Introduction to

Cybersecurity

David J. Malan
malan@harvard.edu

Securing Data

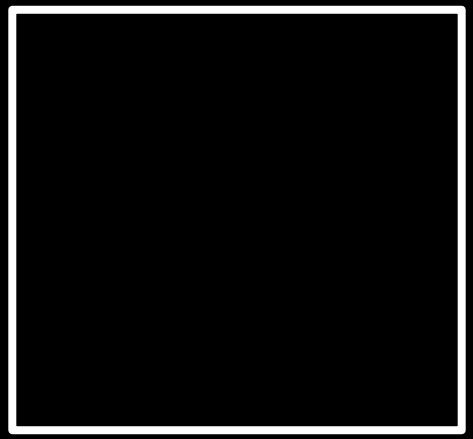
Passwords

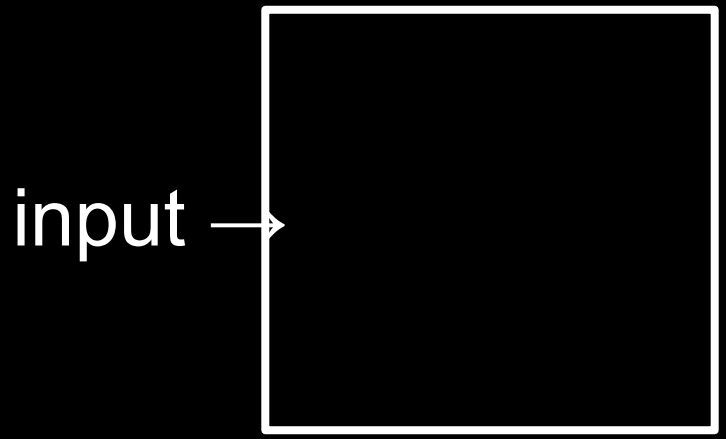
```
alice:apple
bob:banana
...
```

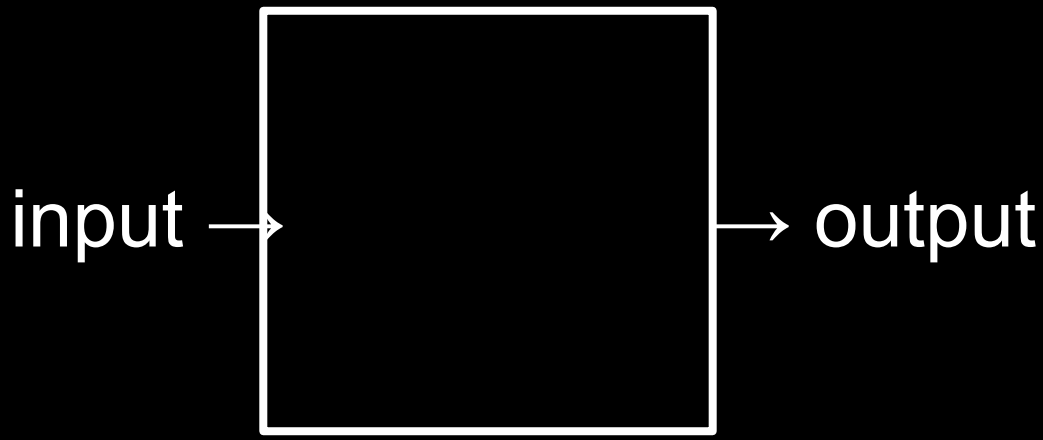
```
alice:apple
bob:banana
...
```

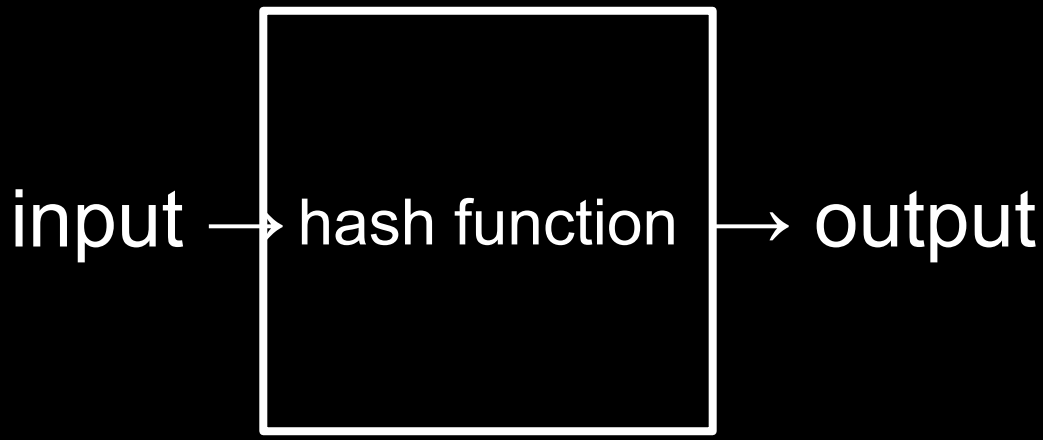
Hashing

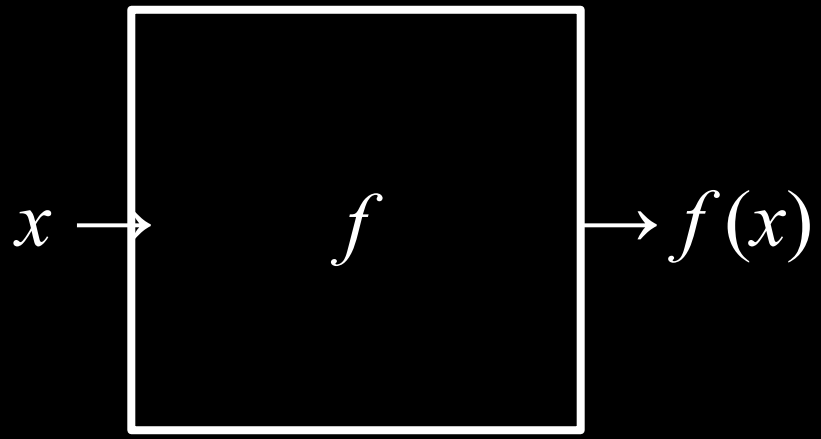
password → hash

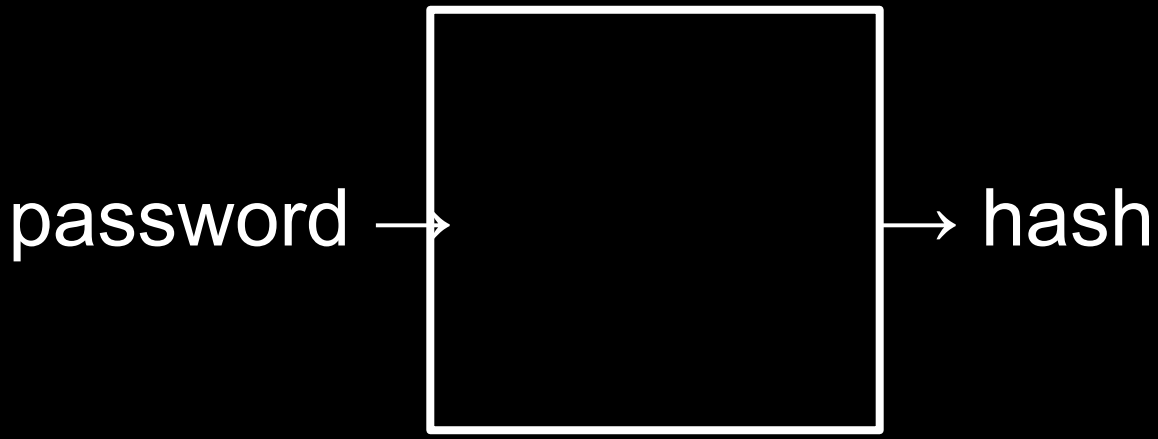


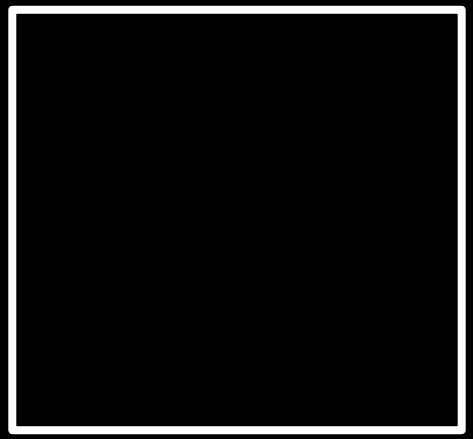

input

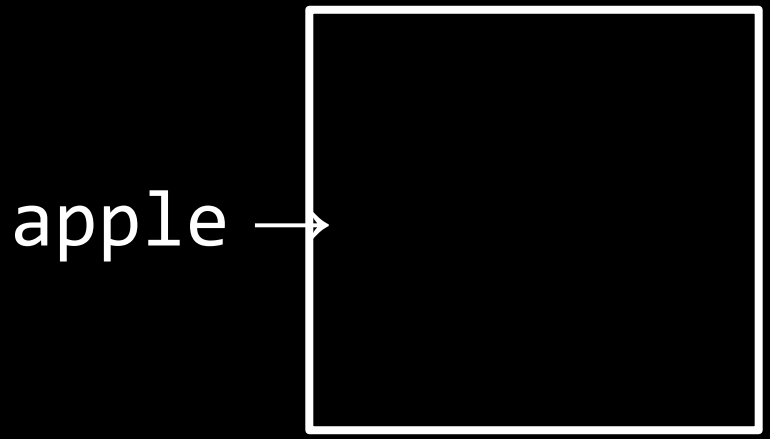

input
output

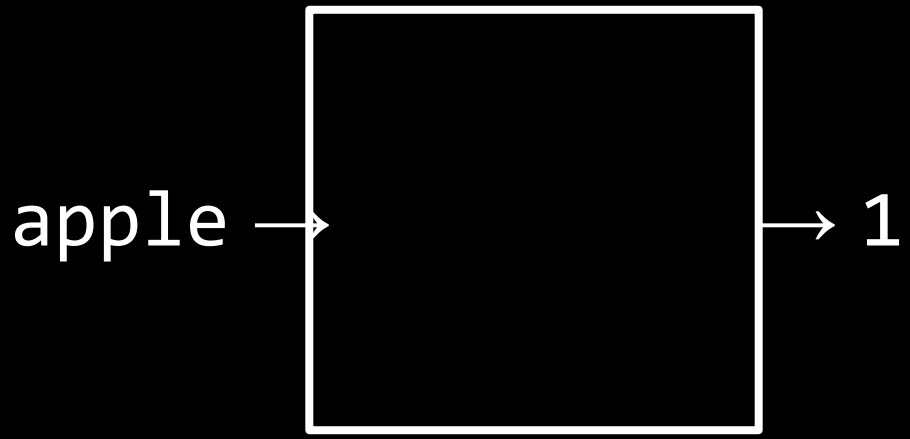

input
hash function
output

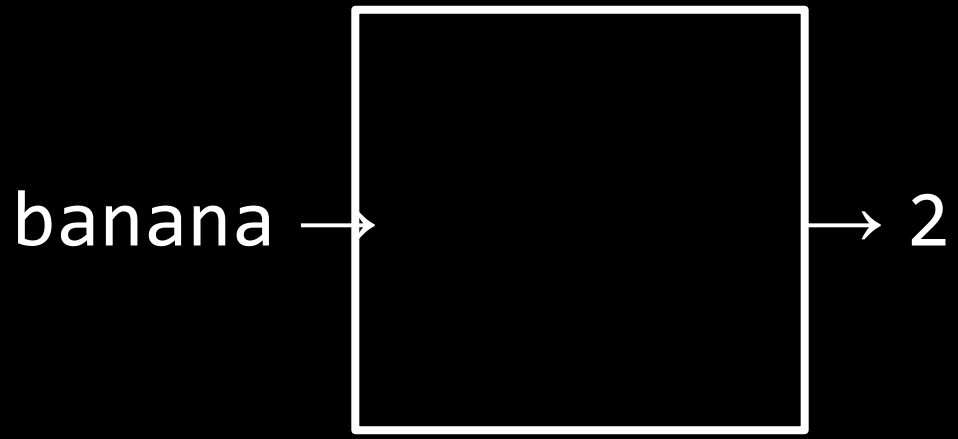

x
f
$f(x)$

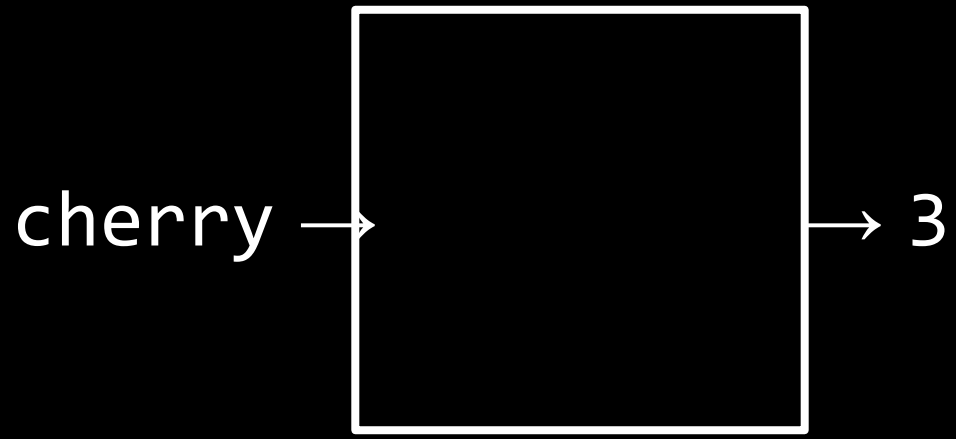

password
hash

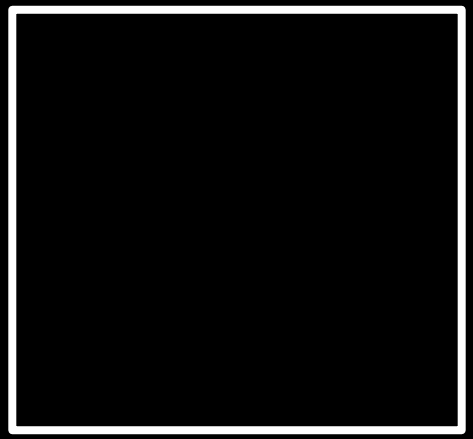


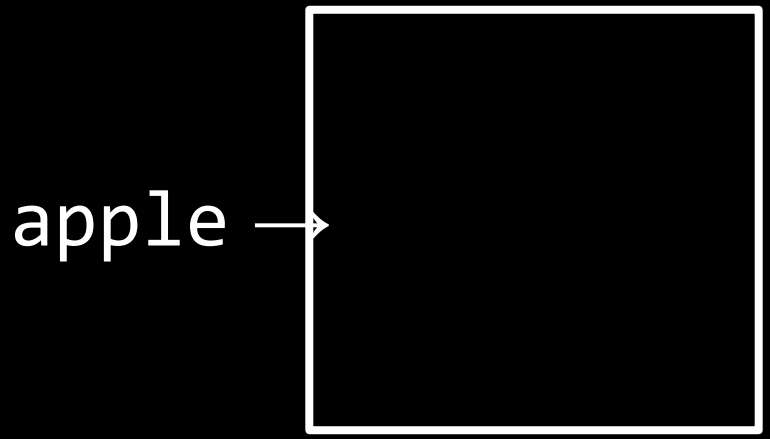

apple

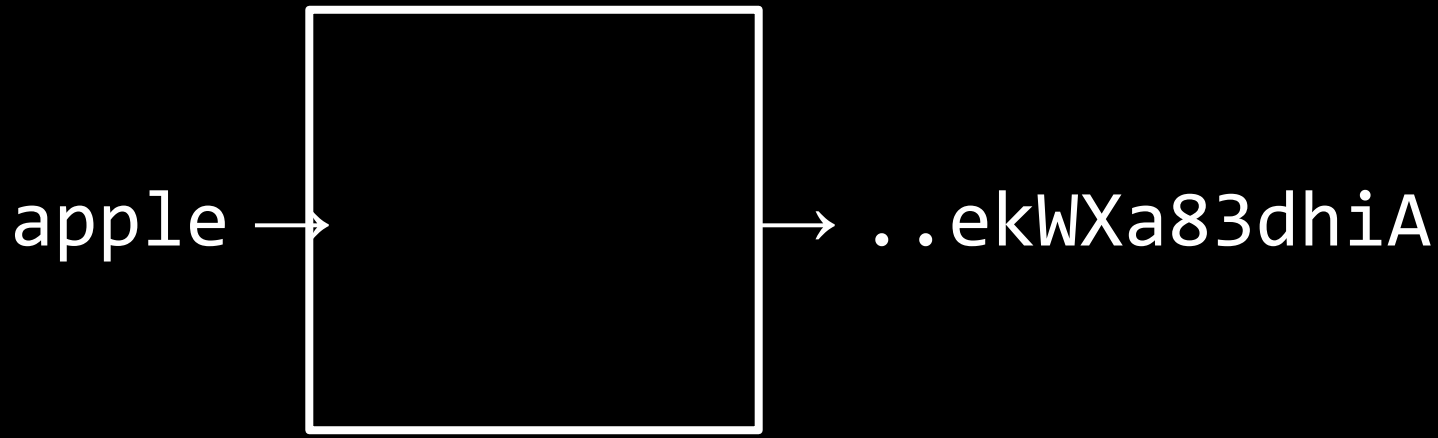

apple
1

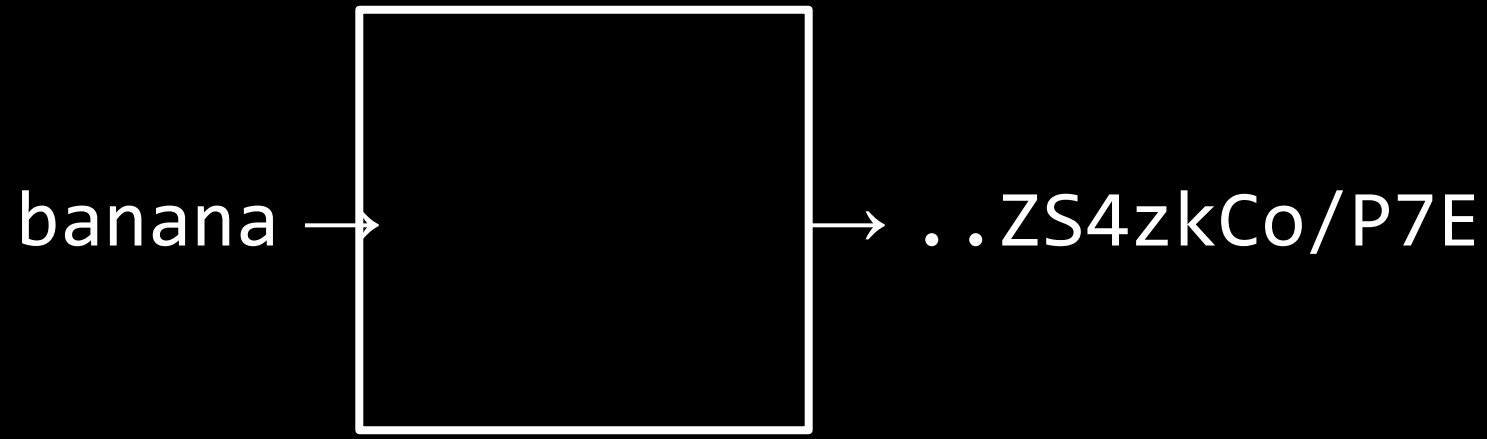

banana
2

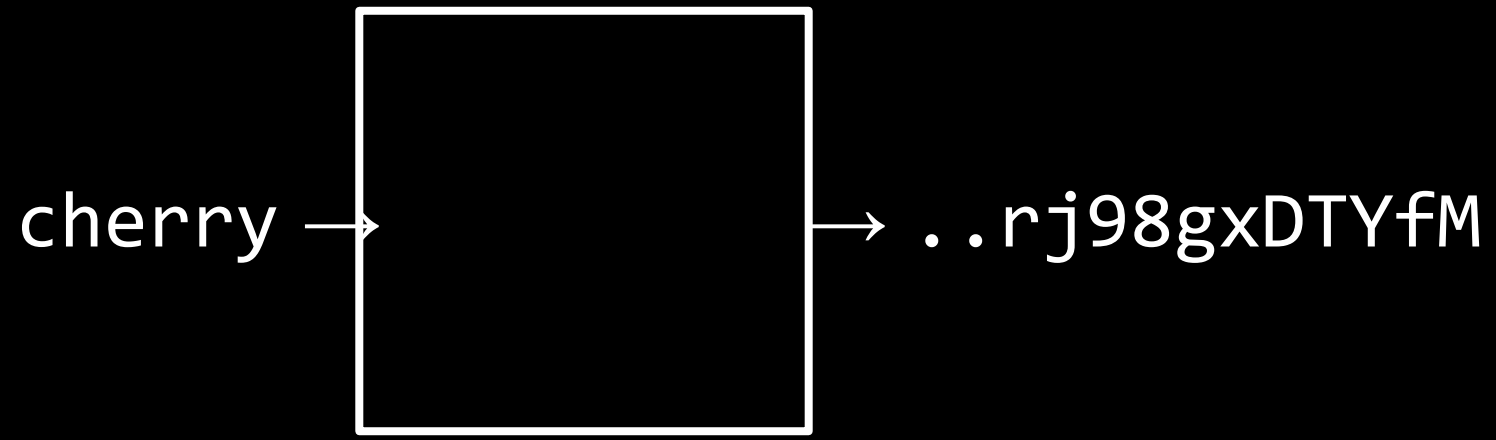

cherry
3




apple


apple
..ekWXa83dhiA


banana
..ZS4zkCo/P7E


cherry
..rj98gxDTYfM

```
alice:apple
bob:banana
...
```

alice:..ekWXa83dhiA
bob:..ZS4zkCo/P7E
…

Dictionary Attacks

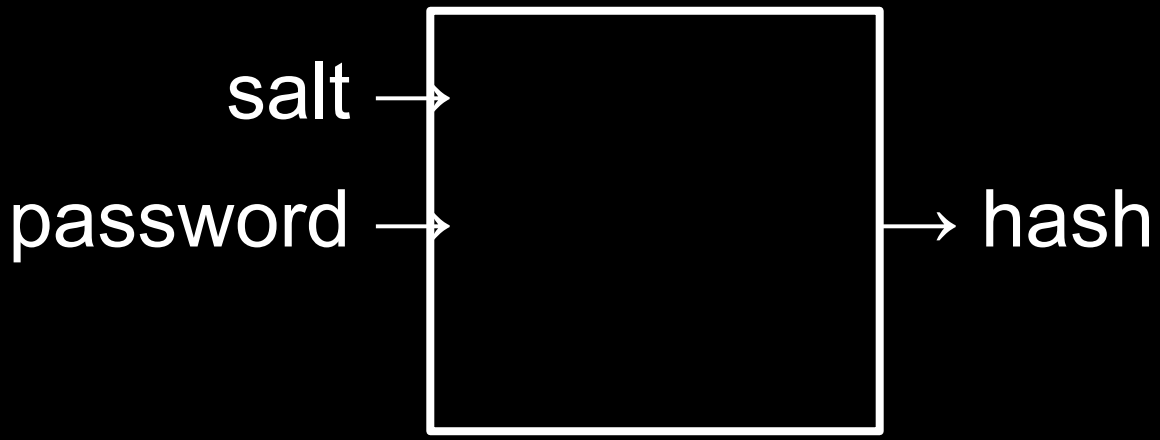
Brute-Force Attacks

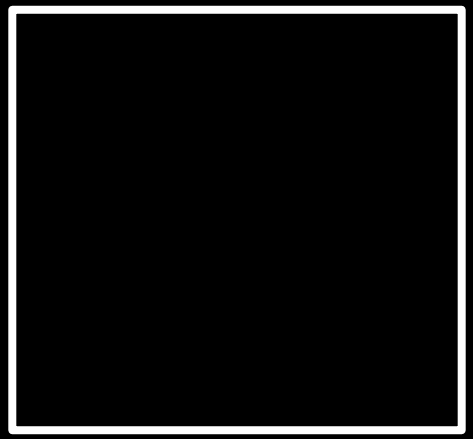
Rainbow Tables

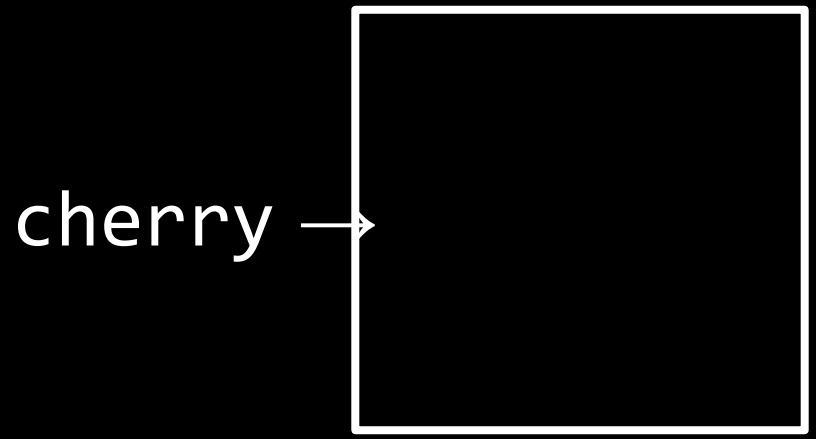
```
alice:apple
bob:banana
carol:cherry
charlie:cherry
...
```

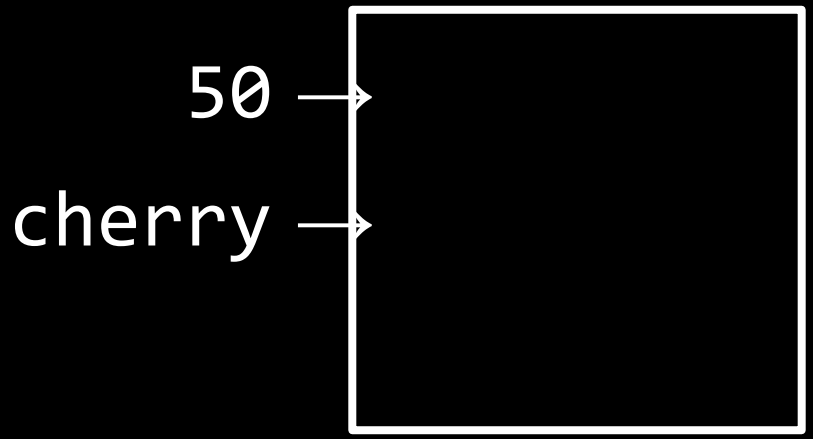
```
alice:..ekWXa83dhiA
bob:..ZS4zkCo/P7E
carol:..rj98gxDTYfM
charlie:..rj98gxDTYfM
...
```

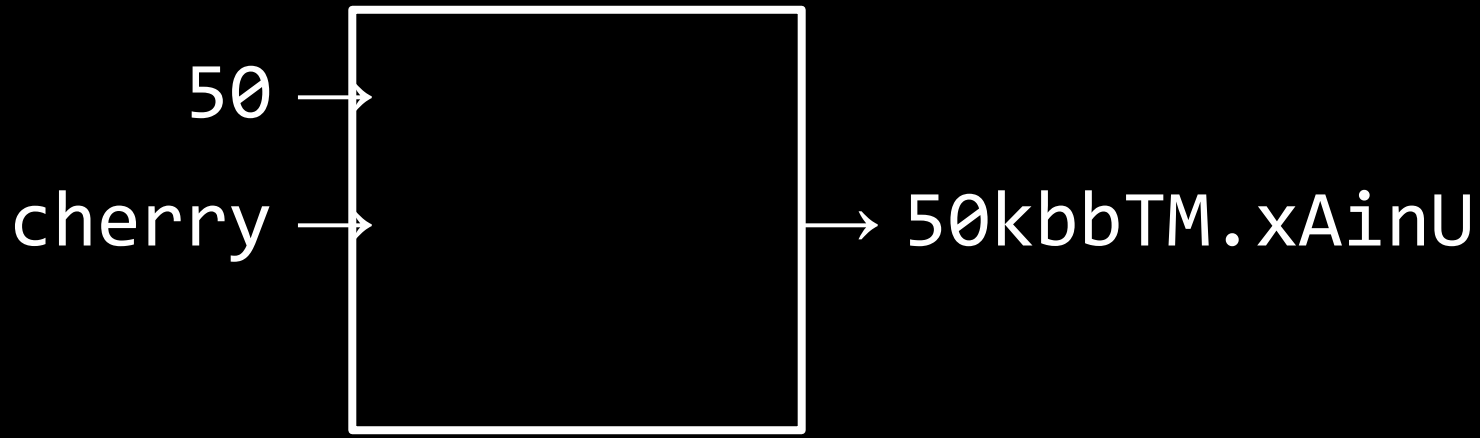
Salting

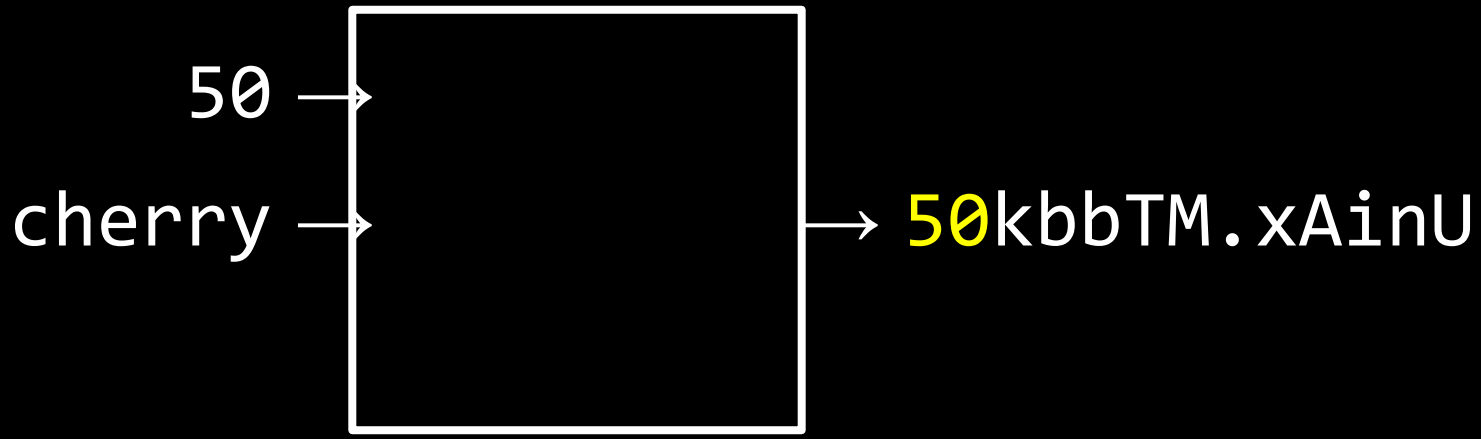

salt
password
hash

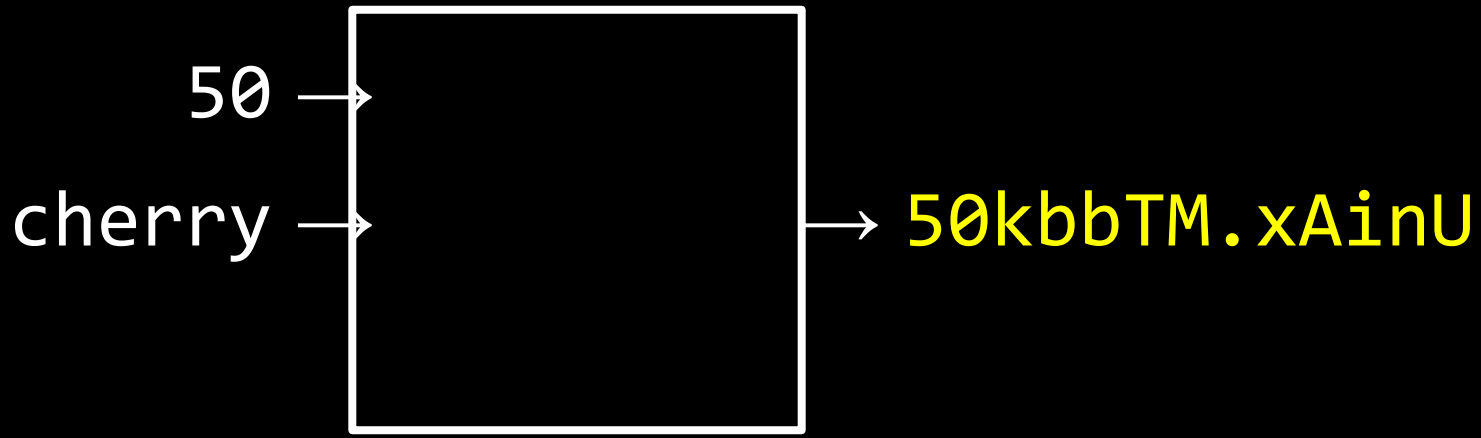


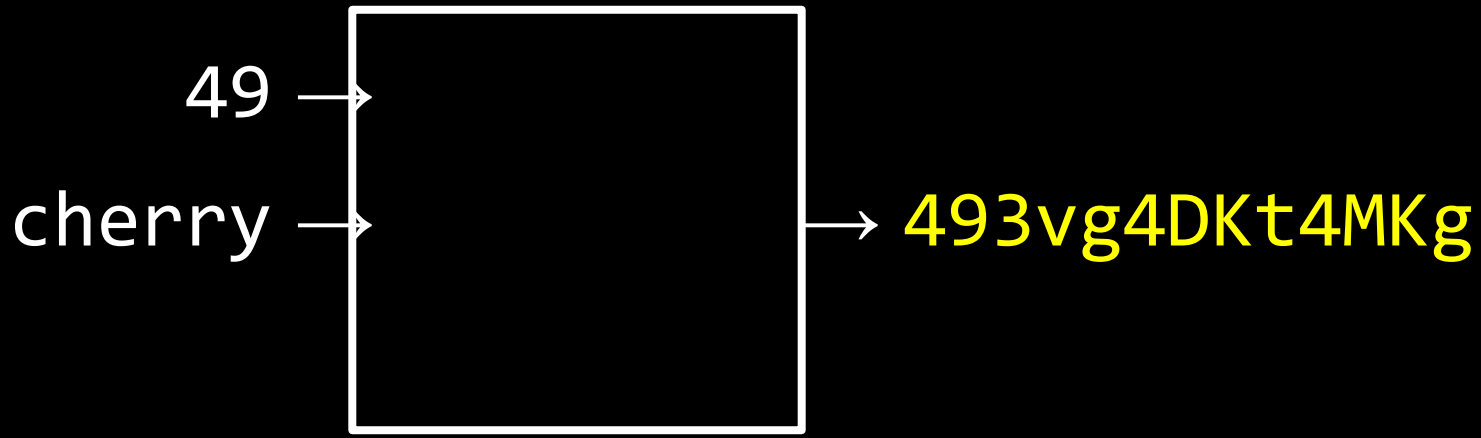

cherry

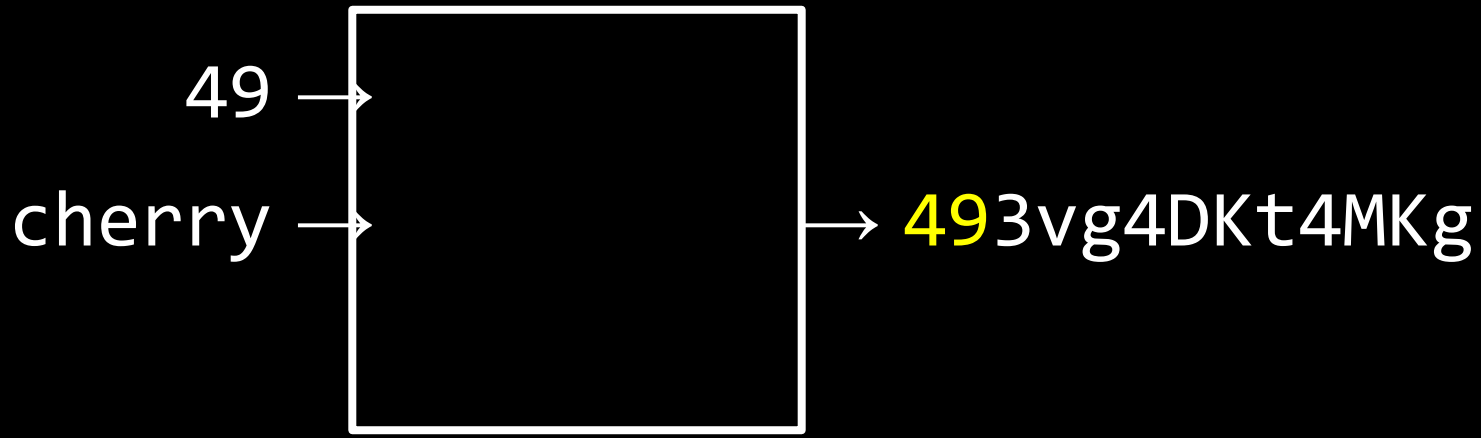

50
cherry


50
cherry
50kbbTM.xAinU


50
cherry
50kbbTM.xAinU


50
cherry
50kbbTM.xAinU


49
cherry
493vg4DKt4MKg


49
cherry
493vg4DKt4MKg

```
alice:..ekWXa83dhiA
bob:..ZS4zkCo/P7E
carol:50kbbTM.xAinU
charlie:493vg4DKt4MKg
...
```

```
alice:$y$j9T$DIXfskUxbz6we5RbfdPCz0$zFd93JMuTyEJHrdIf.6bZ8Rbw4otHvybdOuLn.eD.s3
bob:$y$j9T$ty3B9GwDhm4f6zQIgm9uL.$SbFq.iSFt48A5iQlue8DtUd.57KaBN1tIEdLPmtEjwC
carol:$y$j9T$hqOZx7o4Ts0wyCx0/Yct5/$bMqofMaf6jnOZFS.gT8jXw7gGIlSM5LlDjR77cm.xt2
charlie:$y$j9T$wf55sBgrtZfj2K.2kcVOd.$gzmxkKEQRkVKoCHw0dvYefnT/XZ4VyS9sylQN6M7Kr6
…
```

18,446,744,073,709,551,616

115,792,089,237,316,195,
423,570,985,008,687,907,
853,269,984,665,640,564,
039,457,584,007,913,129,
639,936

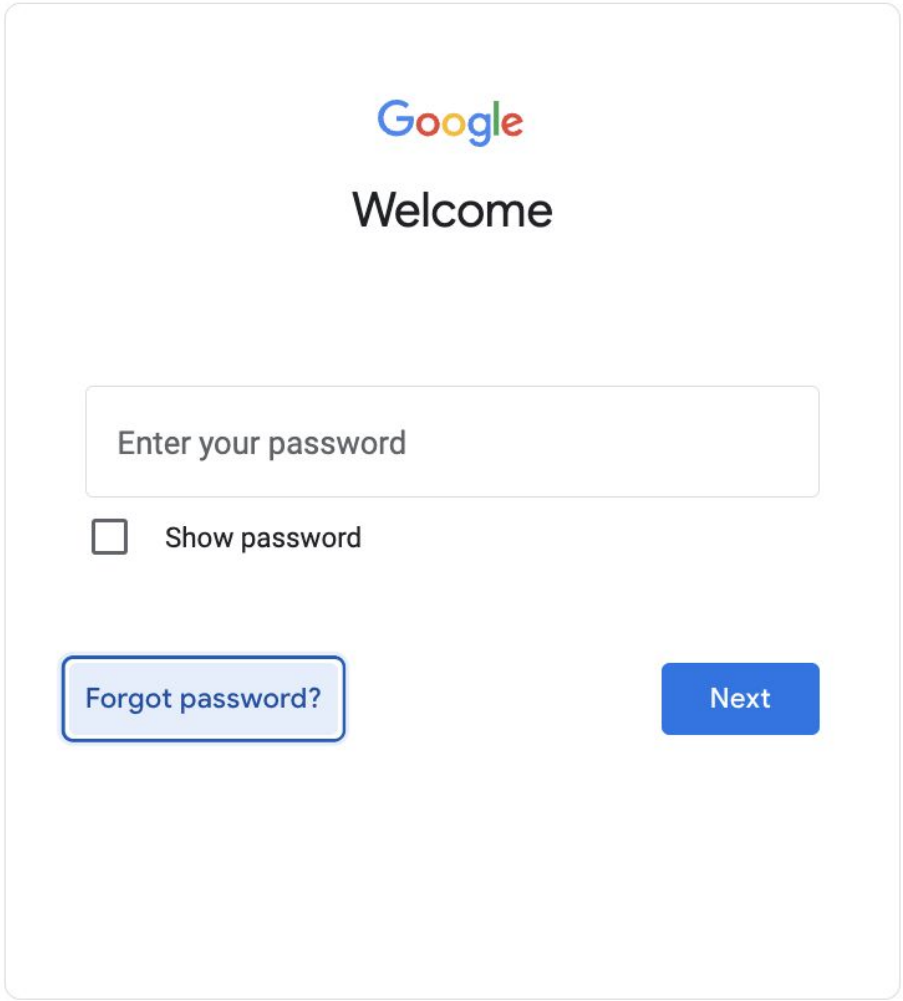
Welcome

Enter your password

Show password

Forgot password?

Next


Google
Welcome
Enter your password
Show password
Forgot password?
Next

"Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks. Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function... Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive. "

SHA-224
SHA-256
SHA-384
SHA-512
SHA-512/224
SHA-512/256
SHA3-224
SHA3-256
SHA3-384
SHA3-512
…

CMAC
HMAC
KMAC
…

One-Way Hash Functions

arbitrary length → fixed length

Cryptographic Hash Functions

arbitrary length → fixed length

Cryptography

Codes

Code word C	Code No 187	Message or true reading.
		Authority—Continued
Cannot	00	Give them authority
Cannula	01	Give you authority
Cannulated	02	Given authority
Canny	03	Great authority
Canoe	04	Has authority
Canoed	05	Has no authority
Canoeing	06	Has not authority
Canoeist	07	Have authority
Canoeists	08	Have authority from
Canoes	09	Have authority to
Canon	10	Have no authority
Canonbit	11	Have no other authority
Canonbone	12	Have they authority
Canoness	13	Have we authority
Canonic	14	Have you authority
Canonical	15	He has authority from
Canonicals	16	I have authority from
Canonicate	17	If they have authority
Canonist	18	If we have authority
Canonistic	19	If you have authority
Canonists	20	Must have authority
Canonize	21	No authority
Canonized	22	No authority has been given
Canonizes	23	Obtain authority
Canonizing	24	On our authority
Canonry	25	On the authority of
Canonship	26	On their authority
Canopied	27	On what authority
Canopies	28	On whose authority
Canopus	29	On your authority
Canopy	30	Our authority
Canorous	31	Published by authority
Cans	32	Some authority
Canso	33	Special authority
Cant	34	The authority
Canta	35	Their authority
Cantabile	36	They have authority
Cantabrian	37	They have no authority
Cantalever	38	Verbal authority
Cantaloupe	39	What is their authority
Cantar	40	What is your authority
Cantaro	41	Who is your authority
Cantata	42	With authority
Cantation	43	With our authority
Cantatory	44	With their authority
Cantatrice	45	With your authority
Canted	46	Without authority
Canteen	47	Without our authority
Canteens	48	Without their authority
Canter	49	Without your authority

Code word C	Code No 187	Message or true reading.
		Authority—Continued
Canterbury	50	You have authority
Cantered	51	You have no authority
Cantering	52	Your authority
Canters	53	Authorization
Canthook	54	Authorizations
Canthus	55	Authorize
Canticle	56	Authorize them to
Canticoy	57	Authorize us to
Canting	58	Authorize you to
Cantingly	59	Do not authorize
Cantle	60	Do they authorize
Canto	61	Do you authorize
Canton	62	I authorize
Cantonal	63	They authorize
Cantoned	64	They will not authorize
Cantoning	65	To authorize
Cantonize	66	Will authorize
Cantonized	67	Will not authorize
Cantonizes	68	Will you authorize
Cantonment	69	Authorized
Cantons	70	Am authorized to
Cantor	71	Are authorized to
Cantoral	72	Are not authorized to
Cantoris	73	Are they authorized to
Cantors	74	Are we authorized to
Cantrap	75	Are you authorized to
Cantrip	76	Duly authorized
Cants	77	Is authorized
Canty	78	Is he authorized
Canvasback	79	Is not authorized
Canvass	80	No more authorized
Canvassed	81	Not authorized
Canvasser	82	Not authorized to
Canvasses	83	Properly authorized
Canvassing	84	They are authorized to
Canzone	85	They are not authorized to
Canzonet	86	Was authorized
Capa	87	Was not authorized
Capability	88	We are authorized to
Capable	89	We are not authorized to
Capacified	90	You are authorized
Capacifies	91	You are authorized to
Capacify	92	You are authorized to answer
Capacious	93	You are authorized to assure
Capacitate	94	You are authorized to convey
Capacities	95	You are authorized to state
Capacity	96	You are hereby authorized
Capapié	97	You are hereby authorized to
Caparison	98	You are not authorized
Caparisons	99	Authorizes

Encode

plaintext → codetext

Decode

codetext → plaintext

Ciphers


TOVER


EURO
24
25
2€

Encipher

plaintext → ciphertext

Encrypt

plaintext → ciphertext

Encryption

plaintext → ciphertext

Decipher

ciphertext → plaintext

Decrypt

ciphertext → plaintext

Decryption

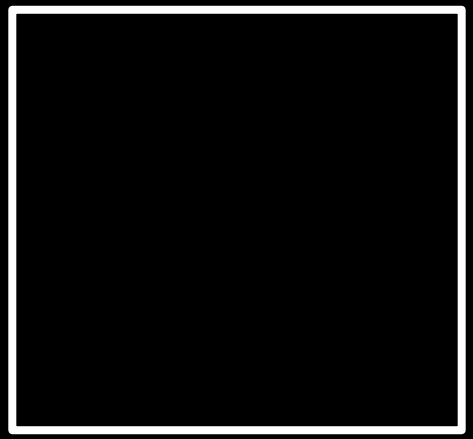
ciphertext → plaintext

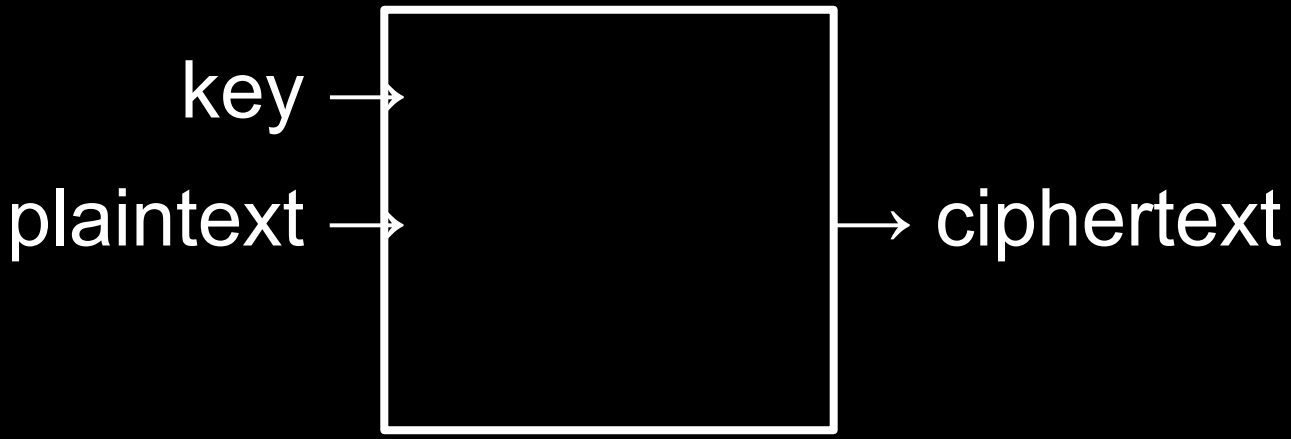
Keys

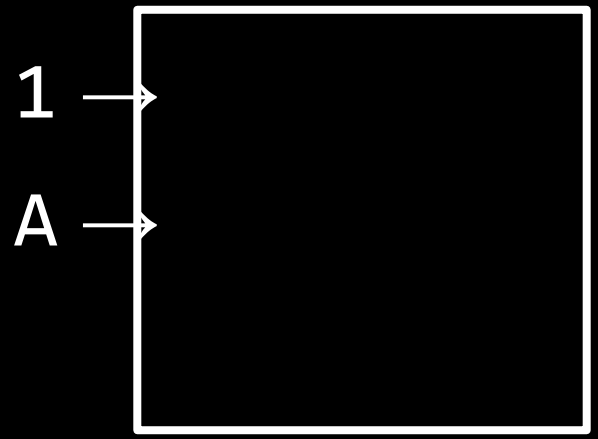
Secret-Key Cryptography

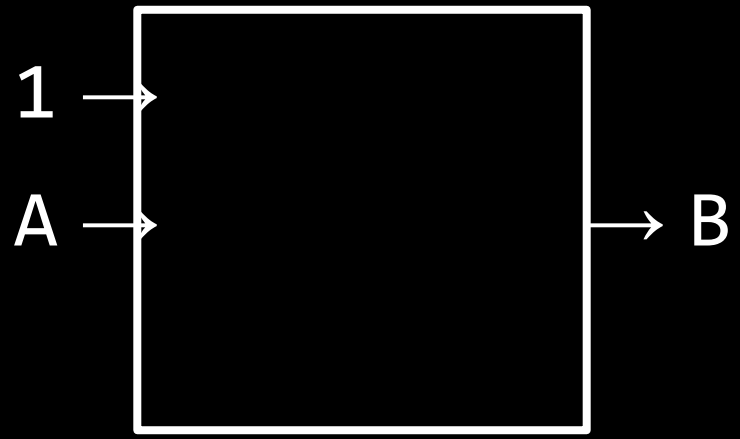
Secret-Key Encryption

Symmetric-Key Encryption



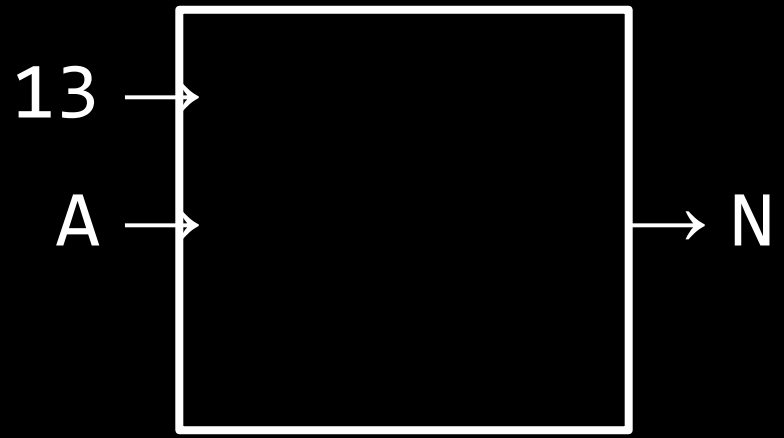

key
plaintext
ciphertext

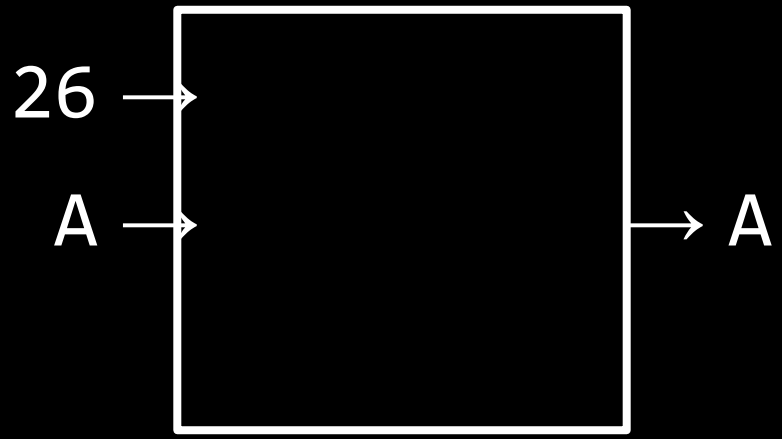

1
A


1
A
B


1
B
C

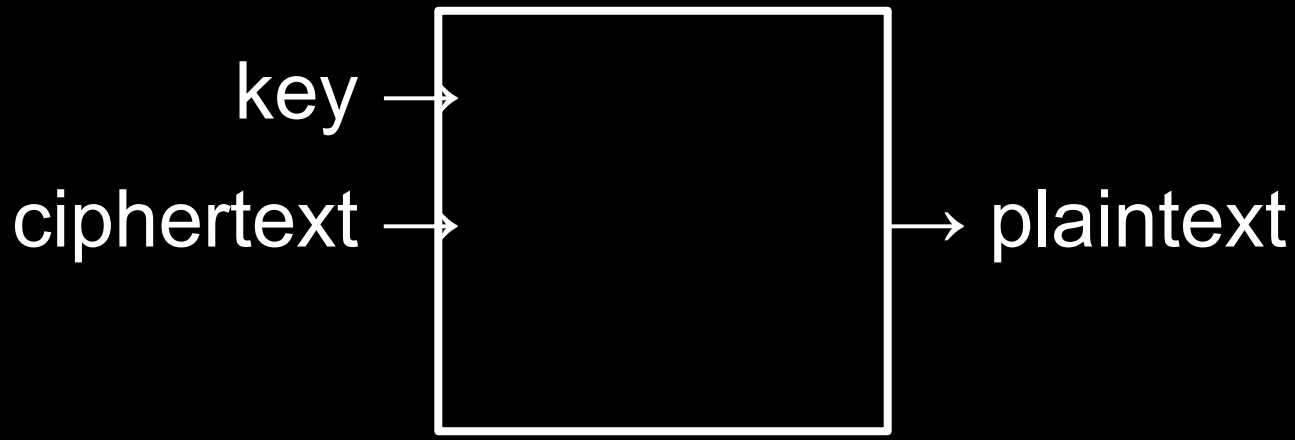

1
Z
A


13
A
N


26
A
A

OR FHER GB QEVAX LBHE BINYGVAR

Decrypting


key
ciphertext
plaintext


1
B
A

OR FHER GB QEVAX LBHE BINYGVAR

Cryptanalysis

OR FHER GB QEVAX LBHE BINYGVAR

BE SURE TO DRINK YOUR OVALTINE

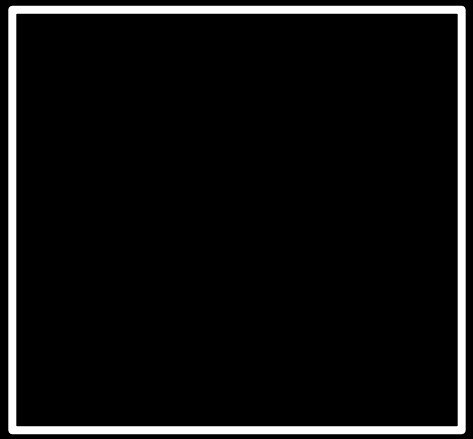
AES
Triple DES
…

Public-Key Cryptography

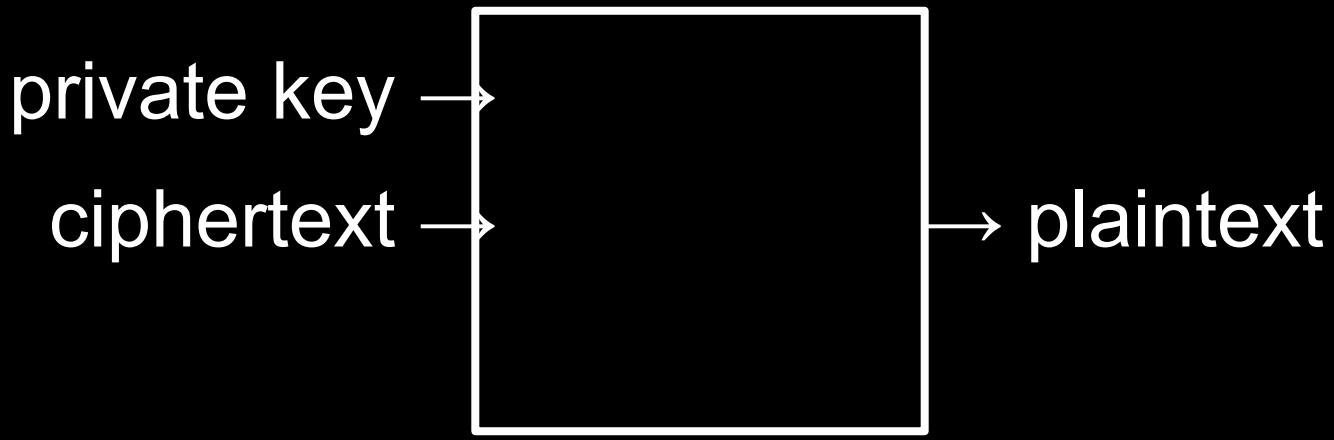
Diffie-Hellman
MQV
RSA
…

Public-Key Encryption

Asymmetric-Key Encryption




public key
plaintext
ciphertext


private key
ciphertext
plaintext

RSA

$n = p \cdot q$

$\ldots$

RSA

$$c = m^e \bmod n$$
$$m = c^d \bmod n$$

Key Exchange

Diffie-Hellman

$A = g^a \bmod p$

$B = g^b \bmod p$

…

Diffie-Hellman

$s = B^{a} \bmod p$

$s = A^{b} \bmod p$

…

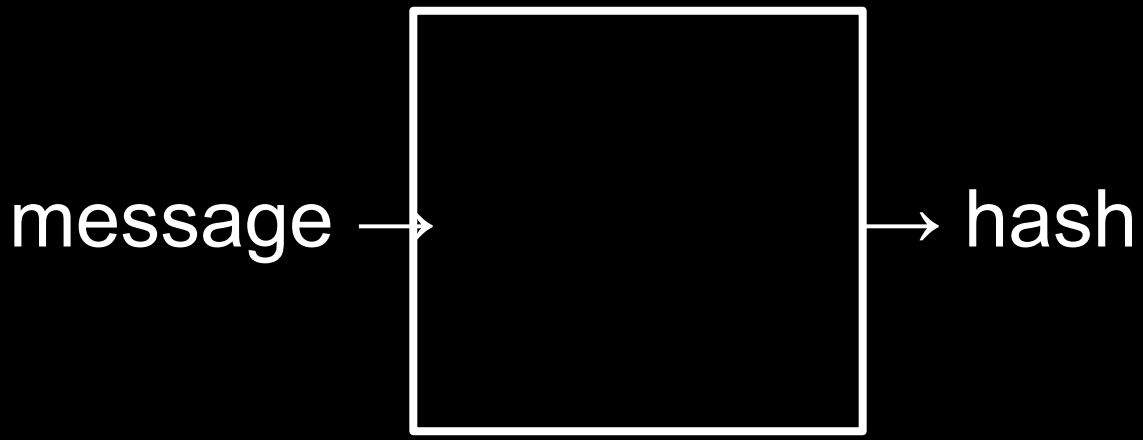
Diffie-Hellman

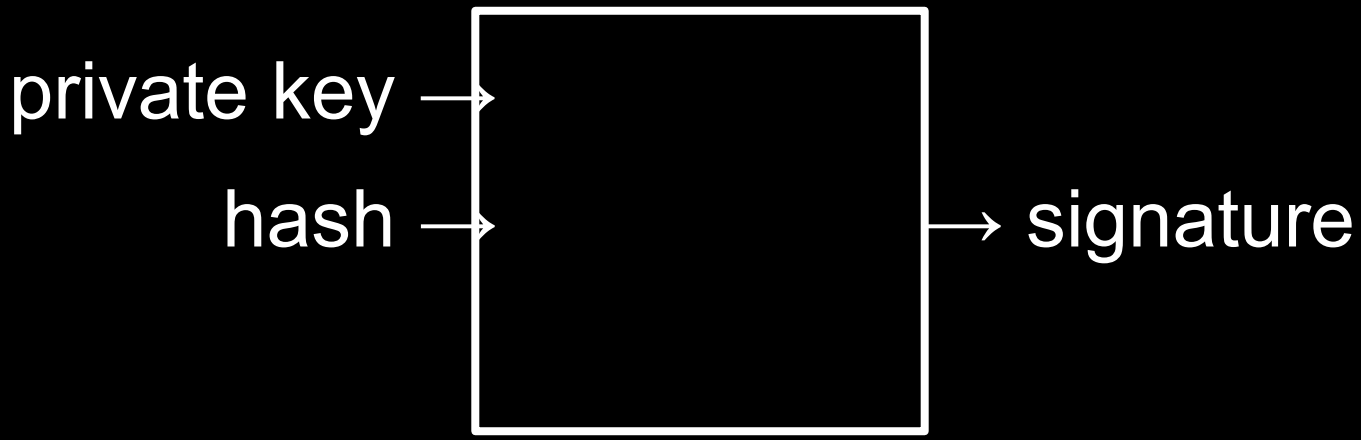
$$s = g^{ab} \bmod p$$

Digital Signatures

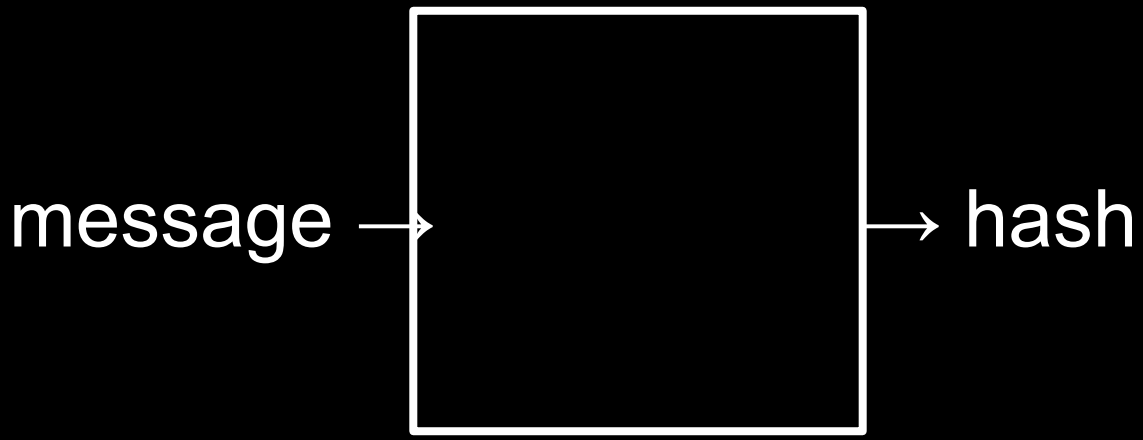
DSA
ECDSA
RSA
…

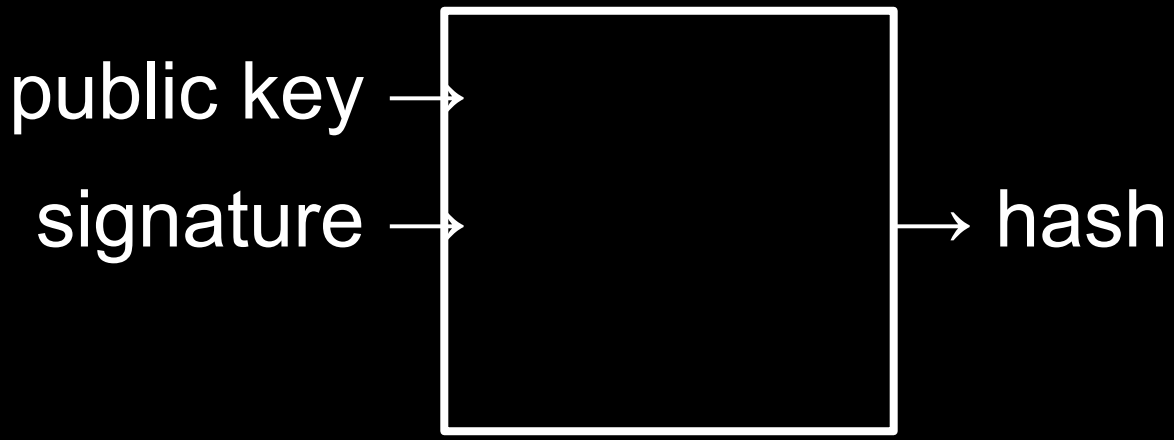
Sign


message
hash


private key
hash
signature

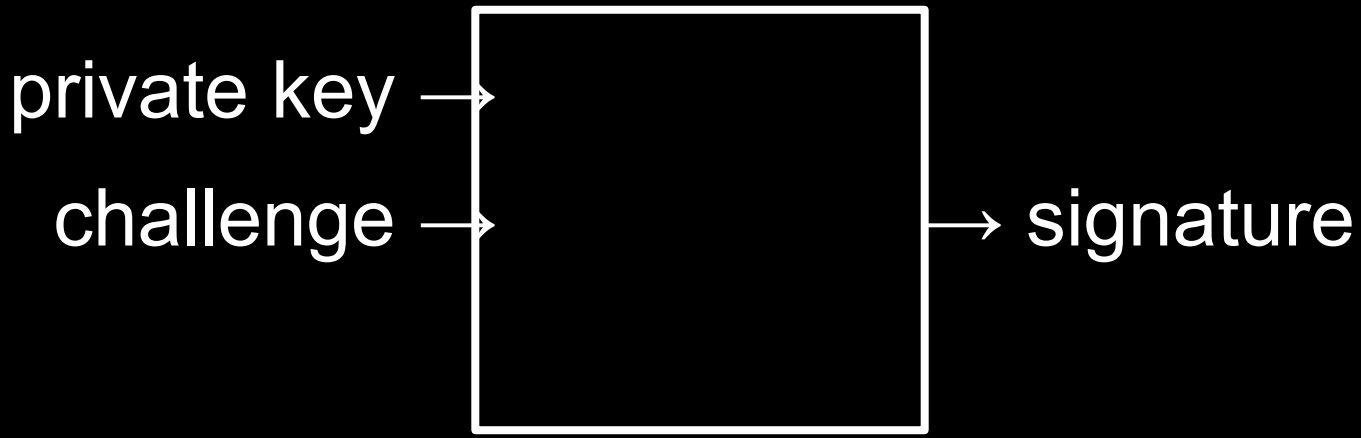
Verify

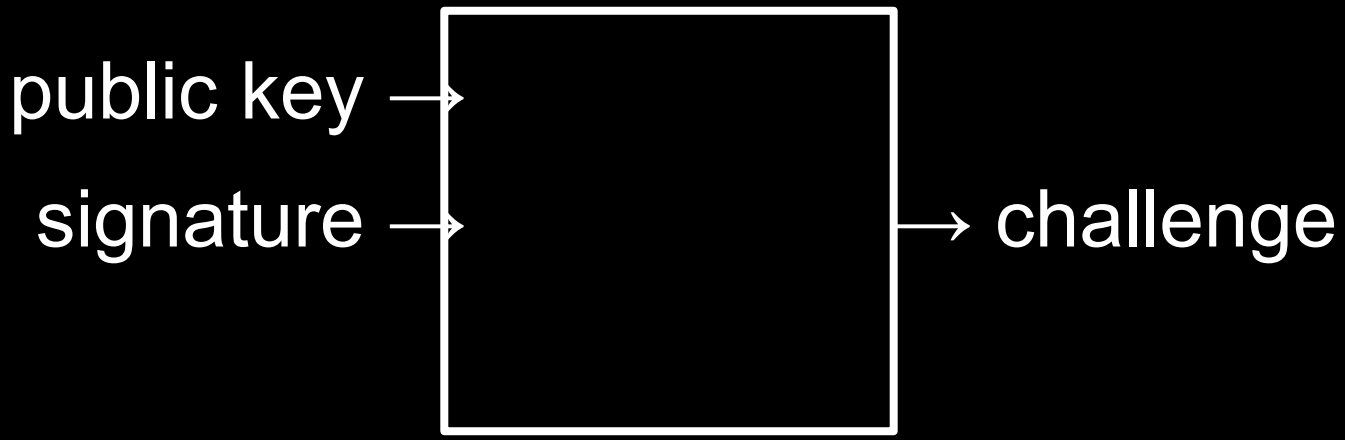

message
hash


public key
signature
hash

Passkeys

WebAuthn


private key
challenge
signature


public key
signature
challenge

Encryption in Transit

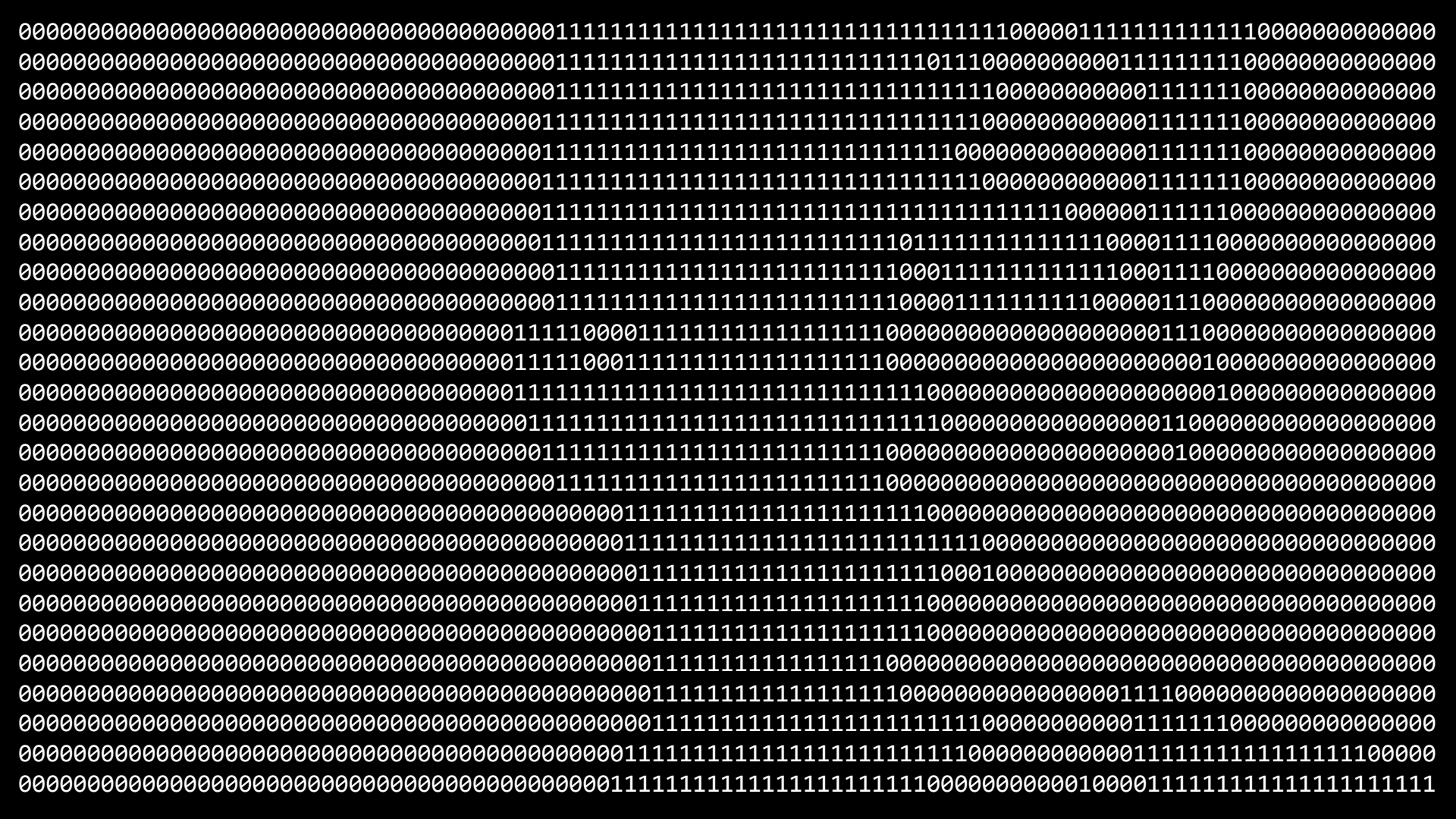
Alice ↔ Eve ↔ Bob

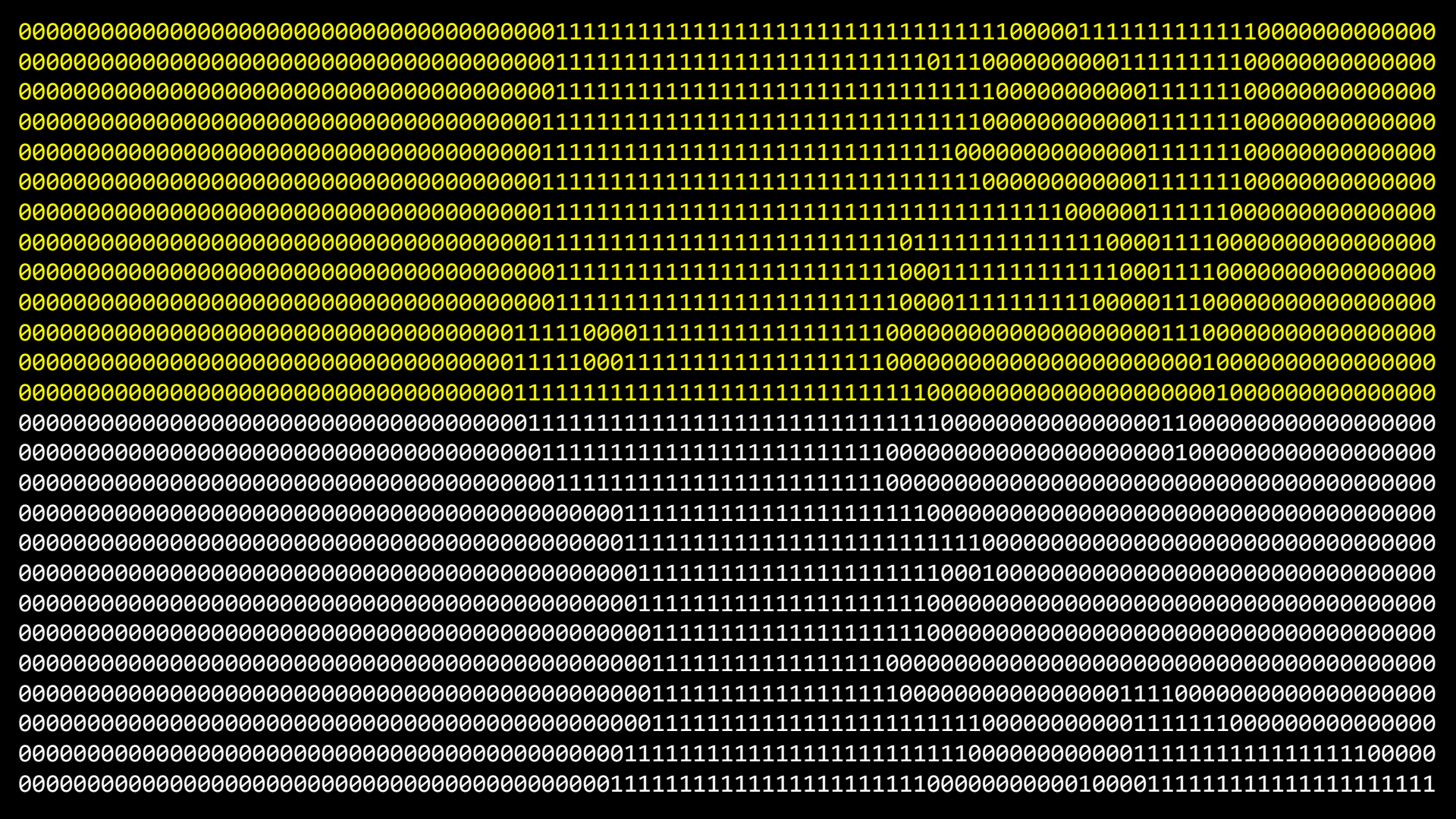
End-to-End Encryption

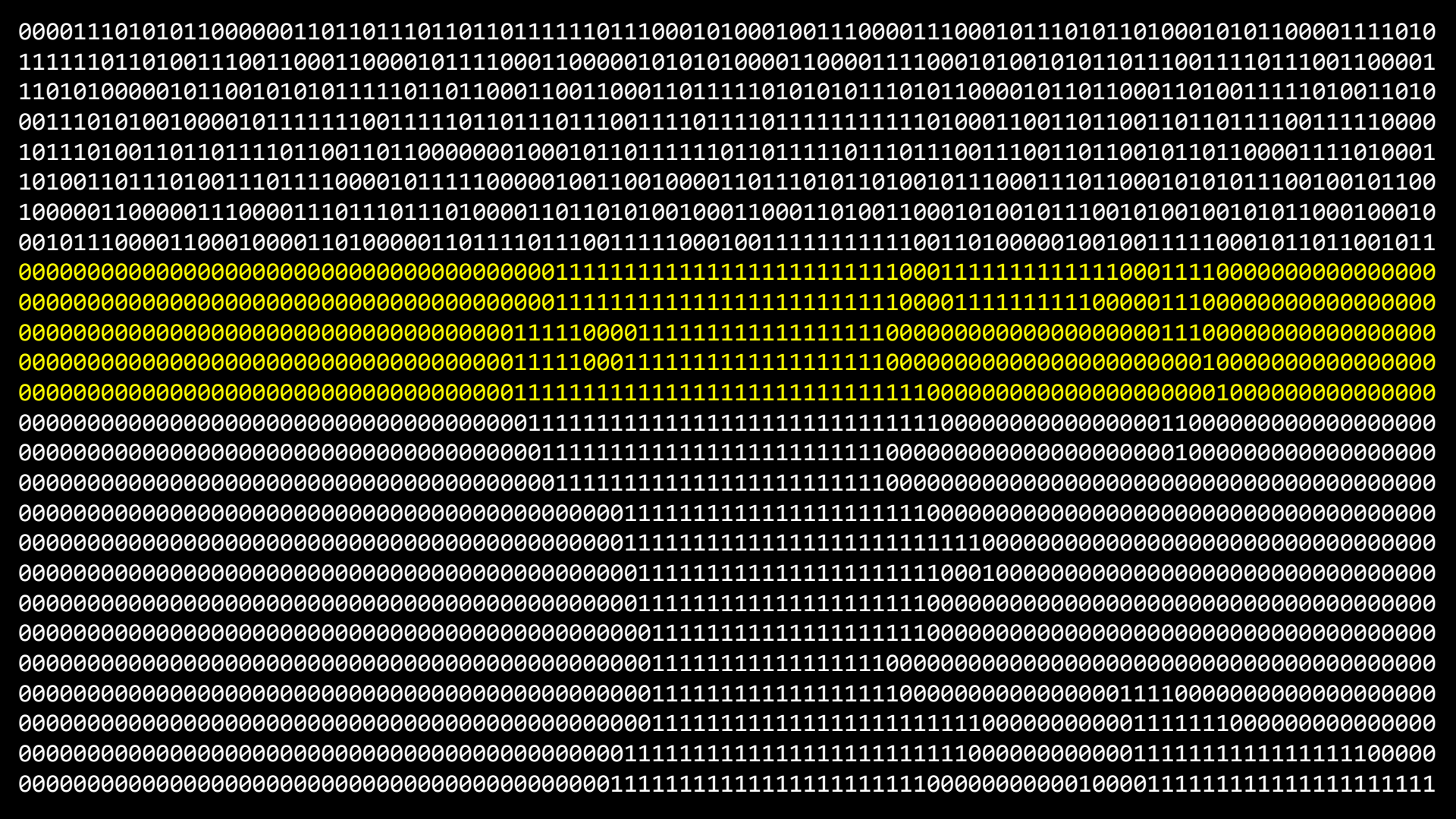
Alice ↔ Bob

Deletion

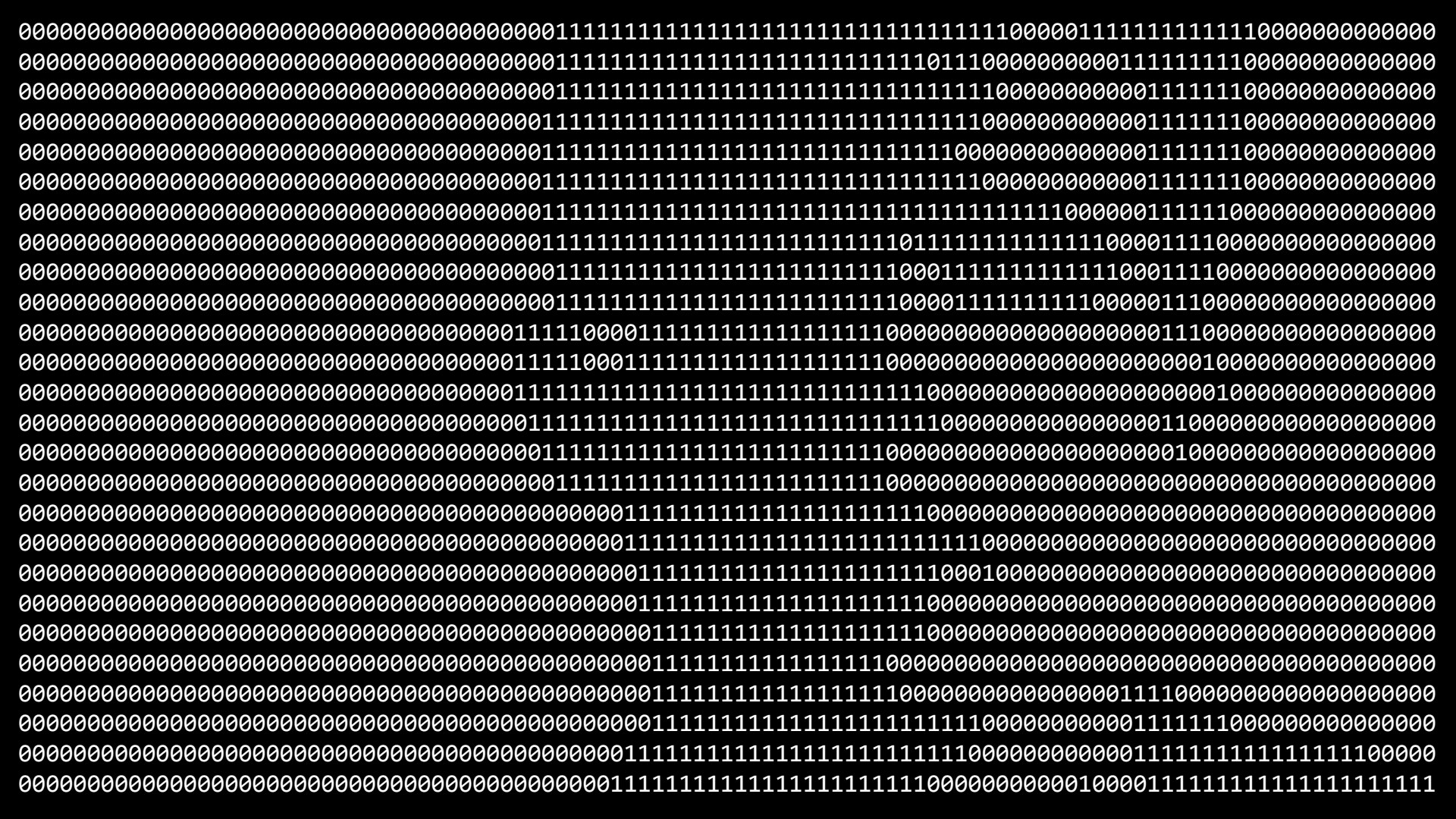

SanDisk

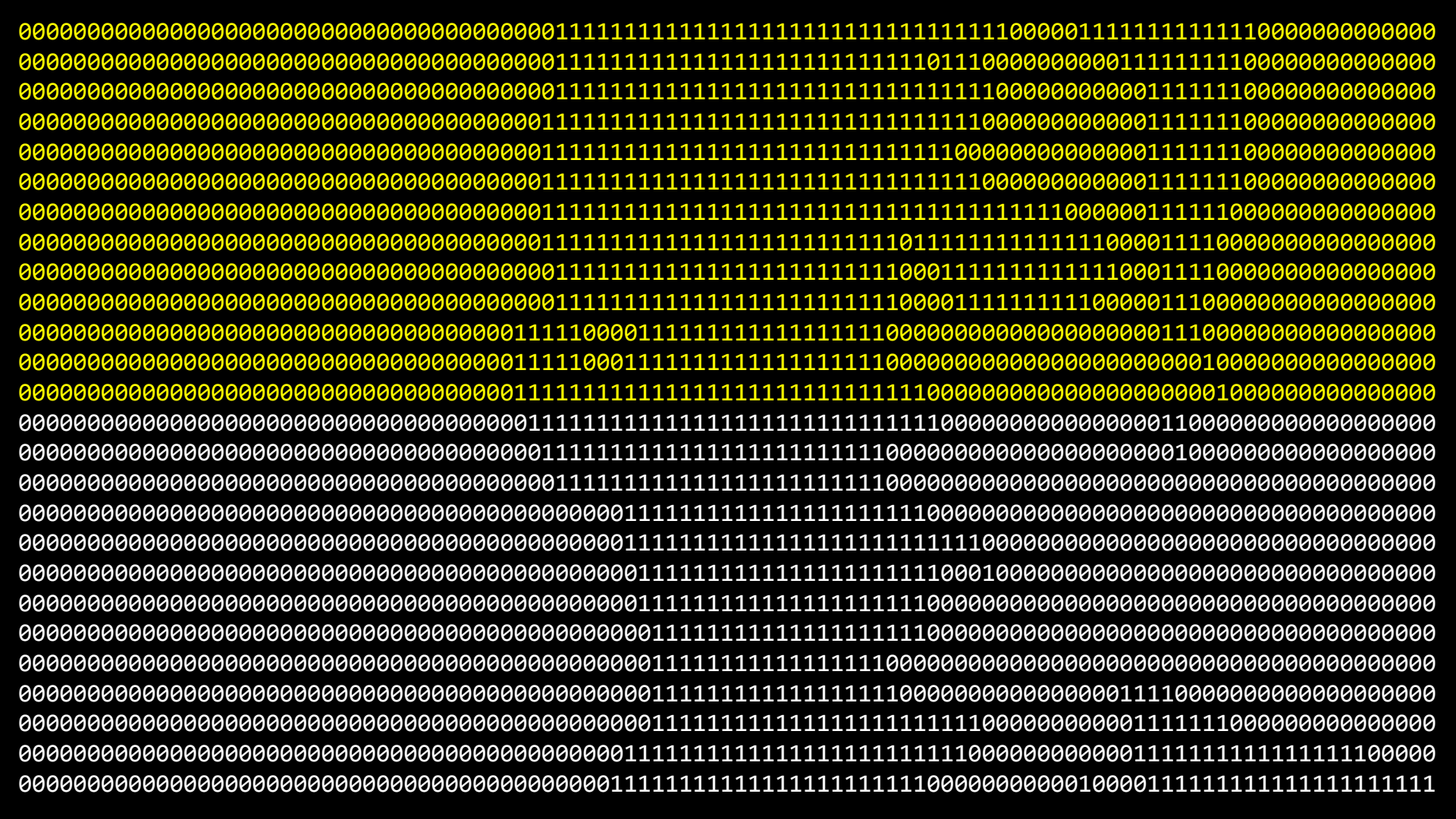


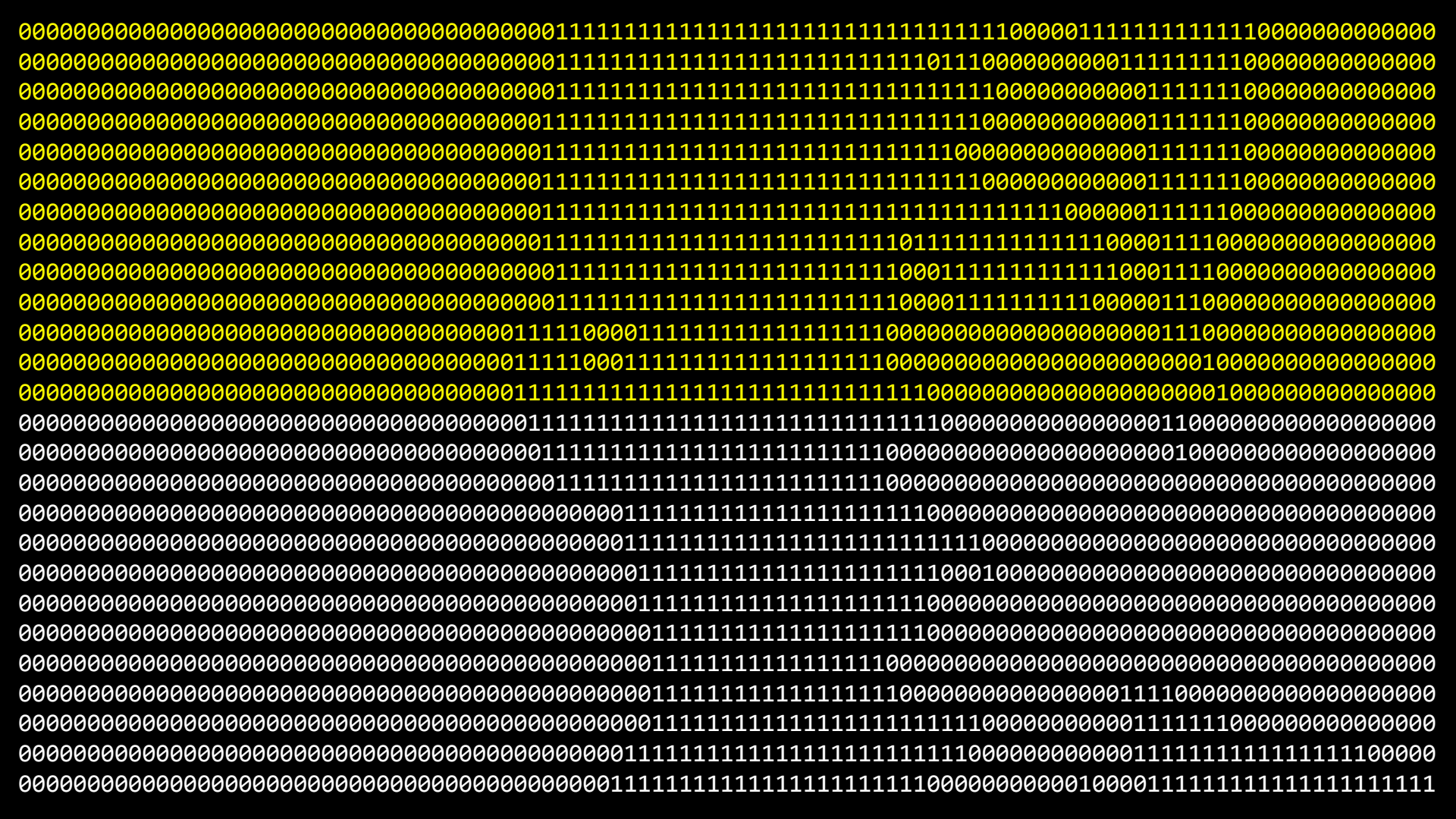


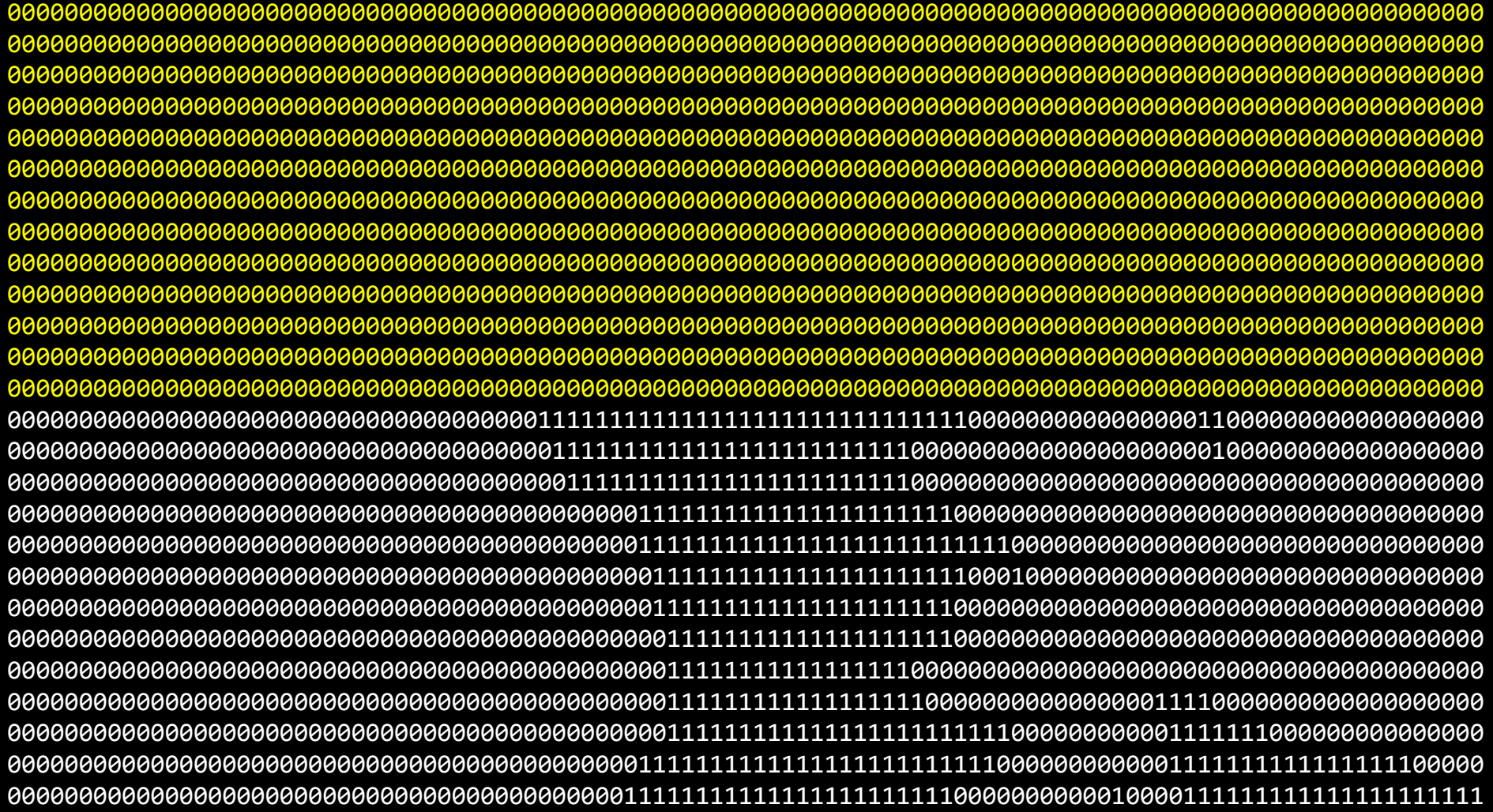


Secure Deletion



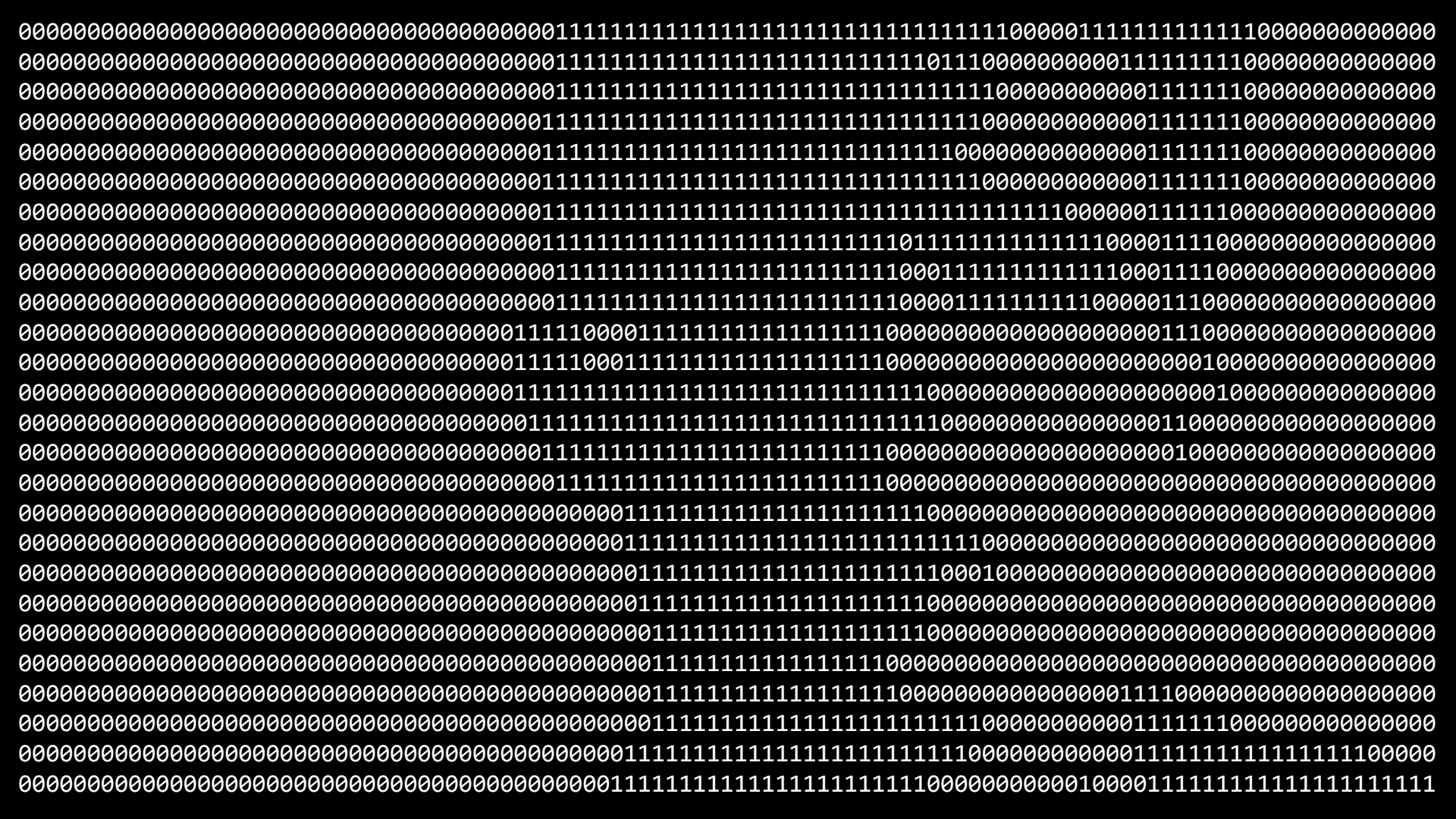


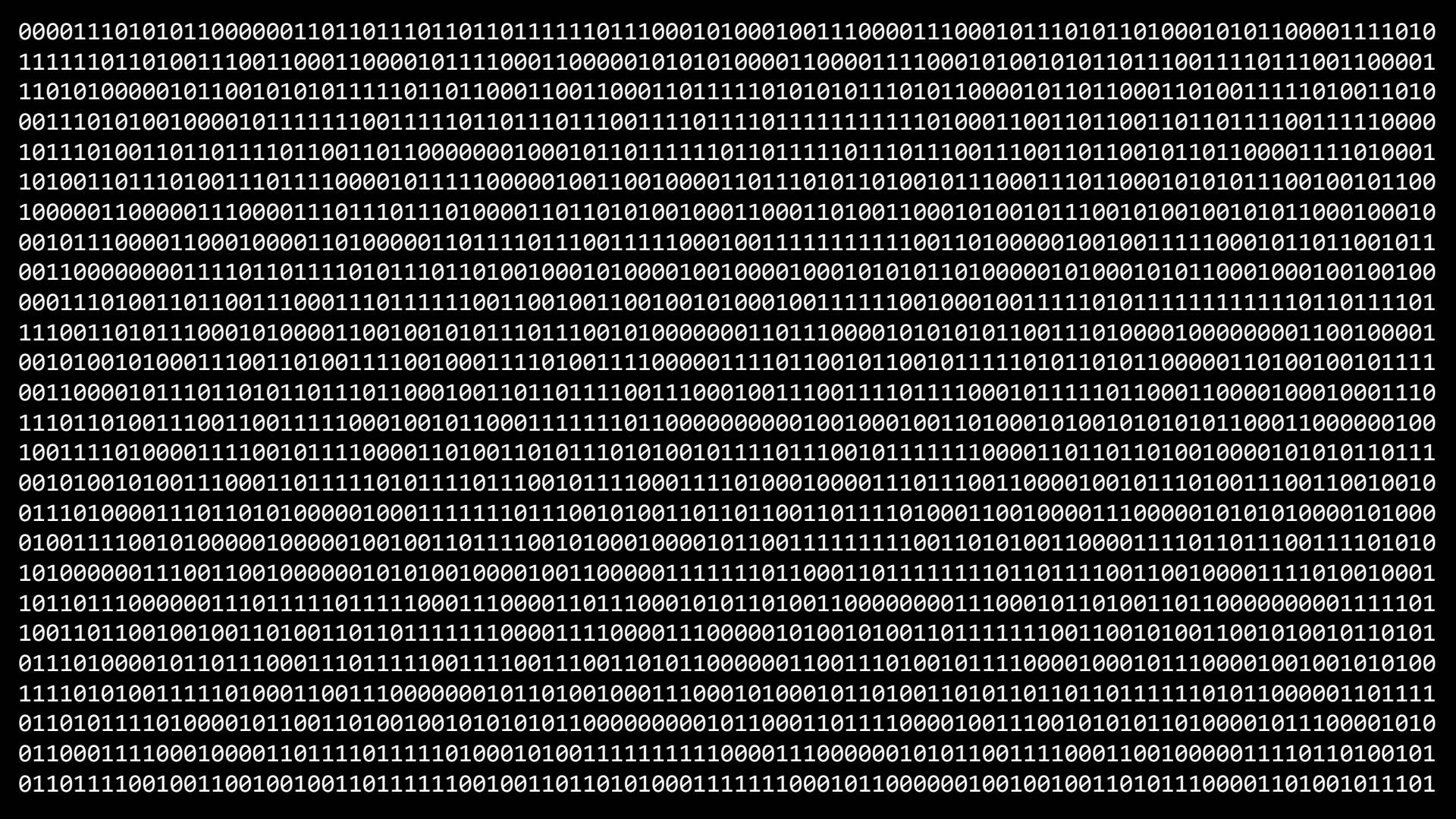


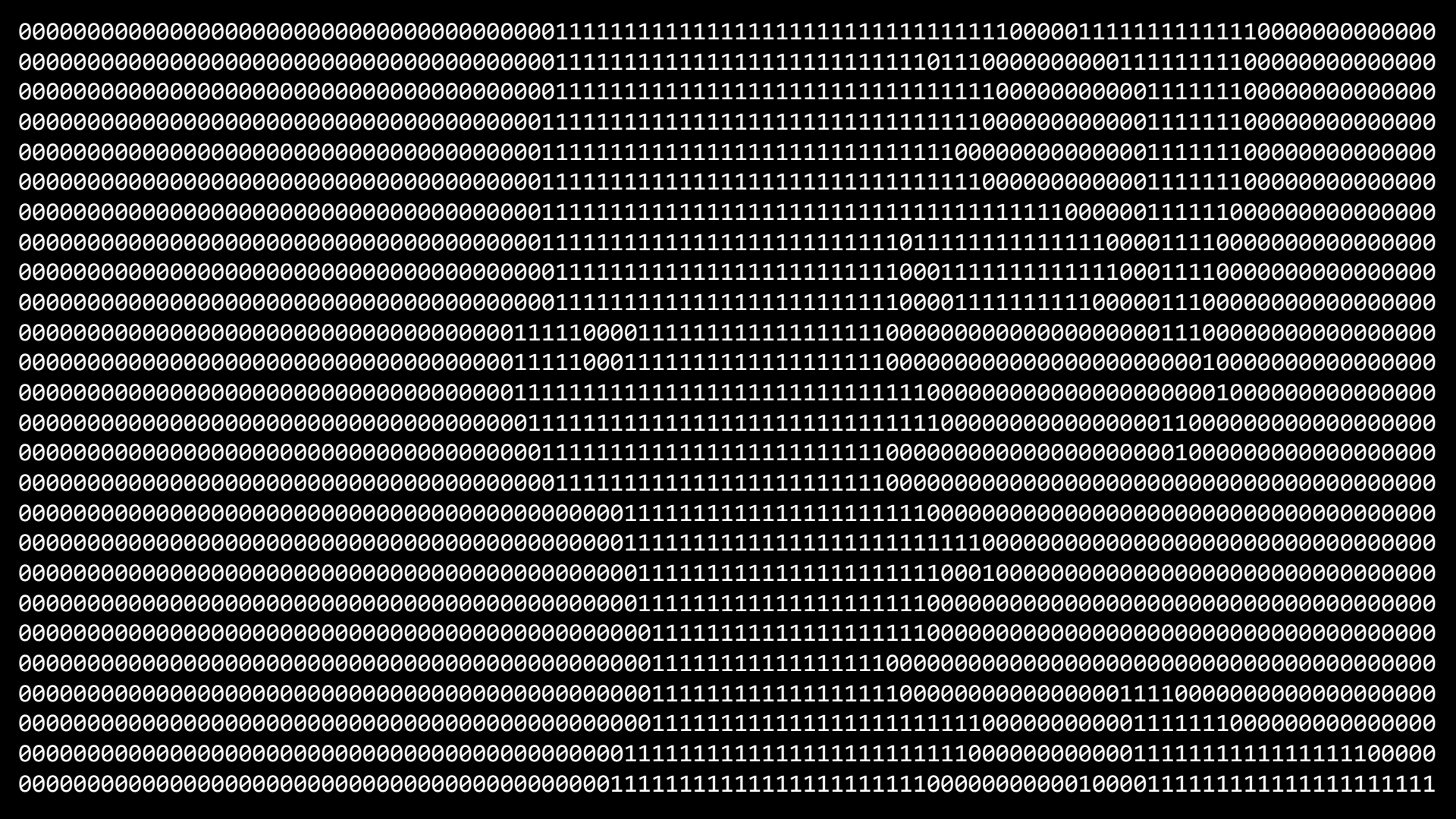


Full-Disk Encryption

Encryption at Rest







Ransomware

Quantum Computing

Introduction to

Cybersecurity

David J. Malan
malan@harvard.edu