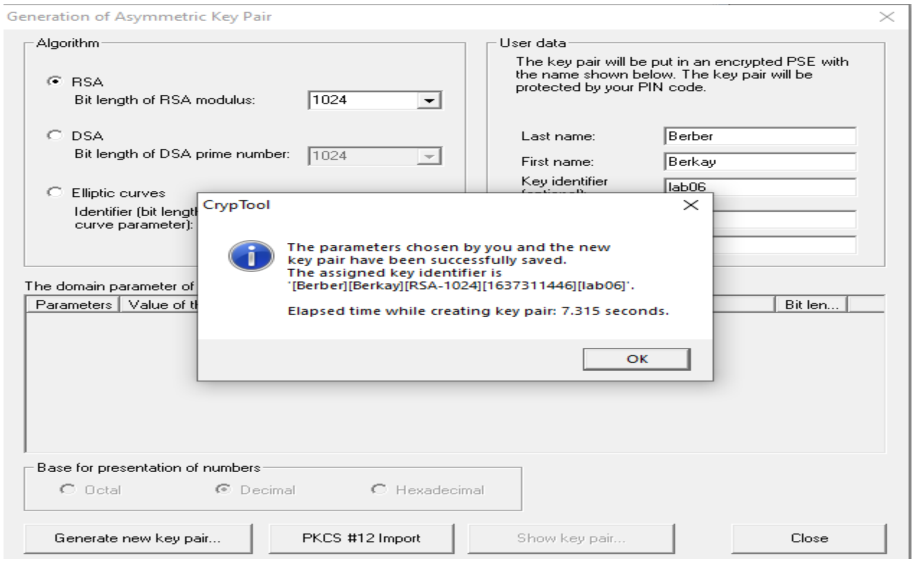
3. Digital signature Tool: Cryptool

I. Tasks:

1. Check the list of available keys and then generate your own key (RSA or DSS algorithm), and include its certificate in the report. Tab: Digital signatures/PKI -> PKI -> Generate Keys

= > The creating key is took something around 7 second.



Generation of Asymmetric Key Pair

Algorithm

● RSA
Bit length of RSA modulus: 1024

○ DSA
Bit length of DSA prime number: 1024

○ Elliptic curves
Identifier (bit lengt
curve parameter):

User data

The key pair will be put in an encrypted PSE with the name shown below. The key pair will be protected by your PIN code.

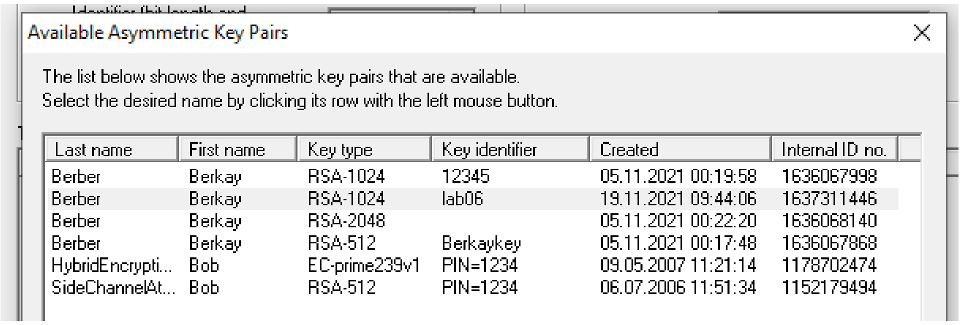
Last name: Berber
First name: Berkay
Key identifier: lab06

CrypTool

The parameters chosen by you and the new key pair have been successfully saved.
The assigned key identifier is
'[Berber][Berkay][RSA-1024][1637311446][lab06]'.

Elapsed time while creating key pair: 7.315 seconds.

Base for presentation of numbers: ○ Octal ● Decimal ○ Hexadecimal

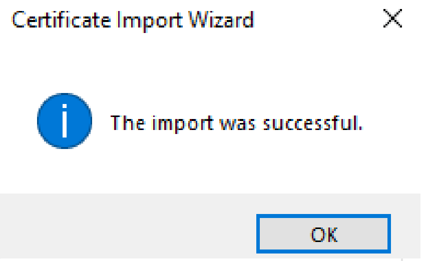


Available Asymmetric Key Pairs

The list below shows the asymmetric key pairs that are available.
Select the desired name by clicking its row with the left mouse button.

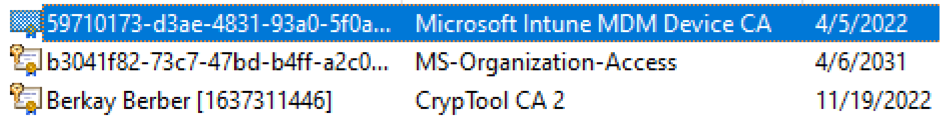
Last name	First name	Key type	Key identifier	Created	Internal ID no.
Berber	Berkay	RSA-1024	12345	05.11.2021 00:19:58	1636067998
Berber	Berkay	RSA-1024	lab06	19.11.2021 09:44:06	1637311446
Berber	Berkay	RSA-2048		05.11.2021 00:22:20	1636068140
Berber	Berkay	RSA-512	Berkaykey	05.11.2021 00:17:48	1636067868
HybridEncrypti...	Bob	EC-prime239v1	PIN=1234	09.05.2007 11:21:14	1178702474
SideChannelAt...	Bob	RSA-512	PIN=1234	06.07.2006 11:51:34	1152179494

2. Export your own certificate and then import it into your web browser.



Certificate Import Wizard

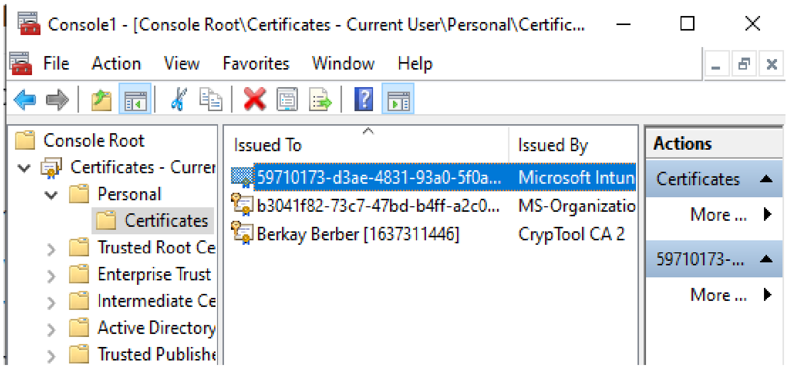
The import was successful.



59710173-d3ae-4831-93a0-5f0a...	Microsoft Intune MDM Device CA	4/5/2022
b3041f82-73c7-47bd-b4ff-a2c0...	MS-Organization-Access	4/6/2031
Berkay Berber [1637311446]	CrypTool CA 2	11/19/2022

3. Watch the demonstration showing the signing process.

= >In order to add the certificate we used mmc command.

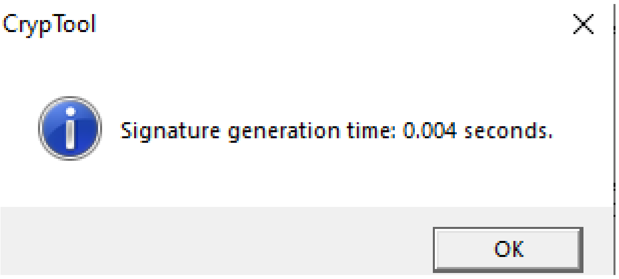


Console1 - [Console Root\Certificates - Current User\Personal\Certific...

Issued To	Issued By
59710173-d3ae-4831-93a0-5f0a...	Microsoft Intun
b3041f82-73c7-47bd-b4ff-a2c0...	MS-Organizatio
Berkay Berber [1637311446]	CrypTool CA 2

4. Sign any document with your own key

= > I tried to sign with several types of hash function and I came across the same signature generation time of each.

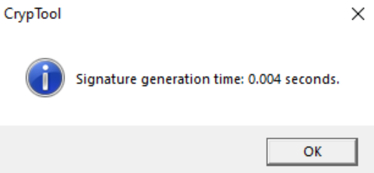


CrypTool

Signature generation time: 0.004 seconds.

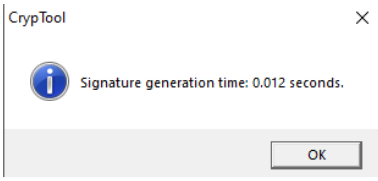
5. Compare the time of signing documents of different sizes using different keys.

RSA 1024 lab06



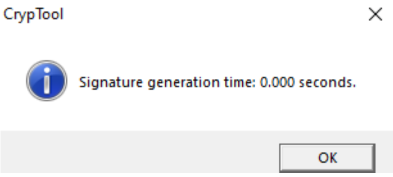
Signature generation time: 0.004 seconds.

RSA 2048



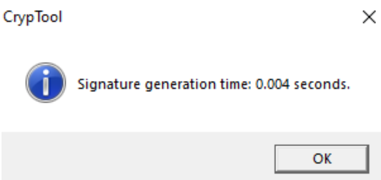
Signature generation time: 0.012 seconds.

RSA 512



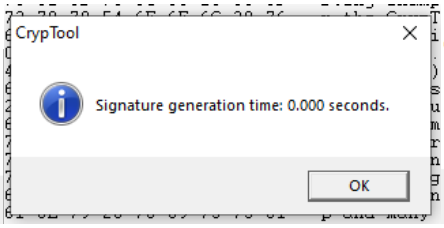
Signature generation time: 0.000 seconds.

EC-prime239v1



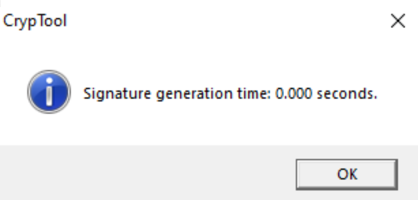
Signature generation time: 0.004 seconds.

DSA 512



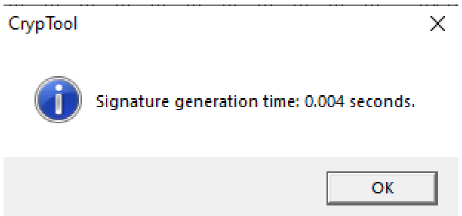
Signature generation time: 0.000 seconds.

DSA 1024



Signature generation time: 0.000 seconds.

DSA 2048



Signature generation time: 0.004 seconds.

Result according to generation times is presented in the below table.

KEY TYPE	TIME
RSA 1024	0.004
RSA 2048	0.012
RSA 512	0.000
EC-prime239v1	0.004
DSA 512	0.000
DSA 1024	0.000
DSA 2048	0.004

II. Questions:

1. **What are the elements of public-key certificates?**

= > Four main components of the PKI are public key encryption, trusted third parties such as the CA, the registration authority and the certificate database or store. The fundamental elements of a public key infrastructure. The certificate consist of a public key, private key, certificate authority, certificate store, Certificate revocation.

2. **What is digital signature? What are the elements of a digital signature?**

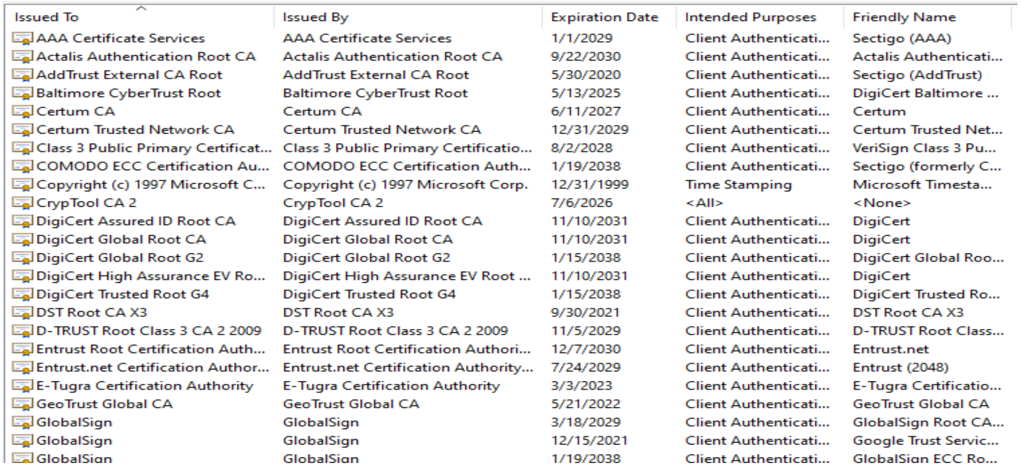
= > Digital signature is a process that protects the content of a message have not been changed during the transit. When we digitally sign a document, we add a one-way hash(encryption) of the message content using our public and private key pair. when the message along with its Digital Signature are sent to client, than client computer proceed to; decrypt the digital Signature using our public key, calculates the hash of the message and compares the (our)hash it has computed from the received message with the (client)decrypted hash received with client message. Client using the server's public key can validate the sender as well as the integrity of message contents. If the transmission arrives but, than client knows that the message has been altered.

3. **How does the time of execution of a digital signature of a document change and what does it depend on?**

= > İt is determined by the algorithms we are using as well as the key size. As we experienced from the above tasks there is a distinct time difference between the algorithm bits we used. Since we increased the bits than the time of execution of a document will be increased simultaneously.

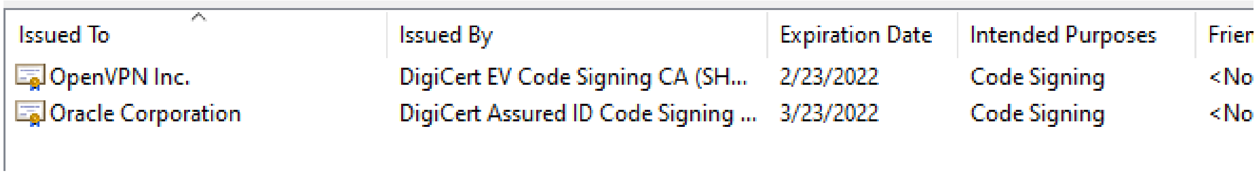
4. **Check which other certificates your can find in your web browser and include some examples in the report.**

Trusted Root Certification Authorities



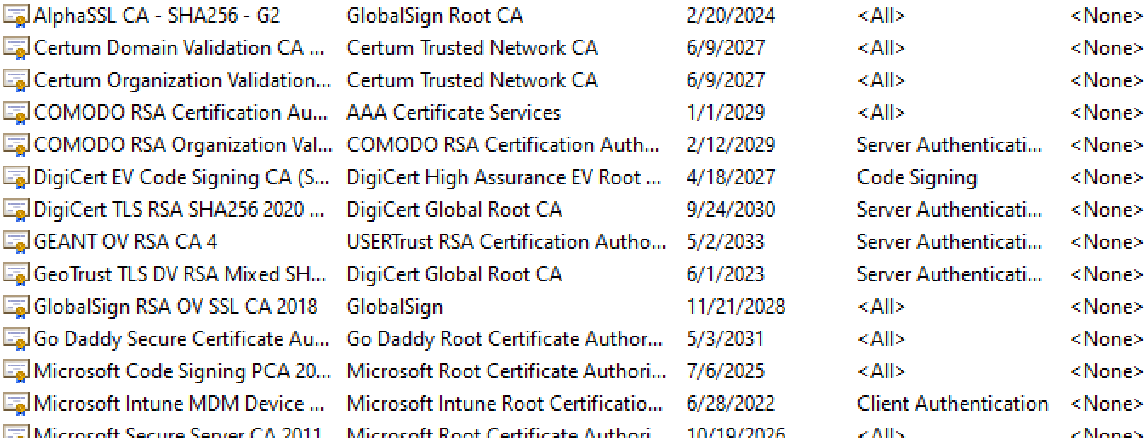
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
AAA Certificate Services	AAA Certificate Services	1/1/2029	Client Authenticati...	Sectigo (AAA)
Actalis Authentication Root CA	Actalis Authentication Root CA	9/22/2030	Client Authenticati...	Actalis Authenticati...
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Client Authenticati...	Sectigo (AddTrust)
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/13/2025	Client Authenticati...	DigiCert Baltimore ...
Certum CA	Certum CA	6/11/2027	Client Authenticati...	Certum
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Client Authenticati...	Certum Trusted Net...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/2/2028	Client Authenticati...	VeriSign Class 3 Pu...
COMODO ECC Certification Au...	COMODO ECC Certification Auth...	1/19/2038	Client Authenticati...	Sectigo (formerly C...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/31/1999	Time Stamping	Microsoft Timesta...
CrypTool CA 2	CrypTool CA 2	7/6/2026	<All>	<None>
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/10/2031	Client Authenticati...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031	Client Authenticati...	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati...	DigiCert Global Roo...
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/10/2031	Client Authenticati...	DigiCert
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati...	DigiCert Trusted Ro...
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authenticati...	DST Root CA X3
D-TRUST Root Class 3 CA 2 2009	D-TRUST Root Class 3 CA 2 2009	11/5/2029	Client Authenticati...	D-TRUST Root Class...
Entrust Root Certification Auth...	Entrust Root Certification Authori...	12/7/2030	Client Authenticati...	Entrust.net
Entrust.net Certification Author...	Entrust.net Certification Authority...	7/24/2029	Client Authenticati...	Entrust (2048)
E-Tugra Certification Authority	E-Tugra Certification Authority	3/3/2023	Client Authenticati...	E-Tugra Certificatio...
GeoTrust Global CA	GeoTrust Global CA	5/21/2022	Client Authenticati...	GeoTrust Global CA
GlobalSign	GlobalSign	3/18/2029	Client Authenticati...	GlobalSign Root CA...
GlobalSign	GlobalSign	12/15/2021	Client Authenticati...	Google Trust Servic...
GlobalSign	GlobalSign	1/19/2038	Client Authenticati...	GlobalSign ECC Ro...

Trusted publishers



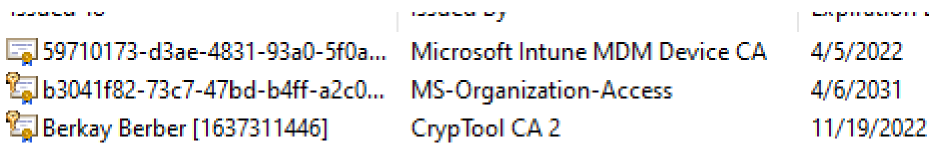
Issued To	Issued By	Expiration Date	Intended Purposes	Frier
OpenVPN Inc.	DigiCert EV Code Signing CA (SH...	2/23/2022	Code Signing	<No
Oracle Corporation	DigiCert Assured ID Code Signing ...	3/23/2022	Code Signing	<No

Intermediate Certification Authorities



AlphaSSL CA - SHA256 - G2	GlobalSign Root CA	2/20/2024	<All>	<None>
Certum Domain Validation CA ...	Certum Trusted Network CA	6/9/2027	<All>	<None>
Certum Organization Validation...	Certum Trusted Network CA	6/9/2027	<All>	<None>
COMODO RSA Certification Au...	AAA Certificate Services	1/1/2029	<All>	<None>
COMODO RSA Organization Val...	COMODO RSA Certification Auth...	2/12/2029	Server Authenticati...	<None>
DigiCert EV Code Signing CA (S...	DigiCert High Assurance EV Root ...	4/18/2027	Code Signing	<None>
DigiCert TLS RSA SHA256 2020 ...	DigiCert Global Root CA	9/24/2030	Server Authenticati...	<None>
GEANT OV RSA CA 4	USERTrust RSA Certification Autho...	5/2/2033	Server Authenticati...	<None>
GeoTrust TLS DV RSA Mixed SH...	DigiCert Global Root CA	6/1/2023	Server Authenticati...	<None>
GlobalSign RSA OV SSL CA 2018	GlobalSign	11/21/2028	<All>	<None>
Go Daddy Secure Certificate Au...	Go Daddy Root Certificate Author...	5/3/2031	<All>	<None>
Microsoft Code Signing PCA 20...	Microsoft Root Certificate Authori...	7/6/2025	<All>	<None>
Microsoft Intune MDM Device ...	Microsoft Intune Root Certificatio...	6/28/2022	Client Authentication	<None>
Microsoft Secure Server CA 2011	Microsoft Root Certificate Authori...	10/19/2026	<All>	<None>

Personal



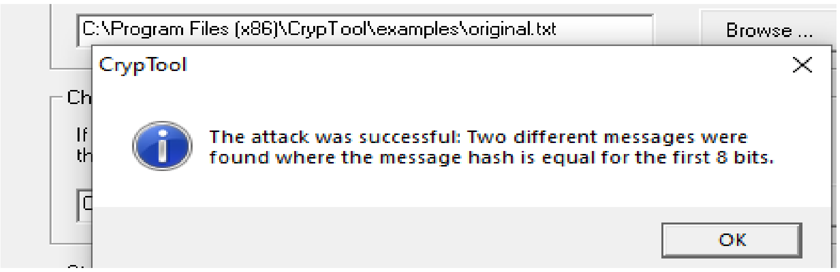
Issued To	Issued By	Expiration
59710173-d3ae-4831-93a0-5f0a...	Microsoft Intune MDM Device CA	4/5/2022
b3041f82-73c7-47bd-b4ff-a2c0...	MS-Organization-Access	4/6/2031
Berkay Berber [1637311446]	CrypTool CA 2	11/19/2022

Using Microsoft Management console, i observed the certificates in console root.

4. Hash function

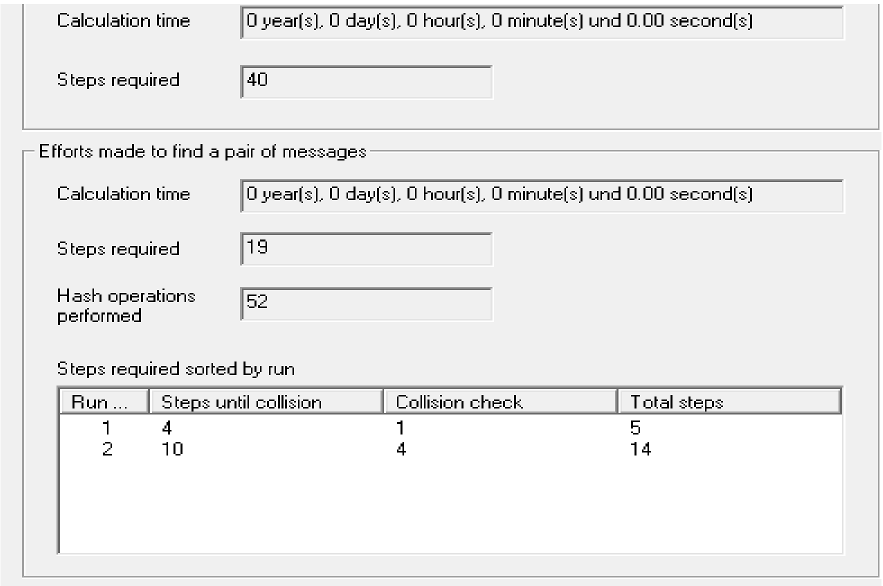
I. Tasks:

1. **Perform the attack on the hash function based on the default files. (Analysis -> Hash -> Attack on the hash value of the digital signature)**



C:\Program Files (x86)\CrypTool\examples\original.txt

The attack was successful: Two different messages were found where the message hash is equal for the first 8 bits.



Calculation time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.00 second(s)

Steps required: 40

Efforts made to find a pair of messages

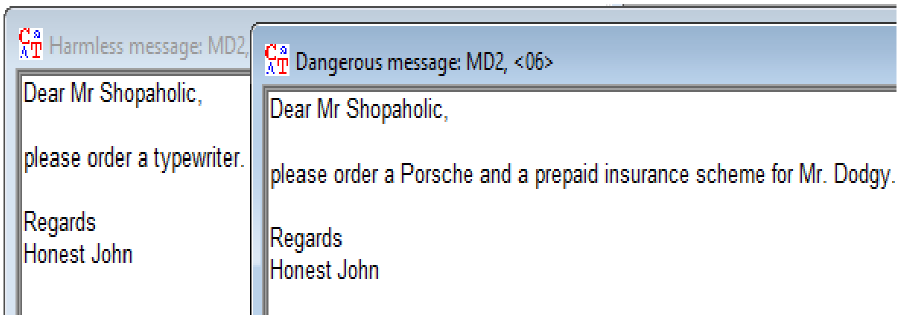
Calculation time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.00 second(s)

Steps required: 19

Hash operations performed: 52

Steps required sorted by run

Run ...	Steps until collision	Collision check	Total steps
1	4	1	5
2	10	4	14



Harmless message: MD2,

Dear Mr Shopaholic,

please order a typewriter.

Regards
Honest John

Dangerous message: MD2, <06>

Dear Mr Shopaholic,

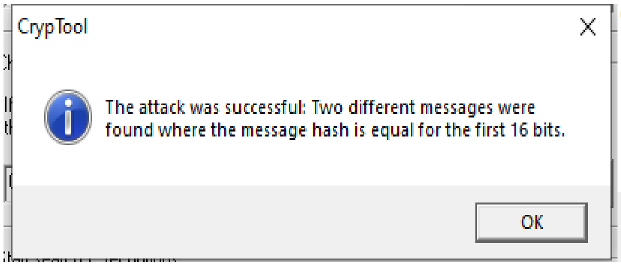
please order a Porsche and a prepaid insurance scheme for Mr. Dodgy.

Regards
Honest John

2. **Perform the attack again. But change the hash function and the significant bit length(at least two others).**

= > İn order to perform the attack again i use SHA-1 and MD5 hash function and 16,30 Significant bit length**.**

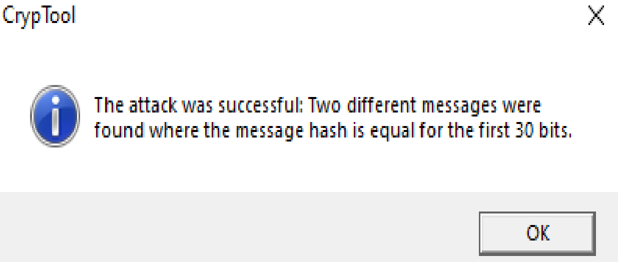
16



CrypTool

The attack was successful: Two different messages were found where the message hash is equal for the first 16 bits.

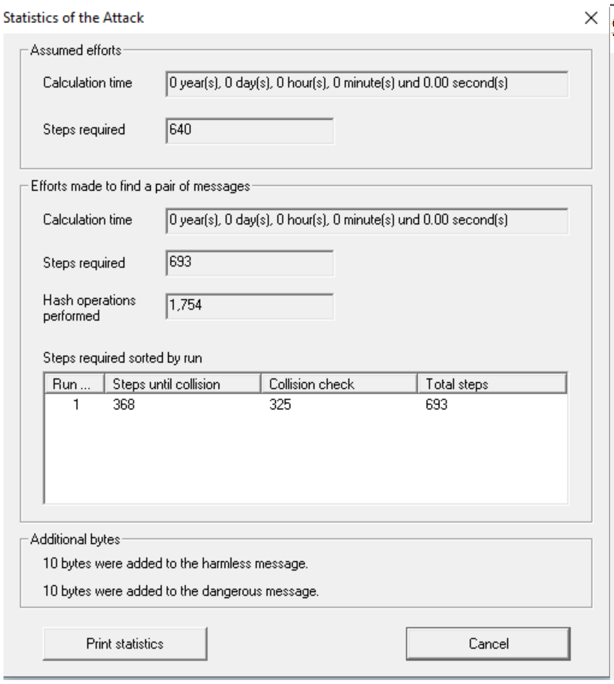
30



CrypTool

The attack was successful: Two different messages were found where the message hash is equal for the first 30 bits.

Statistics of SHA-1



Statistics of the Attack

Assumed efforts

Calculation time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.00 second(s)

Steps required: 640

Efforts made to find a pair of messages

Calculation time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.00 second(s)

Steps required: 693

Hash operations performed: 1,754

Steps required sorted by run

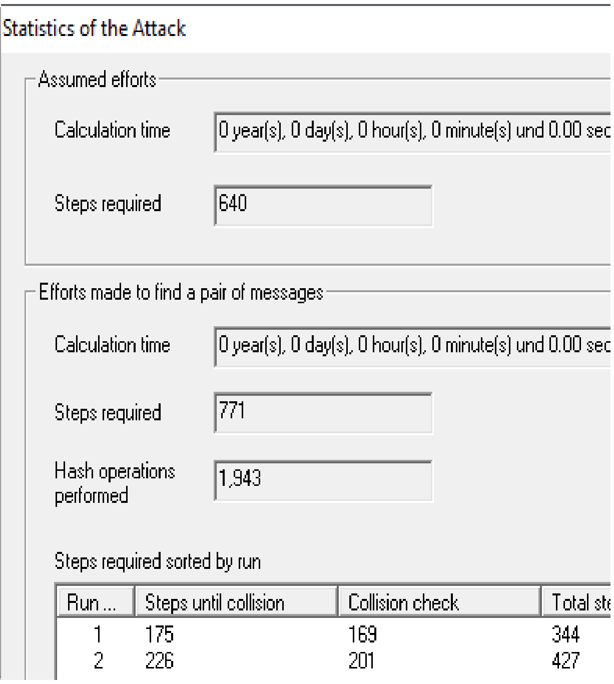
Run ...	Steps until collision	Collision check	Total steps
1	368	325	693

Additional bytes

10 bytes were added to the harmless message.

10 bytes were added to the dangerous message.

Statistics of MD5



Statistics of the Attack

Assumed efforts

Calculation time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.00 sec

Steps required: 640

Efforts made to find a pair of messages

Calculation time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.00 sec

Steps required: 771

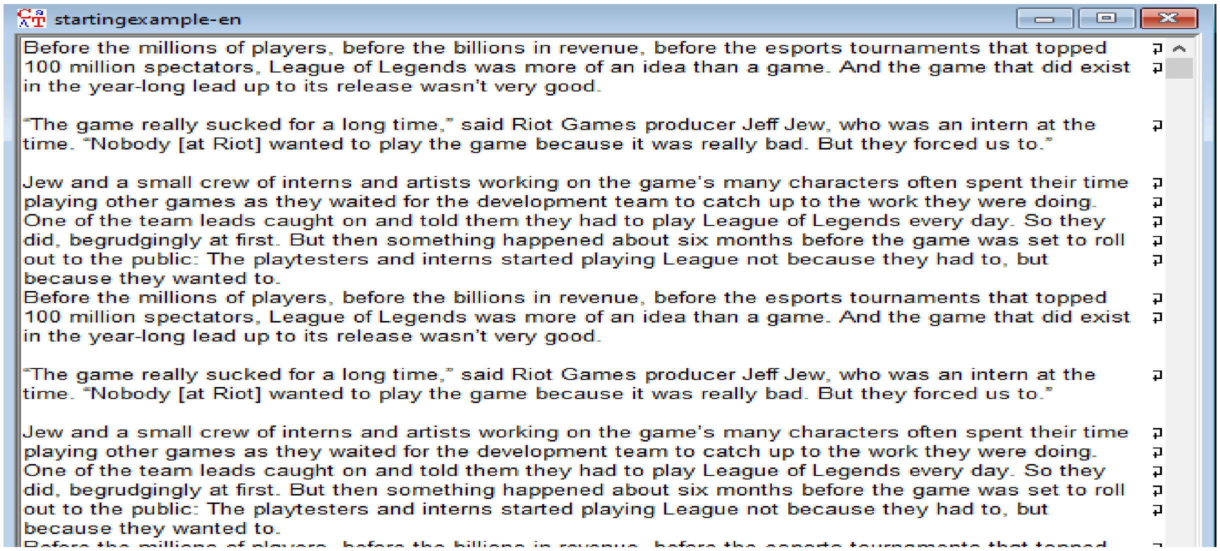
Hash operations performed: 1,943

Steps required sorted by run

Run ...	Steps until collision	Collision check	Total ste
1	175	169	344
2	226	201	427

3. **Perform the attack again using a larger text file (at least a few megabytes).**

= > I used 5.51 mb of text file as shown below In order to perform the attack again with the larger text.



startingexample-en

Before the millions of players, before the billions in revenue, before the esports tournaments that topped 100 million spectators, League of Legends was more of an idea than a game. And the game that did exist in the year-long lead up to its release wasn't very good.

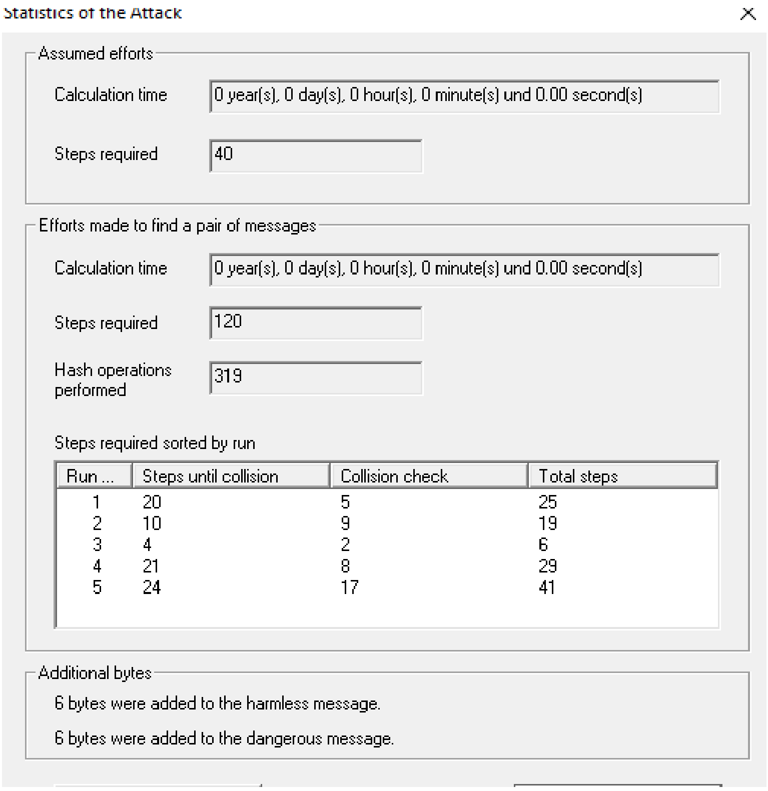
"The game really sucked for a long time," said Riot Games producer Jeff Jew, who was an intern at the time. "Nobody [at Riot] wanted to play the game because it was really bad. But they forced us to."

Jew and a small crew of interns and artists working on the game's many characters often spent their time playing other games as they waited for the development team to catch up to the work they were doing. One of the team leads caught on and told them they had to play League of Legends every day. So they did, begrudgingly at first. But then something happened about six months before the game was set to roll out to the public: The playtesters and interns started playing League not because they had to, but because they wanted to.
Before the millions of players, before the billions in revenue, before the esports tournaments that topped 100 million spectators, League of Legends was more of an idea than a game. And the game that did exist in the year-long lead up to its release wasn't very good.

"The game really sucked for a long time," said Riot Games producer Jeff Jew, who was an intern at the time. "Nobody [at Riot] wanted to play the game because it was really bad. But they forced us to."

Jew and a small crew of interns and artists working on the game's many characters often spent their time playing other games as they waited for the development team to catch up to the work they were doing. One of the team leads caught on and told them they had to play League of Legends every day. So they did, begrudgingly at first. But then something happened about six months before the game was set to roll out to the public: The playtesters and interns started playing League not because they had to, but because they wanted to.
Before the millions of players, before the billions in revenue, before the esports tournaments that topped

MD2 8bit



Statistics of the Attack

Assumed efforts

Calculation time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.00 second(s)

Steps required: 40

Efforts made to find a pair of messages

Calculation time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.00 second(s)

Steps required: 120

Hash operations performed: 319

Steps required sorted by run

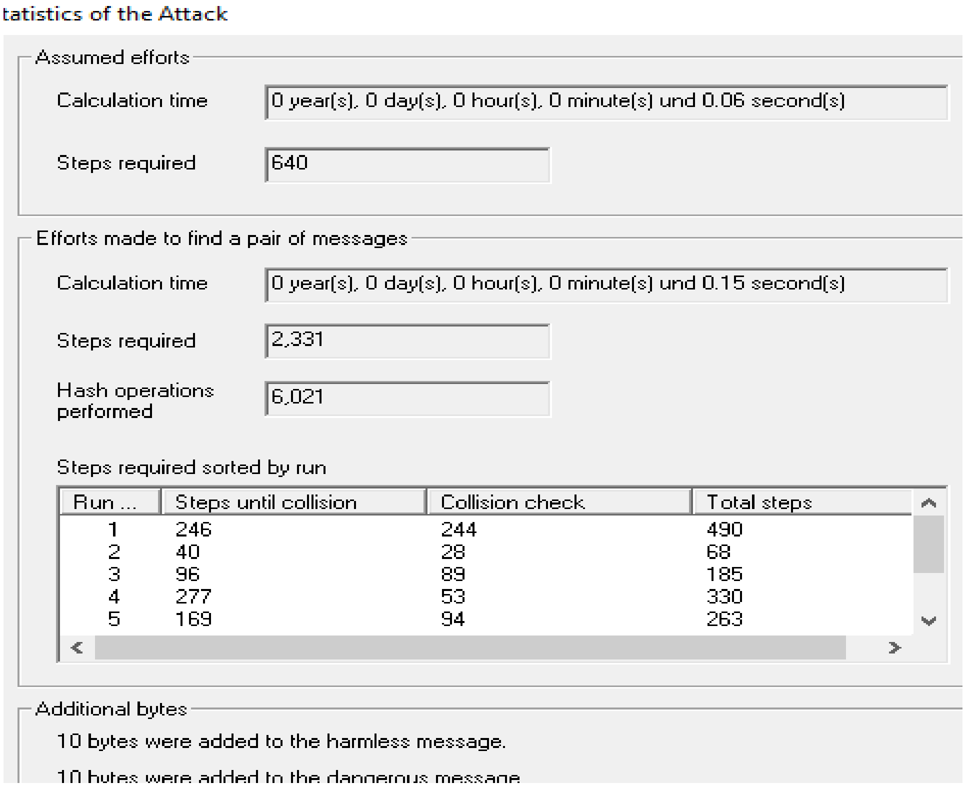
Run ...	Steps until collision	Collision check	Total steps
1	20	5	25
2	10	9	19
3	4	2	6
4	21	8	29
5	24	17	41

Additional bytes

6 bytes were added to the harmless message.

6 bytes were added to the dangerous message.

MD2 16bit



tatistics of the Attack

Assumed efforts

Calculation time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.06 second(s)

Steps required: 640

Efforts made to find a pair of messages

Calculation time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.15 second(s)

Steps required: 2,331

Hash operations performed: 6,021

Steps required sorted by run

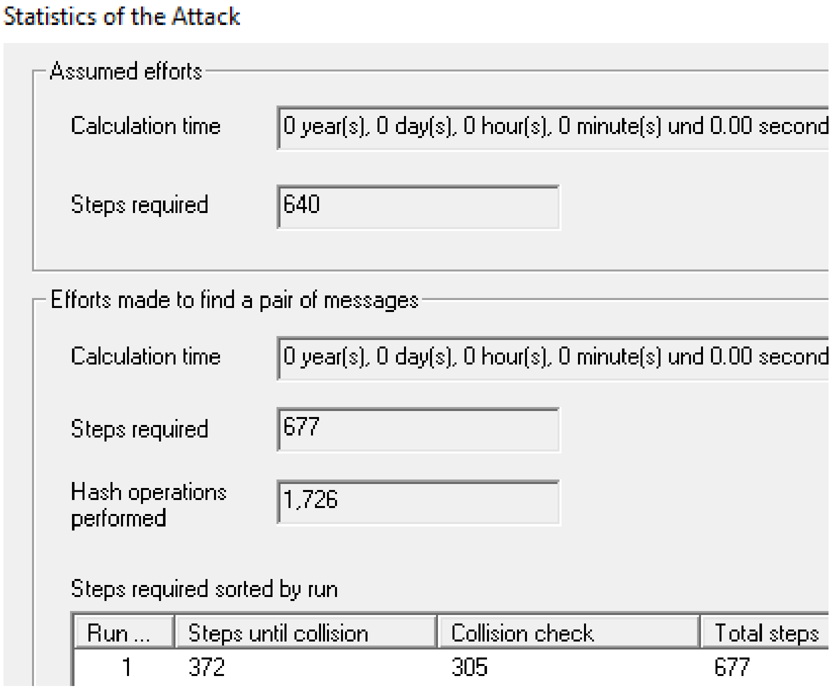
Run ...	Steps until collision	Collision check	Total steps
1	246	244	490
2	40	28	68
3	96	89	185
4	277	53	330
5	169	94	263

Additional bytes

10 bytes were added to the harmless message.

10 bytes were added to the dangerous message

MD5 16



Statistics of the Attack

Assumed efforts

Calculation time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.00 second

Steps required: 640

Efforts made to find a pair of messages

Calculation time: 0 year(s), 0 day(s), 0 hour(s), 0 minute(s) und 0.00 second

Steps required: 677

Hash operations performed: 1,726

Steps required sorted by run

Run ...	Steps until collision	Collision check	Total steps
1	372	305	677

II. Questions:

1. **How does changing the key length affect the time of the attack?**

= > As we saw from the above exercises changing key length didn’t affect much at the statistics of the attack. Just a steps are increased and observed a bit difference in the calculation time.

2.Does the selection of the hash function affect the time of the collision search task(attack)?

= > As we can see from the above table, since we keep the same Significance bit length but change the algorithm, we observed at the statics that MD5 function has more steps than the MD2 function. But its not that big difference we can observe.

3.What is advantage of an attack(finding a collision whose aim is to modify two documents than one?

4.Can the hash function be regarded as safe? If so, for which parameters?

= > Secure Hash Algorithms, also known as SHA, are a family of cryptographic functions designed to keep data secured. It works by transforming data using a hash function. Consist of bitwise operations, modular additions, and compression functions.

Although originally designed as a cryptographic message authentication code algorithm for use on the internet, MD5 hashing is no longer considered reliable for use as a cryptographic checksum because security experts have demonstrated techniques capable of easily producing