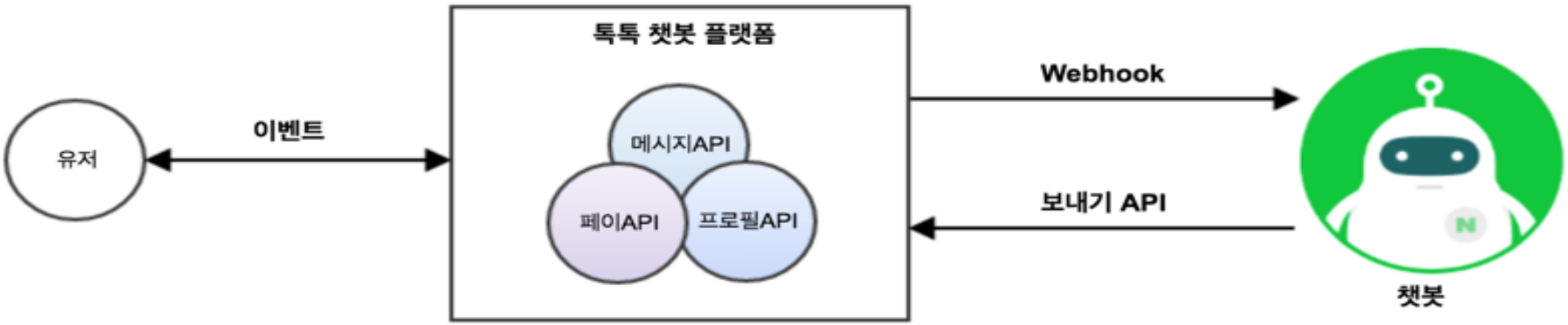
3. 설계

- Naver Talk Talk Chat Bot 프로그램이란?

웹에서 이용할 수 있는 웹 채팅 어플리케이션

사용자에게 다양한 메시지를 주고 받는 기능 제공

- ChatBot 작동 구조



- 왜 챗봇에 HTTPS가 들어가는 것일까?

- **네이버톡톡 Webhook 요구 사항**

Webhook 작성 방법

사용자 이벤트를 챗봇에게 전달할 때 `webhook`을 이용합니다. `webhook` 작성 방법은 다음과 같습니다.

Webhook 요구 사항

- `Webhook`은 `TLS` 기반의 통신을 지원해야 합니다.
  - 네이버 톡톡과 연동하는 외부 서비스 간의 메시지는 암호화 없이 평문으로 전달되므로 반드시 보호되어야 합니다.
  - 지원하는 TLS는 `TLSv1`, `TLSv1.1`, `TLSv1.2`입니다.
  - 정식 인증 기관으로부터 발급받은 유효한 인증서만 사용할 수 있습니다.
- `Webhook`을 사용하기 위해 ACL을 등록해야 한다면 다음의 IP 주소 목록을 추가합니다.
  - 117.52.141.192/27(117.52.141.193 ~ 117.52.141.222)
- 네이버 톡톡에서 `Webhook` 호출 시 설정값은 다음과 같습니다.
  - Connection timed out: `3초`
  - Read timed out: `5초`

- 왜 챗봇에 HTTPS가 들어가는 것일까?

- **네이버톡톡 Webhook 요구 사항**

Webhook 작성 방법

사용자 이벤트를 챗봇에게 전달할 때 `webhook`을 이용합니다. `webhook` 작성 방법은 다음과 같습니다.

Webhook 요구 사항

- `Webhook`은 `TLS` 기반의 통신을 지원해야 합니다.
  - 네이버 톡톡과 연동하는 외부 서비스 간의 메시지는 암호화 없이 평문으로 전달되므로 반드시 보호되어야 합니다.
  - 지원하는 TLS는 `TLSv1`, `TLSv1.1`, `TLSv1.2`입니다.
  - 정식 인증 기관으로부터 발급받은 유효한 인증서만 사용할 수 있습니다.
- `Webhook`을 사용하기 위해 ACL을 등록해야 한다면 다음의 IP 주소 목록을 추가합니다.
  - 117.52.141.192/27(117.52.141.193 ~ 117.52.141.222)
- 네이버 톡톡에서 `Webhook` 호출 시 설정값은 다음과 같습니다.
  - Connection timed out: `3초`
  - Read timed out: `5초`

- 왜 챗봇에 HTTPS가 들어가는 것일까?

- **네이버톡톡 API 스펙 이슈**

- [채팅창에 `hello world` 메시지를 보냈을 때 이벤트 로그]

```
{
  "event": "send",
  "user": "a1-2eGuGr5WQOnco1_V-FQ",
  "textContent": {
      "text": "hello world",
      "inputType": "typing"
  }
}
```

3. 설계

- SSL 인증서를 발급받기 위해서

Single Domain SSL 인증서 상품 - 단일 도메인에 SSL 인증서 적용

	1년	2년 (10%할인)	배상금	
Comodo PositiveSSL	₩ 12,000	₩ 21,000 (10,500/y)	$ 10,000	상세보기
Comodo Essential SSL				
RapidSSL Standard				
Thawte SSL 123				
Comodo SSL				
GeoTrust QuickSSL Premium				

Wildcard Domain SSL 인증서 상품 - 무제한 서브(*.) 도메인에 SSL 인증서 적용

	1년	2년 (10%할인)	배상금	
Comodo PositiveSSL Wildcard	₩ 150,000	₩ 270,000 (135,000/y)	$ 10,000	상세보기
Comodo Essential Wildcard	₩ 180,000	₩ 324,000 (162,000/y)	$ 10,000	상세보기
RapidSSL Wildcard	₩ 180,000	₩ 324,000 (162,000/y)	$ 10,000	상세보기
Comodo SSL Wildcard	₩ 380,000	₩ 684,000 (342,000/y)	$ 250,000	상세보기
Thawte SSL 123 Wildcard	₩ 430,000	₩ 774,000 (387,000/y)	$ 500,000	상세보기
GeoTrust QuickSSL Premium Wildcard	₩ 480,000	₩ 864,000 (432,000/y)	$ 500,000	상세보기

3. Let’s Encrypt

- Let’s Encrypt 이란?

HTTPS Everywhere 를 추구하는 비영리 프로젝트

TLS 암호화를 위해 무료 X.509 인증서를 제공하는 인증 기관

스폰서 : Mozilla, Akamai, Cisco, eff, Identrust

콘솔상에서 인증서 발급/갱신/설치 가능한 편리성 제공

서버 설계 및 개발 환경

- **개발 환경 :** AWS EC2 Instance
- **운영 체제 :** Ubuntu 16. 04. 4 LTS
- **사용 언어 :** Python (버전: 3.5.2)
- **사용한 웹 프레임워크 :** Flask
- **테스트에 사용한 툴 :** Postman, Whale 브라우저

4. 구현

- 웹 프레임워크에 SSL 인증서 링크

```
if __name__ == "__main__":
    ssl_cert = '/etc/letsencrypt/live/daeta.ga/fullchain.pem'
    ssl_key =  '/etc/letsencrypt/live/daeta.ga/privkey.pem'
    contextSSL =  (ssl_cert, ssl_key)
    app.run(host="0.0.0.0", port=443, debug = True, ssl_context = contextSSL)
```

- Let's Encrypt로 발급받은 SSL 인증서의 **경로를 링크**
- HTTPS 를 지원하는 **443**번 포트를 사용

4. 구현

- 웹 프레임워크에 SSL 인증서 링크

```
if __name__ == "__main__":
    ssl_cert = '/etc/letsencrypt/live/daeta.ga/fullchain.pem'
    ssl_key =  '/etc/letsencrypt/live/daeta.ga/privkey.pem'
    contextSSL =  (ssl_cert, ssl_key)
    app.run(host="0.0.0.0", port=443, debug = True, ssl_context = contextSSL)
```

- Let's Encrypt로 발급받은 SSL 인증서의 **경로를 링크**
- HTTPS 를 지원하는 **443**번 포트를 사용

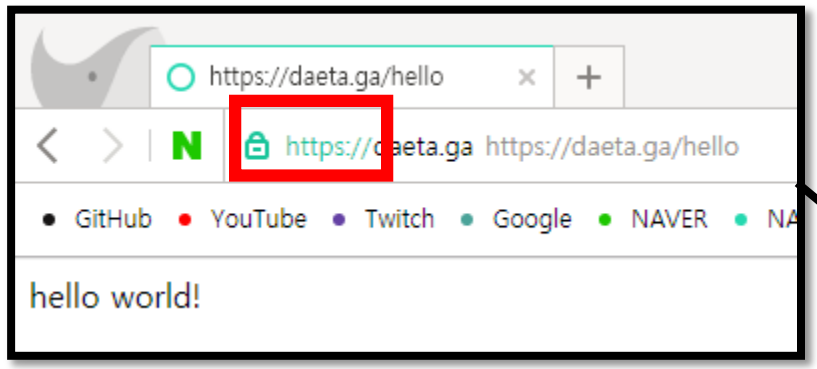
4. 구현

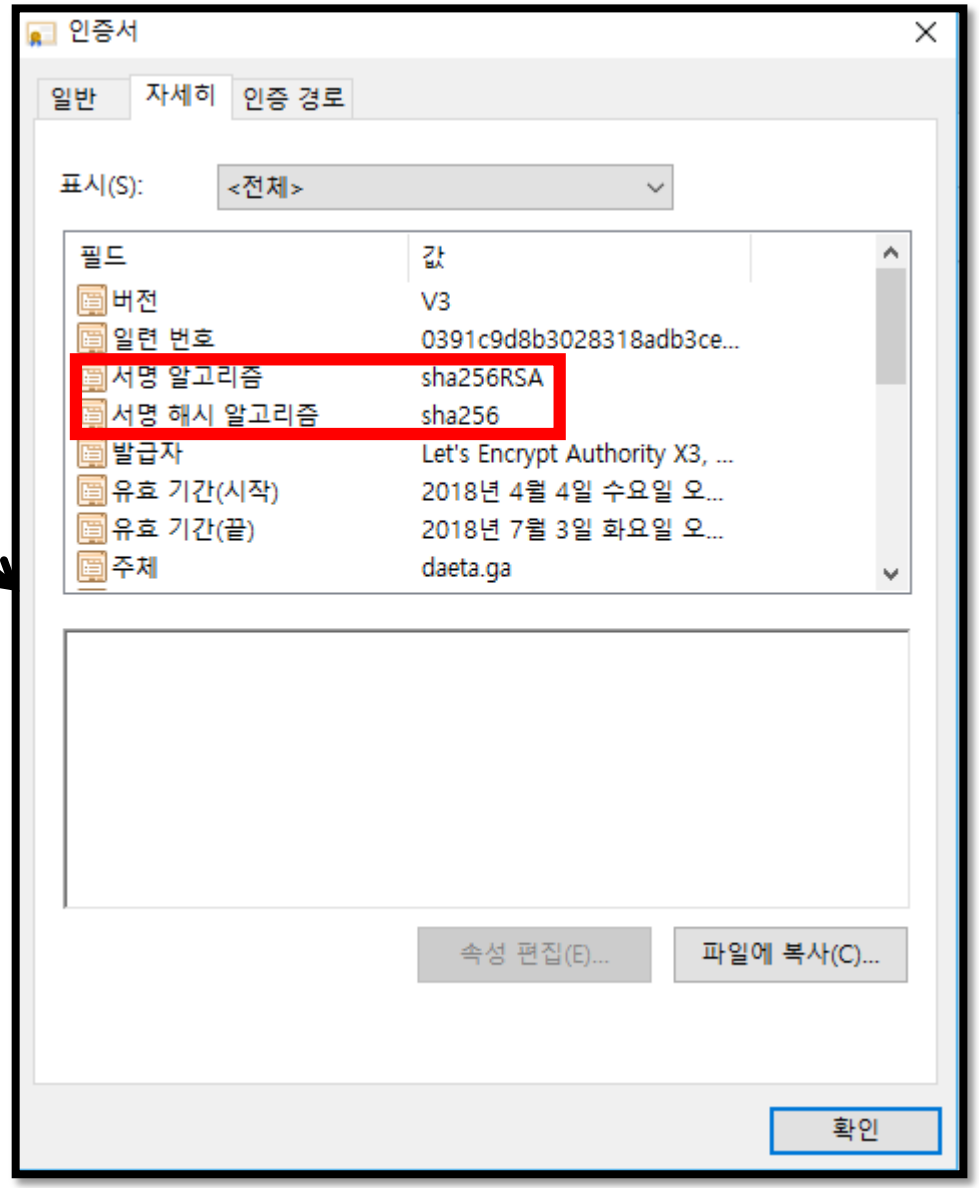
- 챗봇 API에 따른 핸들러 작성

```python
def get_handler(data):
    sendMSG = "None"
    user = data["user"]

    if data["event"] == "open":
        sendMSG = openEvent()

    elif data["event"] == "leave":
        sendMSG = leaveEvent()

    elif data["event"] == "send":
        message = data["textContent"]["text"]
        if data["textContent"]["inputType"] == "typing":
            sendMSG = sendEvent(message=message)
        else:
            sendMSG = "현재 지원하지 않는 타입의 메세지에요 ㅠㅠ"

    return setData(user=user, sendMSG=sendMSG)
```

5. 결과

- HTTPS 테스트

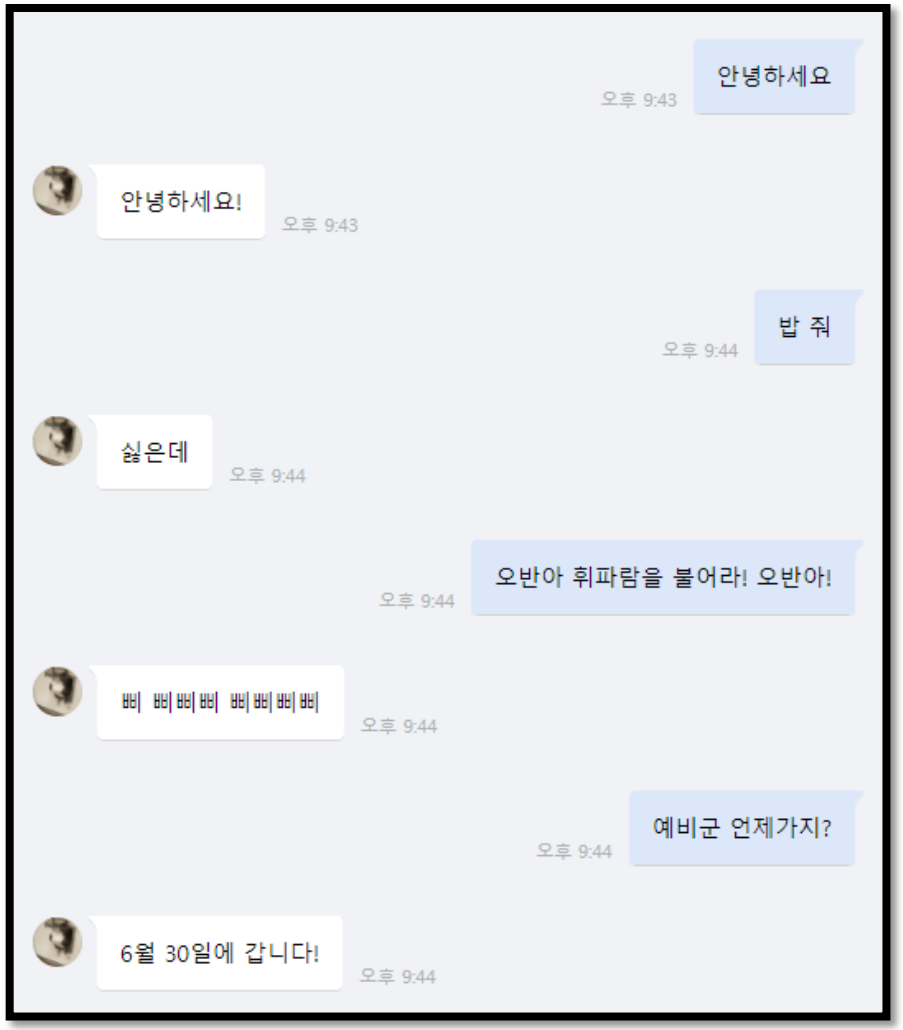




- 제대로 HTTPS 적용이 됨
- 서명과정에서 암호화가 됨을 확인 가능

5. 결과

- 결과 스냅샷



네이버톡톡(클라이언트)

```
 * Detected change in '/home/ubuntu/report/sec/server.py', reloading
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 213-827-650
 * Detected change in '/home/ubuntu/report/sec/handler.py', reloading
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 213-827-650
117.52.141.201 - - [30/May/2018 12:43:55] "POST / HTTP/1.1" 200 -
117.52.141.201 - - [30/May/2018 12:44:06] "POST / HTTP/1.1" 200 -
117.52.141.201 - - [30/May/2018 12:44:33] "POST / HTTP/1.1" 200 -
117.52.141.201 - - [30/May/2018 12:44:47] "POST / HTTP/1.1" 200 -
117.52.141.201 - - [30/May/2018 12:44:51] "POST / HTTP/1.1" 200 -
117.52.141.201 - - [30/May/2018 12:45:00] "POST / HTTP/1.1" 200 -
```

챗봇 서버

References

[1]"SSL이란 무엇이며 인증서(Certificate)란 무엇인가?", Wiki.kldp.org, 2018. [Online]. Available: https://wiki.kldp.org/HOWTO/html/SSL-Certificates-HOWTO/x70.html. [Accessed: 29- May- 2018].

[2]"HTTPS와 SSL 인증서 - 생활코딩", 인터넷, 2018. [Online]. Available: https://opentutorials.org/course/228/4894. [Accessed: 29- May- 2018].

[3]"SSL Protocol 개념과 동작 원리", Programmer, 2018. [Online]. Available: http://yagi815.tistory.com/168. [Accessed: 29- May- 2018].

[4]"apache/httpd", GitHub, 2018. [Online]. Available: https://github.com/apache/httpd/tree/trunk/modules/ssl. [Accessed: 29- May- 2018].

[5]"BaconRemovalUnit/SHA256", GitHub, 2018. [Online]. Available: https://github.com/BaconRemovalUnit/SHA256/blob/master/src/sha256-384-512.pdf. [Accessed: 29- May- 2018].

[6]"openssl/openssl", GitHub, 2018. [Online]. Available: https://github.com/openssl/openssl. [Accessed: 29- May- 2018].

[7]"openssl/openssl", GitHub, 2018. [Online]. Available: https://github.com/openssl/openssl/blob/master/crypto/sha/sha256.c. [Accessed: 29- May- 2018].

[8]"What is the Difference Between SHA-1, SHA-2 and SHA-256?", Hashed Out by The SSL Store™, 2018. [Online]. Available: https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/. [Accessed: 29- May- 2018].

[9]"IT news, careers, business technology, reviews", ITworld, 2018. [Online]. Available: http://www.itworld.co.kr/opinion/108321. [Accessed: 29- May- 2018].

Q&A

END