암호?

고전/근대 암호

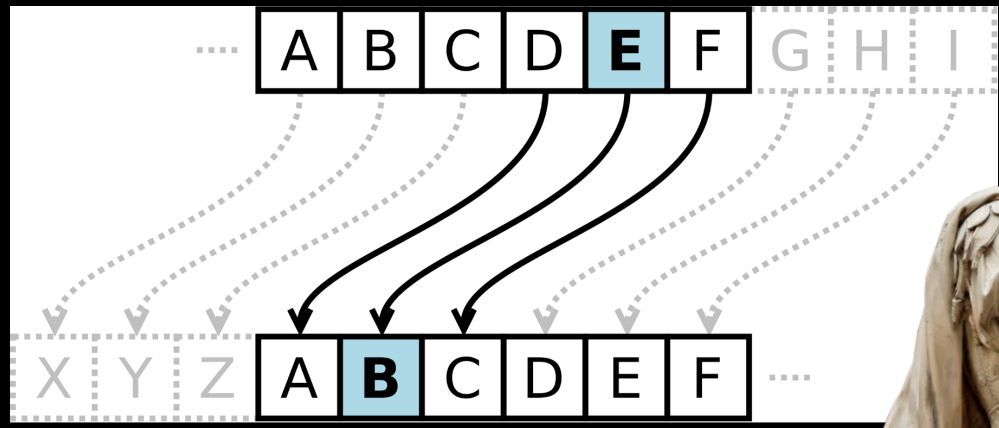
RUSH HOUR 3

PRISON BREAK

고전/근대 암호

Scytale

고대 그리스 스파르타군 사용



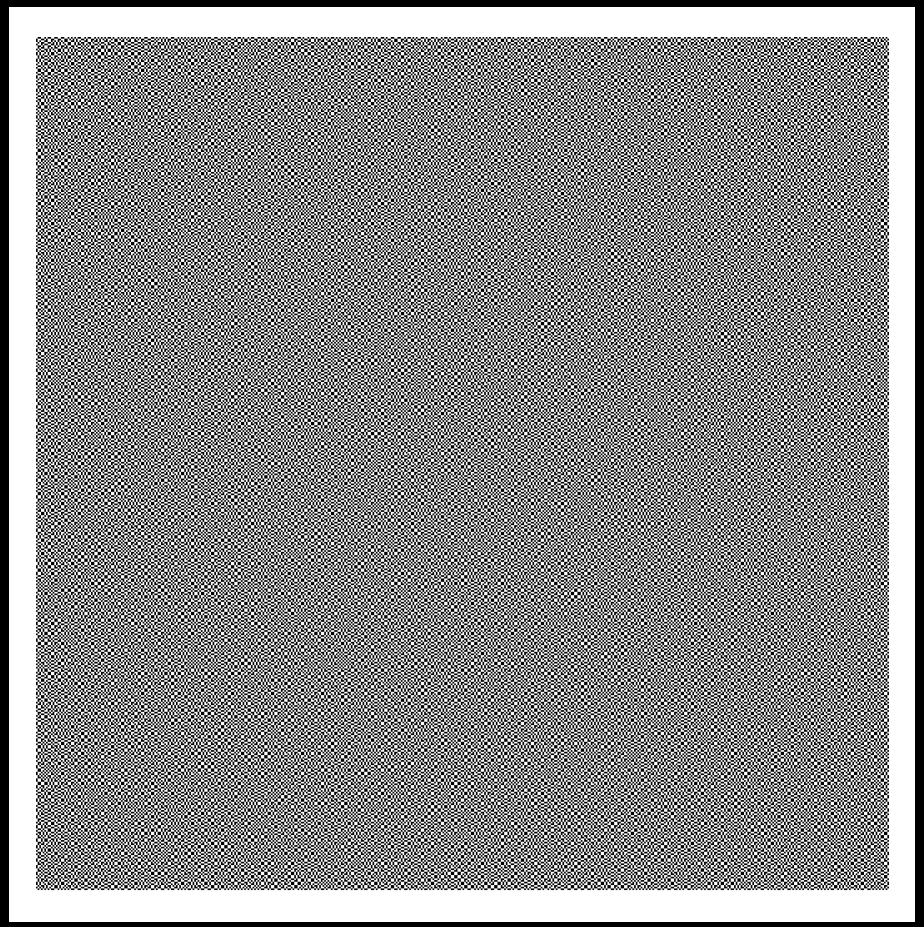
Julius Caesar

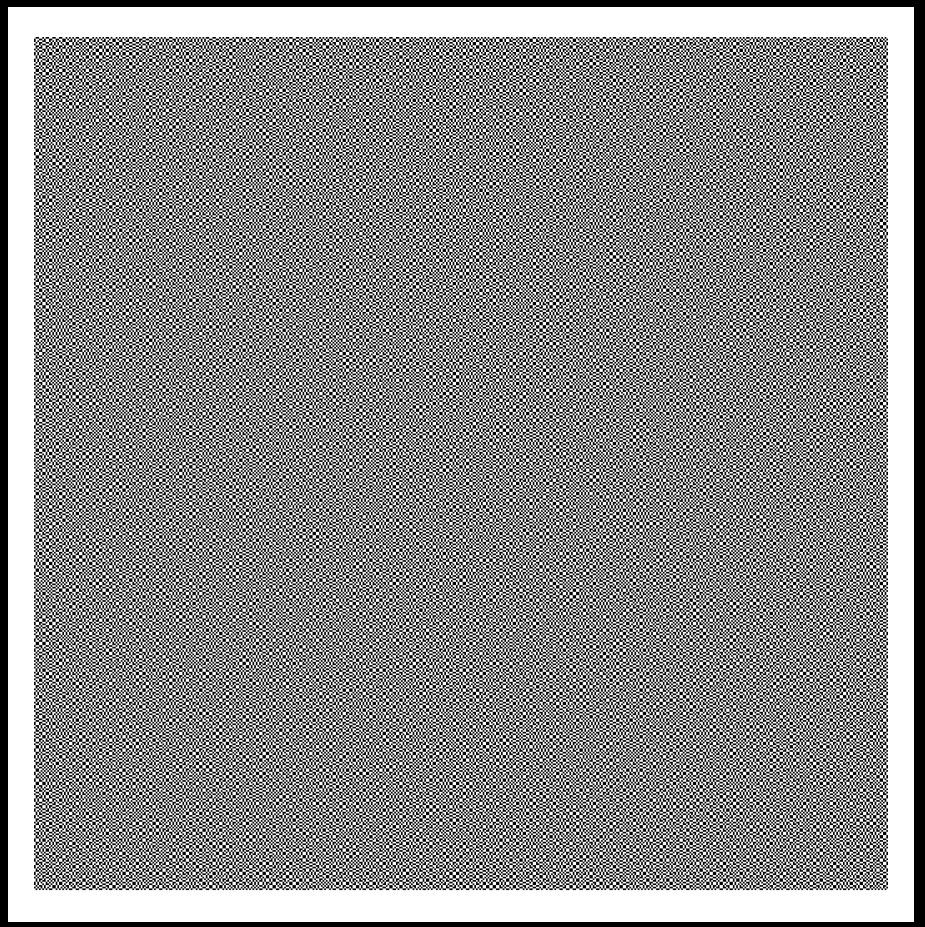
Nicolas Coustou.

Louvre Museum.

고전/근대 암호

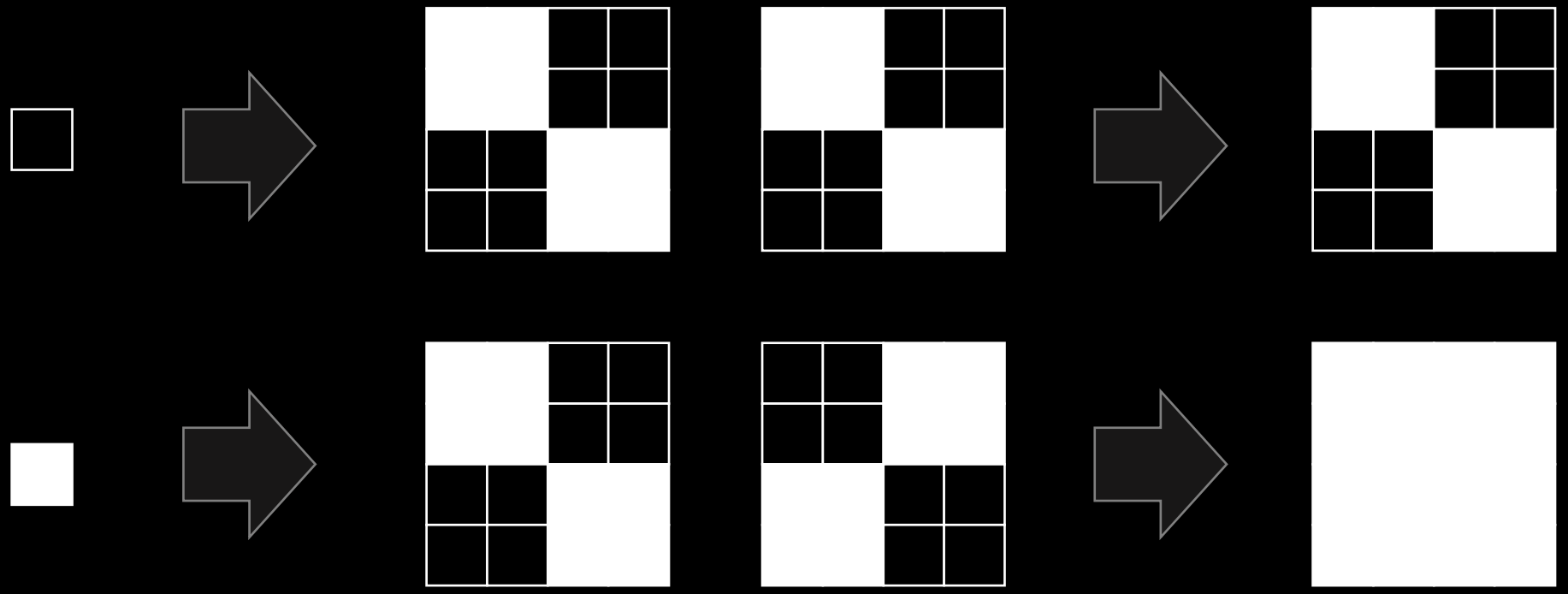
Visual Cryptography





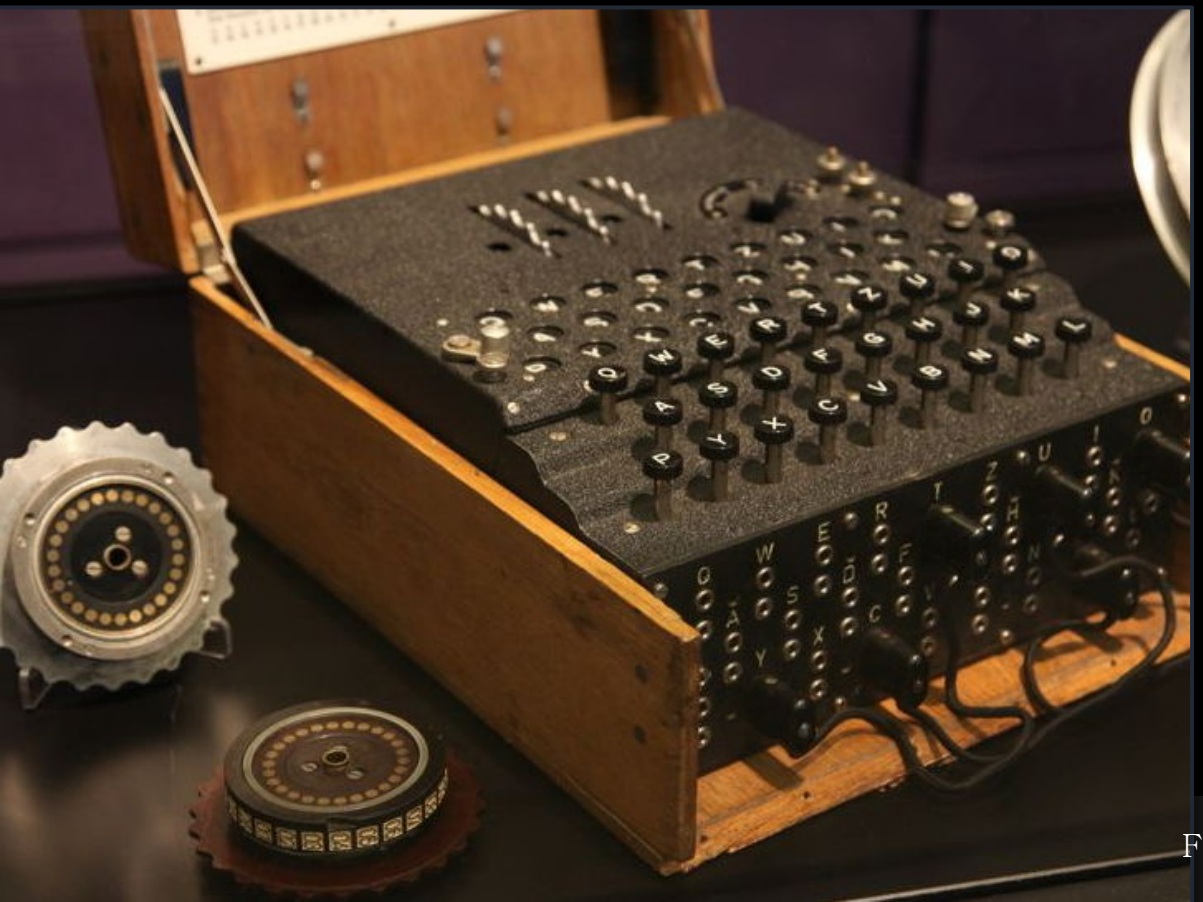
고전/근대 암호

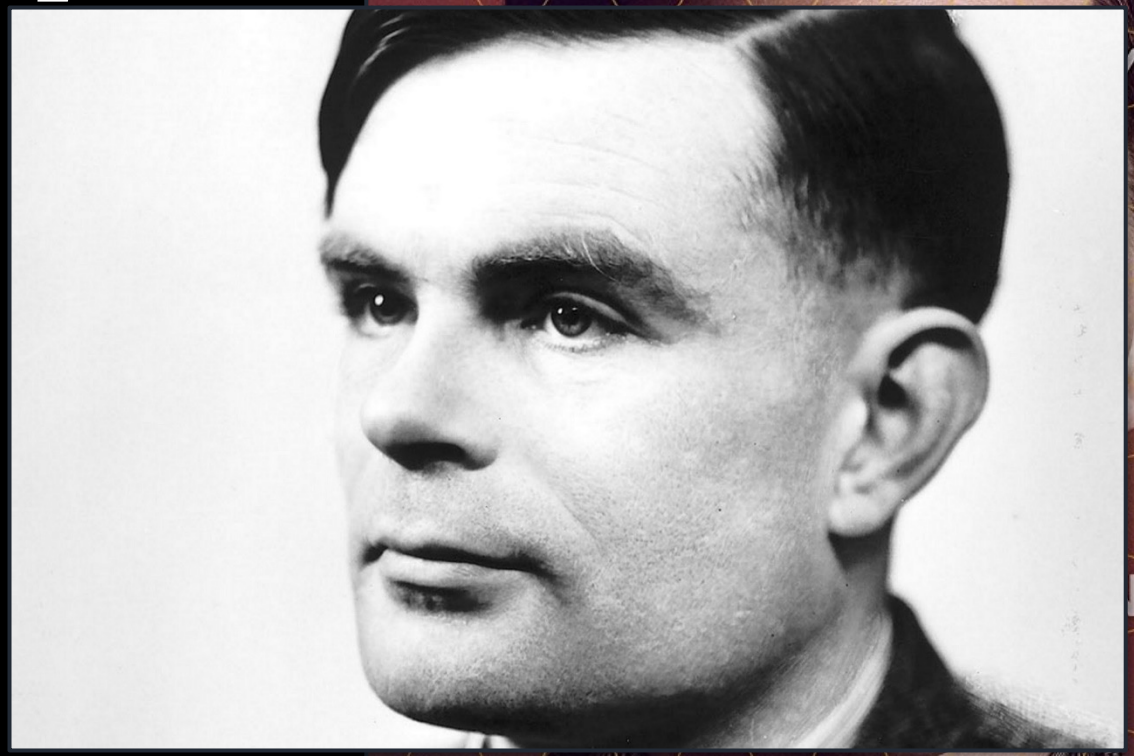
Visual Cryptography



고전/근대 암호

158,962,555,217,826,360,000 = 2^{68}





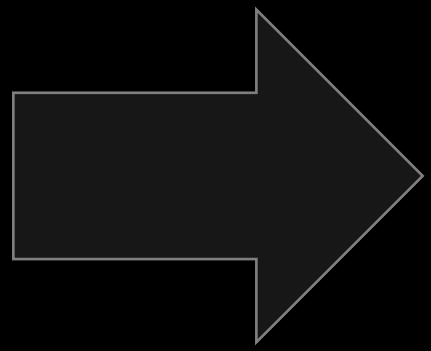
현대 암호의 기능 (목적)

고전/근대

정보

은닉

기술



현대

정보

보호

기술

현대 암호의 기능 (목적)

기밀성
Confidentiality

인증
Authentication

무결성
Integrity

부인 봉쇄
Non-repudiation

현대 암호의 기능 (목적)

기밀성
Confidentiality

비인가 사용자는 정보를 알 수 없다.

In my younger and more vulnerable years my father gave me some advice that I've been turning over in my mind ever since.

"Whenever you feel like criticizing anyone," he told me, "just remember that all the people in this world haven't had the advantages that you've had."

He didn't say any more, but we've always been unusually communicative in a reserved way, and I understood that he meant a great deal more than that. In consequence, I'm inclined to reserve all judgements, a habit that has opened up many curious natures to me and also made me the victim of not a few veteran bores. The abnormal mind is quick to detect and attach itself to this quality when it appears in a normal person, and so it came about that in college I was unjustly accused of being a politician, because I was privy to the secret griefs of wild, unknown men. Most of the confidences were unsought—frequently I have feigned sleep, preoccupation, or a hostile levity when I realized by some unmistakable sign that an intimate revelation was quivering on the horizon; for the intimate revelations of young men, or at least the terms in which they express them, are usually plagiaristic and marred by obvious suppressions. Reserving judgements is a matter of infinite hope. I am still a little afraid of missing something if I forget that, as my father snobbishly suggested, and I snobbishly repeat, a sense of the fundamental decencies is parcelled out unequally at birth.

w. key

암호(Encryption)

00734C8D9A084D103E7F79D86F2886750B3DFE4D5DCCAD08555FCA0E18E5867E0135E98B922A28461B0BA4C36DA674A7AF26999
DB8F0B5AC5AF9DD859AF332F5FE3972CD4FD96861011DE3239519FDB80458079489CE290D474FB1223D23E548D9F7859428D4B7
34118493F624612FF7C589DFD40B688EFCB980414425EBC5974A641582C741F83665D265C6B882EC47C1DD276765A614064E99F21
49B5134AA3AC43982F2CBBB5D1B46624C230944E65DCF03F4B67613CA1A1F9915ADE8B89CFAFFF89F5A78C22AC05F0976079D448
B46A034C0F6FD378C2C92C7036AA10E2FA85563C983DC21208270365316D9D3A5FBF7085196613F359A2ED839F7A799A009DF56F
29259681088BF6B798735E532BE1A8DDC6E69C841EE7FACE29CA249418BD6BA68523E4E404793540A73696E31BA99D61D545BBE
942990435B8736CD4D2C5498470A75E884A32F2114F42FFC3C7A831834C1AC400008F5C38D7736A05D7AB9A1E78CE796655F2DA3
98342E9770E4A90ACA10B4A293374A186376A2934E41BFCD849EC3EC8A4F4D5F7087ECCD466F9A9BE4DAB3E852791E16AA0B529
7A32E9DD21B06F5C4D0E58FA3ACE2A530EB02474984303F358D2A7B99762ADFA46A89DD34FAC388F5AD4821EF203B22FB17994B
6BE0E8134627BCC3713D7D7BDA2C68D00294DABD5ACF1065CA81F9ED987F04B4FDE22095BC3BEBEC2D2DECD03CDCB2BDA733B
4FC25F9BD865E82A26D4C059D964585CC81F3355E4442E8C1630DAF92002988C9688E54EB4C9878F9930A4D1941BBB65D42742C1
B22975C5789B9FD9E5356E9EF5B132A4E9F0293A0F7F5F45419B32A631D0E5210FEAA49D8F790C36900CE59E0D4842719951243A3
E1AE079176DA35EDC9A9566692C2A4649CEA3E203E0DB765E9D4EB91D84D5F0521753D988D4927A0DAF5C8C2415629D4F5516A9
4D95131224A856A33136BA60589F9CFAF6FC26D075E6D0DC308492631C0FD29734D7889839E62D5C98B4290464F321B1B3997C68
F38C871D55337D37CE3C4CC6D13BFFC3259B55943ABF8D6B0377B49D7612BDD5E735CF1D8BFC6FDDBAE43C8CEA6AB4B25C3B67
AA26F050C72C25162D0348BBC76562ACBED50D535124620830110737 9A64E7EE6675A836A77665263E52AAC67DF25FE1772B7916
84D1E31530887CE70E4F5B052E5304601BE72BAD90D78A610D70512BC52CD75A89C5BEE592CD023C73709E7CD3367D668EB57C0
071F71B7CF36CD21A2BB64712BBB5EB5462CC9AB2DF49B41E0A60D377C6A581F5823A34606C7FC58A8E596D96650725EA3750F5
C55C5B6A53482109DEB7C9B62FEAC8A96103F19C2F27FBADEAA8B9B673E140919D2B681231AF653E7FE6B92315403E8033BBE580
838B4C09488C4DE4DDCC1A3358E82226D85D7135F9002E81DB08A00F96A81BD6804F4238C03AA1795071BF707256873E6604873
C764DA1BA27B0AF004B3E61AA9809561CA367FFDD110F7E18DA887BC0A74C3577E584B0BA73B83ABAEAE880CA416237E3638E10
EB25D4C9EC72A435BC75519E1ABB6E9BB898187494DC03B4D9F40DB81F795E7896B4FCC924BA7E244BFFDBBA46A48FF57C694C2
C6B9303293E101944F5F415EE3B511532A660A85539493308488B33CC54783D996D84B784CBE32574E2831D82AAF3BDB281FF9CF
EB5060FE96CB4B86BFB24C4CB55F085A1BD224E3DC889375DF747D449BB70E26EA791910E1923F88E9D30D1BF2AFBC69683DBCC
FE59FCA15B87808532CDA3D4098E34931F0D5B967C8F6F3DC507733990BE6C2E65C2B5AB69514A6FD77C7358DE98AE5555406017
89DA27024DB735F5B0C437B46AAEB5E394A41C41EF45C984878957C599CA1B46FF9A1B7F929BBB25B666352FA44D6AE6A5B5876
4D8008B55F3D8BB052BD93924F1AC9F0837A37D201C0FF32818E9D64E8D47D701F150DC07A0DDB830788B7D8BF3246835C87EEA
ADD2A2449FB51793D0986BCF1D2011D79B619E37132F84B34913E974BB86A818DCC9E18EBC06D1EF691AC723C3D59D18F0CB08C
7583D56D534FED3056A19B75EF794876F0C77AA090A27B4CA8C28C7E4433C6CEA48C7DC09A92AA7F2C

현대 암호의 기능 (목적)

무결성
Integrity

비인가 사용자는
정보를 임의 수정 또는
생산할 수 없다.

메시지 인증 부호 w. key

전자 서명 w. key

해시 함수 w/o key

현대 암호의 기능 (목적)

인증
Authentication

사용자(또는 정보) 식별

메시지 인증 부호 w. key
(인가 사용자 간)

전자 서명 w. key
(누구나)

https://heimdalsecurity.com/blog/biometric-authentication/

현대 암호의 기능 (목적)

부인 봉쇄
Non-repudiation

행위에 대한 부인 불가

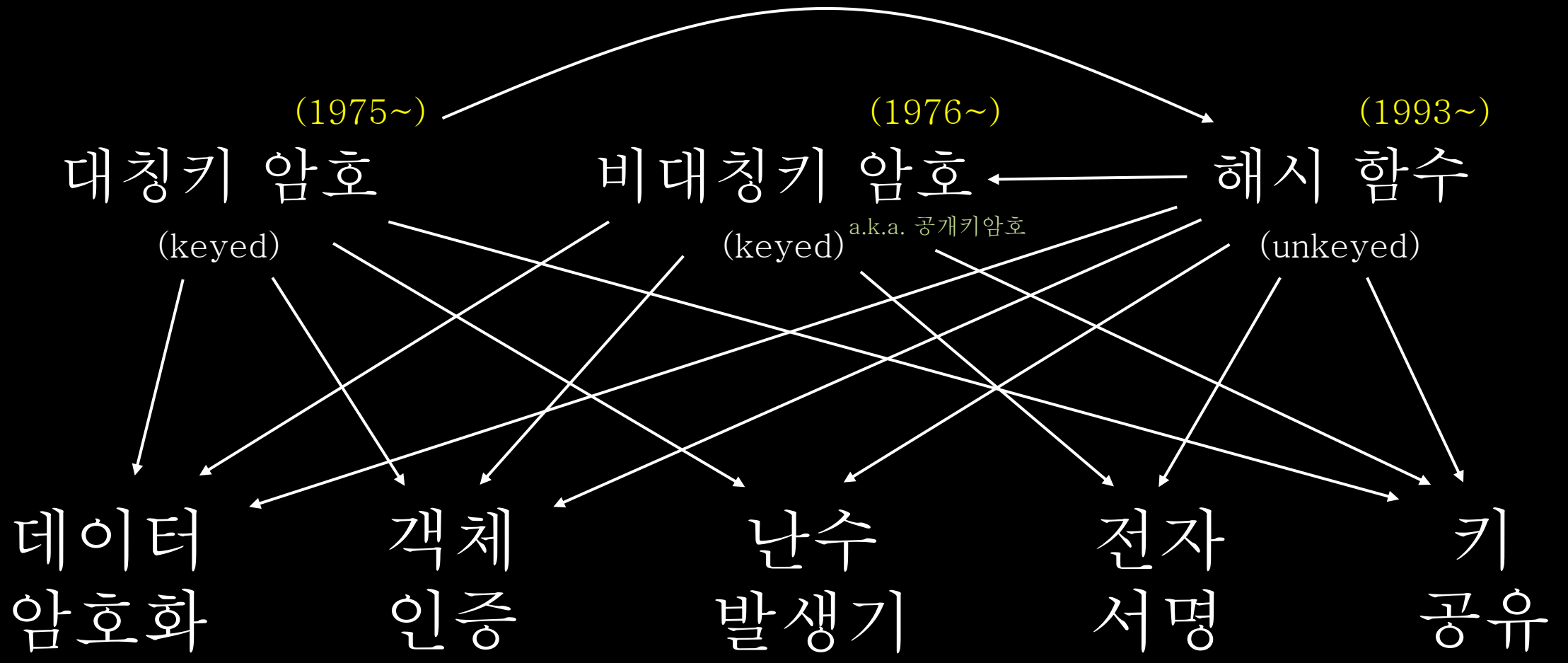
전자 서명
(누구나)

w. key

오리발?

http://blog.naver.com/PostView.nhn?blogId=bonggui8502&logNo=110142596865

암호의 분류


(1975~)
(1976~)
(1993~)
대칭키 암호
비대칭키 암호
해시 함수
(keyed)
(keyed)
a.k.a. 공개키암호
(unkeyed)
데이터 암호화
객체 인증
난수 발생기
전자 서명
키 공유

공격 목표

Key Recovery

Attack

(any information about key)

Forgery

Attack

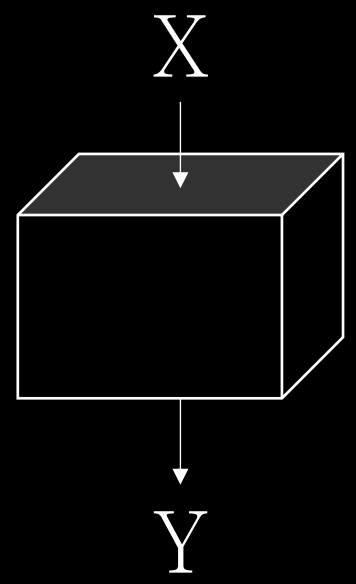
Message Recovery

Attack

(any information about message)

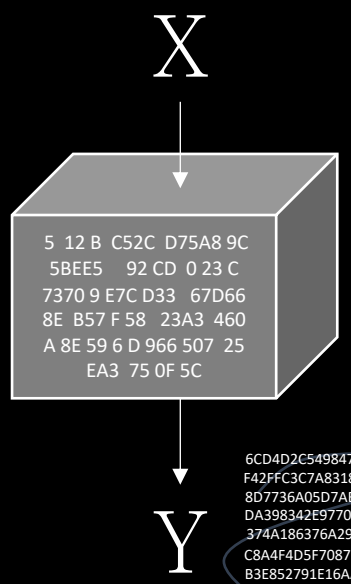
공격 환경

Blackbox



ciphertext or mactag

Graybox



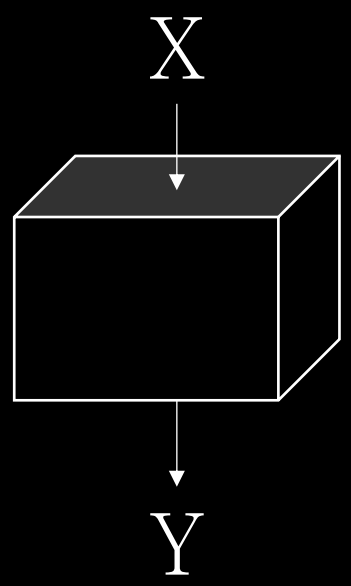
6CD4D2C5498470A75E884A32F2114
F42FFC3C7A831834C1AC400008F5C3
8D7736A05D7AB9A1E78CE796655F2
DA398342E9770E4A90ACA10B4A293
374A186376A2934E41BFCD849EC3E
C8A4F4D5F7087ECCD466F9A9BE4DA
B3E852791E16AA0B5297A32E9DD21
D865E82A26D4C059D964585CC81F3
355E4442E8C1630DAF92002988C968
8E54EB4C9878F9930A4D

Whitebox

6CD4D2C5498470A75E884A32F2114F42FFC3C7A831834C1AC400008F
8D7736A05D7AB9A1E78CE796655F2DA398342E9770E4A90ACA10
374A186376A2930348BBC76562ACBED50D5351246208
107379A64E7EE6675A836A77665263E52AAC67DF25FE1
772B791684D1E31530887CE70E4F5B052E5304601BE72BAD
90D78A610D70512BC52CD75A89C5BEE592CD023C73709E7
CD3367D668EB57C0071F71B7CF36CD21A2BB64712BBB5EB5
462CC9AB2DF49B41E0A60D377C6A581F5823A34606C7FC58
A8E596D96650725EA3750F5C55C5B6A53482109DEB7C9B62
FEAC8A96103F19C2F27FBADEAA8B9B673E140919D2B68123
1AF653E7FE6B92315403E8033BBE580838B4C09488C4DE4D
DCC1A3358E82226D85D7135F9002E81DB08A00F96A81BD6
804F4238C03AA1795071BF707256873E6604873C764DA1BA
27B0AF004B3E61AA9809561CA367FFDD110F7E18DA887BC0
A74C3577E584B0BA73B83ABAEAE880CA416237E3638E10EB
25D4C9EC72A435BC75519E1ABB64E41BFCD849EC3EC8A4F4D5F
7087ECCD466F9A9BE4DAB3E852791E16AA0B5297A32E9DD21D865E8
2A26D4C059D964585CC81F3355E4442E8C1630DAF92002988C9688E5
4EB4C9878F9930A4D

Blackbox Security

Blackbox Security



OW: Onewayness

IND: Indistinguishability

COA: Ciphertext-only Attack

KPA: Known-Plaintext Attack

CPA: Chosen-Plaintext Attack

CPA2: Adaptive Chosen-Plaintext Attack

CCA: Chosen-Ciphertext Attack

CCA2: Adaptive Chosen-Ciphertext Attack

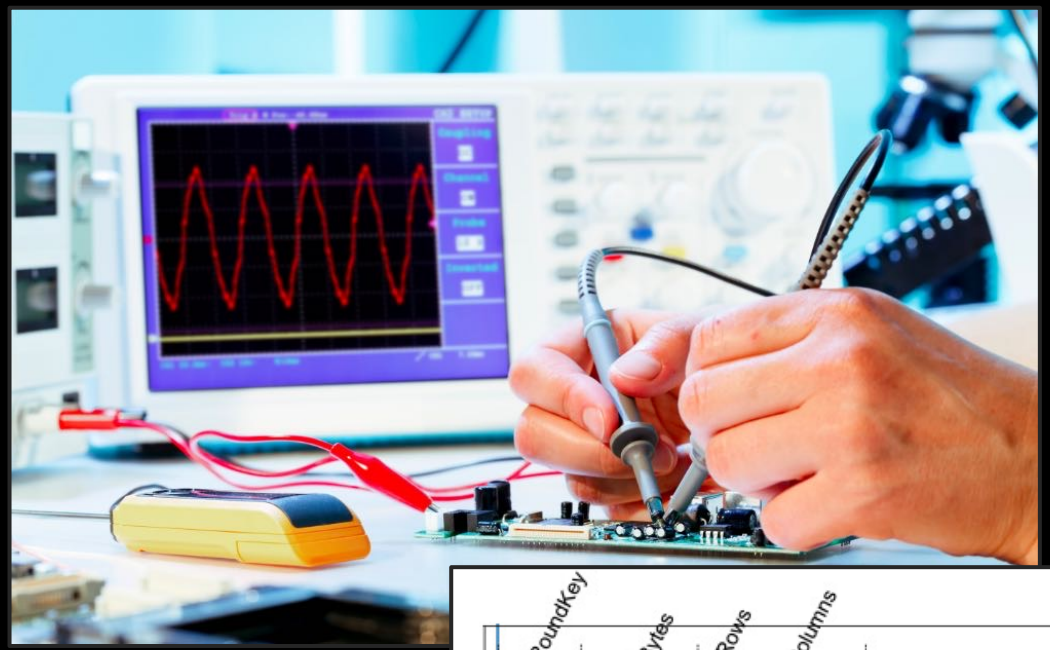
UUF: Universal Unforgeability Forgery

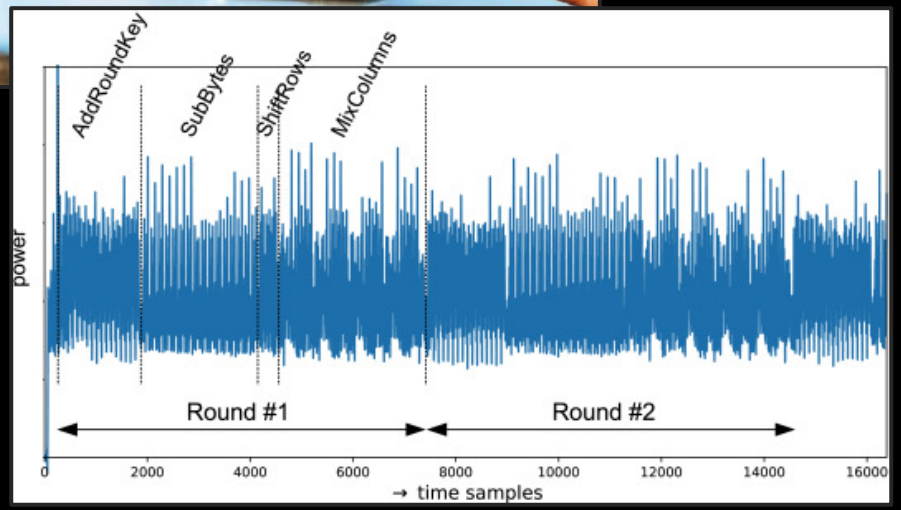
SUF: Selective Unforgeability Forgery

EUF: Existential Unforgeability Forgery

CMA: Chosen-Message Attack

Graybox Security





Whitebox Security

```
…
000649b0  27 a2 84 a6 12 eb cb a3  82 82 94 8f e4 de 48 66  |'.............Hf|
000649c0  12 bf 31 75 c0 f7 13 2a  64 1a f7 24 ef 52 56 49  |..1u...*d..$.RVI|
000649d0  c2 7c 53 9a 56 bb a9 1b  7d 01 3c 79 4a 26 2f 5d  |.|S.V...}.<yJ&/]|
000649e0  e1 e2 bf 52 de 37 8b 6f  3f b5 25 5f 97 56 c1 5a  |...R.7.o?.%_.V.Z|
000649f0  fc 50 65 44 6a e6 24 70  5c 66 d4 4d ac 55 e5 f4  |.PeDj.$p\f.M.U..|
00064a00  af 9d 17 f2 f6 a6 60 b5  72 38 c0 22 cc bd 9b 89  |......`.r8."....|
00064a10  7f 3b b5 bc 32 ba a2 5c  de 8f 4a c9 59 28 c2 76  |.;..2..\..J.Y(.v|
00064a20  4e 43 28 cd fb a8 fb a2  d1 5a 3f 8e d7 5b 02 03  |NC(......Z?..[..|
…
00065bd0  d8 80 6f 70 99 41 c7 2a  a9 a5 7a 33 3e 42 26 3f  |..op.A.*..z3>B&?|
00065be0  c9 90 15 19 5e d7 22 a3  6a 72 98 47 61 02 f1 d0  |....^."jr.Ga....|
00065bf0  3b 22 9b 11 ef 48 d4 8d  b7 e6 24 7e 44 2d 88 6b  |;"...H....$~D-.k|
00065c00  15 96 56 90 f5 db d6 9d  2f eb 7c 43 2c ad a8 4b  |..V...../.|C,..K|
00065c10  e4 fa ed 58 85 21 70 49  c9 41 e1 15 6d 09 56 37  |...X.!pI.A..m.V7|
00065c20  58 dc c6 2a e8 92 14 62  e4 a2 dc 36 98 e2 c6 ad  |X..*...b...6....|
00065c30  00 cf 10 47 cb fa 52 a0  89 ae 9d 73 e6 3b a4 eb  |...G..R....s.;..|
00065c40  00 31 ae 12 92 3d b7 0d  44 d5 e4 66 4f 22 66 e2  |.1...=..D..fO"f.|
…
```

KEYS LOADED INTO MEMORY

일반 구현

```
…
000652c0  bf 88 25 09 ce 83 6f 42  61 65 b8 bd c9 1f 7c c8  |..%...oBae....|.|
000652d0  2f 1d 58 5c ca 73 e6 97  9d 23 52 79 04 b0 2c 40  |/.X\.s...#Ry..,@|
000652e0  bb 6b f1 64 63 68 a3 c5  e5 2f 63 d6 20 73 a6 4e  |.k.dch.../c. s.N|
000652f0  25 92 30 c6 5f f1 20 2b  f3 0b 57 51 47 b2 d8 56  |%.0._. +..WQG..V|
00065300  6e 15 7f ea b9 2b 94 1e  2c 35 90 fd d5 96 62 07  |n....+..,5....b.|
00065310  1e 0b d0 44 95 45 a9 88  97 3f 49 5a ba 7f 5d f8  |...D.E...?IZ..].|
00065320  7e 97 3f e6 e0 fc c9 14  de cd 54 e3 c7 d6 b7 db  |~.?.......T.....|
00065330                                                   |<.P..yo..|
00065340                                                   |40Q......|
00065350                                                   |.......)...W..R|
00065360  07 16 66 33 a9 6c 5f 1e  b4 e4 f9 90 35 a8 bf 8b  |..f3.l_.....5...|
00065370  71 77 47 80 2c 71 5f 35  bb 03 21 aa 1e 90 39 e7  |qwG.,q_5..!...9.|
00065380  eb e4 ec 7e 2a 4a df 47  f6 9a 8c 12 04 8f 24 2f  |...~*J.G......$/|
00065390  3c f7 0f 82 5a 7d a2 a5  21 3c 74 04 62 09 32 25  |<...Z}..!<t.b.2%|
000653a0  3e 0a 70 61 9f 72 ac c8  0c 2c ae 05 8b c6 dc a8  |>.pa.r...,......|
000653b0  af 94 a4 b0 24 8f cf 2e  6b c1 68 8d e2 49 8b 24  |....$...k.h..I.$|
000653c0  c5 b4 89 b8 63 0c ee 34  2d b5 79 59 f8 7f 29 76  |....c..4-.yY..)v|
…
```

NO KEYS LOADED INTO MEMORY

화이트박스 구현

암호 강도 (Security Strength)

안전한 암호?

안전한 암호는 없다.

모든 키를 전수조사할 수 있다면...

만일 키후보 개수 >= 2^{128}라면...

→ 비현실적인 전수조사량

공격자 is "다항식 복잡도"의 알고리듬

암호 강도 (Security Strength)

128비트 강도 암호

키 공간 크기: 2^{128}

(= 전수조사 량 = 핵심암호연산호출횟수)

1초에 1,000,000,000개($2^{29.89}$)의 키를 조사한다면 (함수를 호출한다면)

1년이면 365 x 24 x 60 x 60 x 10^9 = $2^{31.55 + 29.89}$ = $2^{61.44}$

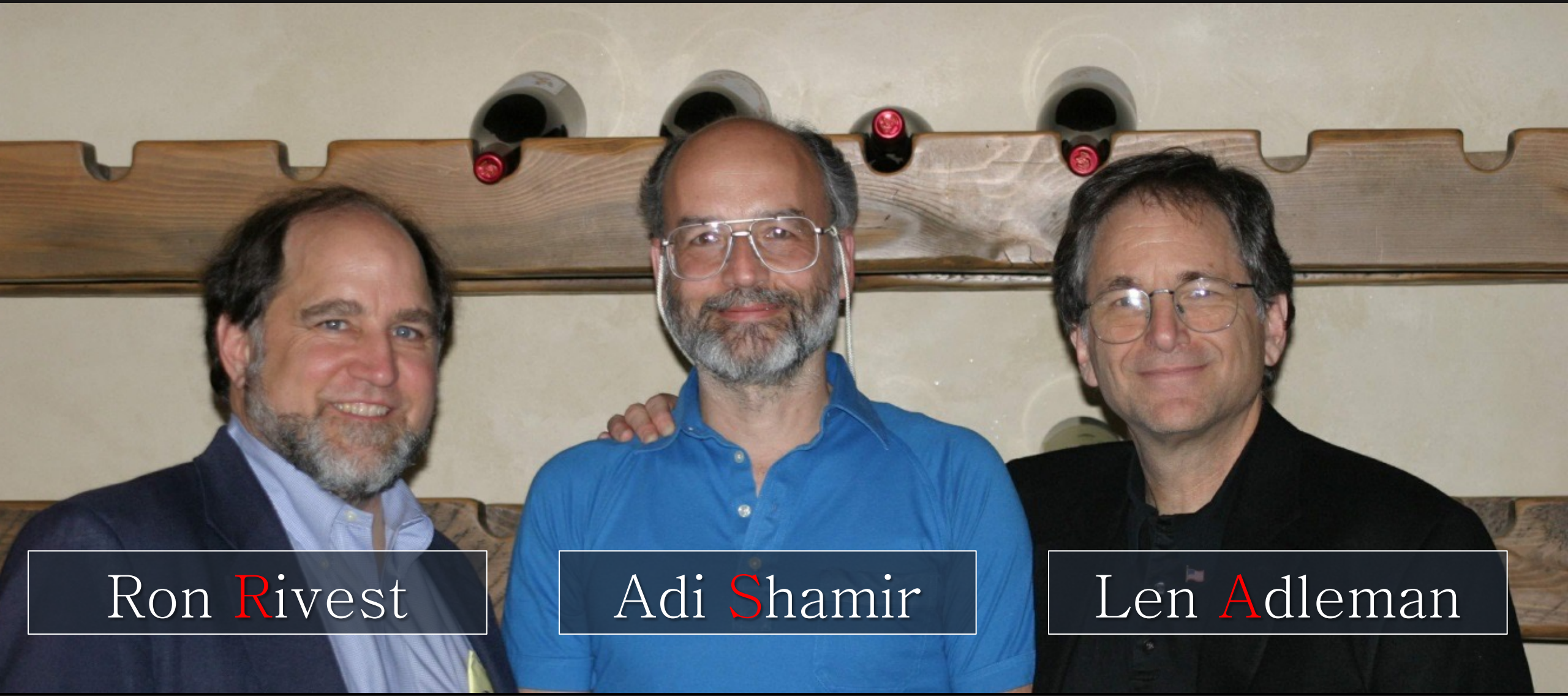
1,000년이면 1,000 x $2^{61.44}$ = $2^{71.40}$

암호 강도 (Security Strength)

단위: 비트

사용 기간	암호 강도	블록암호키	IFP N(=pq)	DLP |G|
2010 <	80		1024	160
2011~2030	112		2048	224
> 2030	128	128	3072	256
>> 2030	192	192	7,680	384
>>> 2030	256	256	15,360	512

RSA (1977)



RSA-n (Textbook)

Key Generation

- Generate two distinct primes p and q
- Compute N = pq
- Choose e such that gcd(e,Φ(N))=1
- Compute d such that ed ≡ 1 mod Φ(N)=(p-1)(q-1)

Public Key Private Key

Encryption

$$C := M^e \bmod N$$

Decryption

$$M := C^d \bmod N$$

RSA-1024

- p = 0x00ff6dbcaef11702ab941a65ecf43ee3aef90d4148e7e76800f31213dee4f43d2a8644544ab91e9a3e581dd06ba879decbd5a239aa4433c6b43273d53636332d43
- q = 0x00f6b23d23bf6ba6b8db8296e647ccba0826dee37a38a0639adf873539c1e1ac6a72a4c9cf0d2036cfad3feb0d08cfe754a2aa29bdabaa98d1c9784021331cb3a3
- N = pq = 0x00f6254a9e1e4482ec2aa3c26dfab64659bfcf8d728277e64cf0780e88b599176f8c9d809b5dc9eced0d18c77a6a6638e0d8230980a9903012d5f68e1795a75c1ef41390d0ca6c20b042e36de43762f5dfc652e43427145f25e32fee74773ac3d68149670d6deb533d904065885c4f8f6679246203ad0377ebd6e15eaa978faaa9

- e (public key) = 3 (0x3)
- d (private key)

0x00a418dc69698301f2c717d6f3fc79843bd53508f701a544334afab45b23bb64f50869006793dbf348b365da519c4425eb3ac20655c660200c8ea45eba63c4e81353f7b9febbf0fa328cd9a0b5fce4e5706eef2a4b59b30d06b5b9c3928aede6d65aeadb4d1a7301750741c6b51cae862eab3aa9bd28c365993ca38637742a8683