

Introduction to Cybersecurity

David J. Malan
malan@harvard.edu

Securing Data

Passwords

alice:apple

bob:banana

...

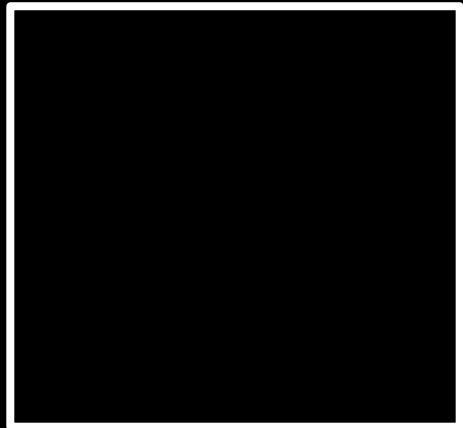
alice:apple

bob:banana

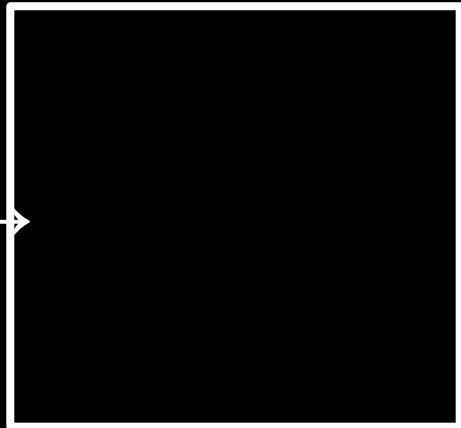
...

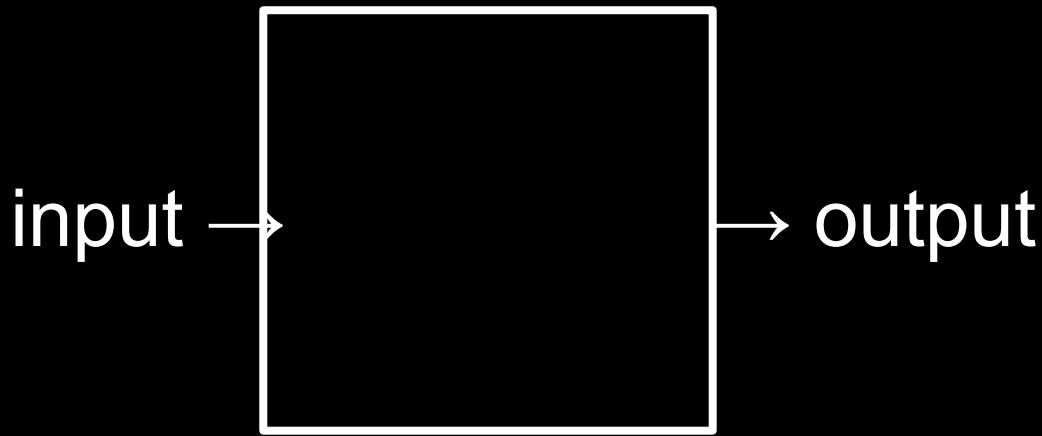
Hashing

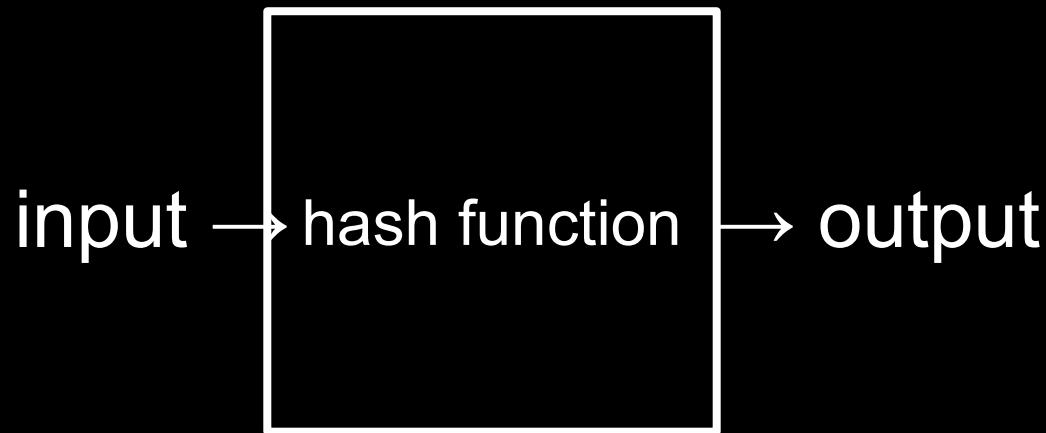
password → hash

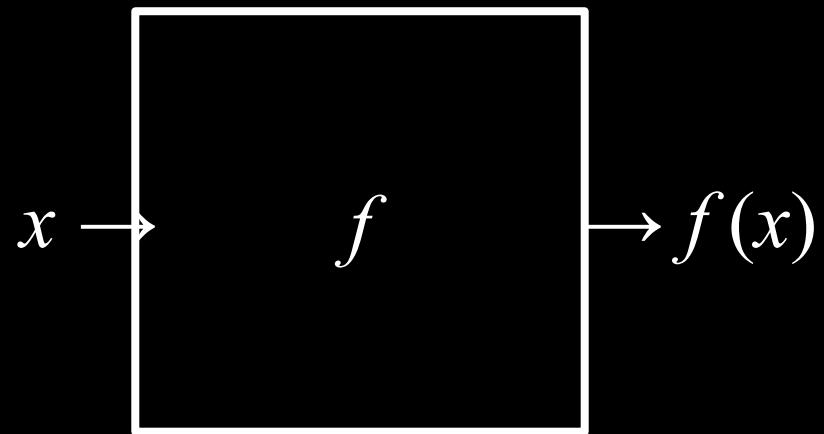


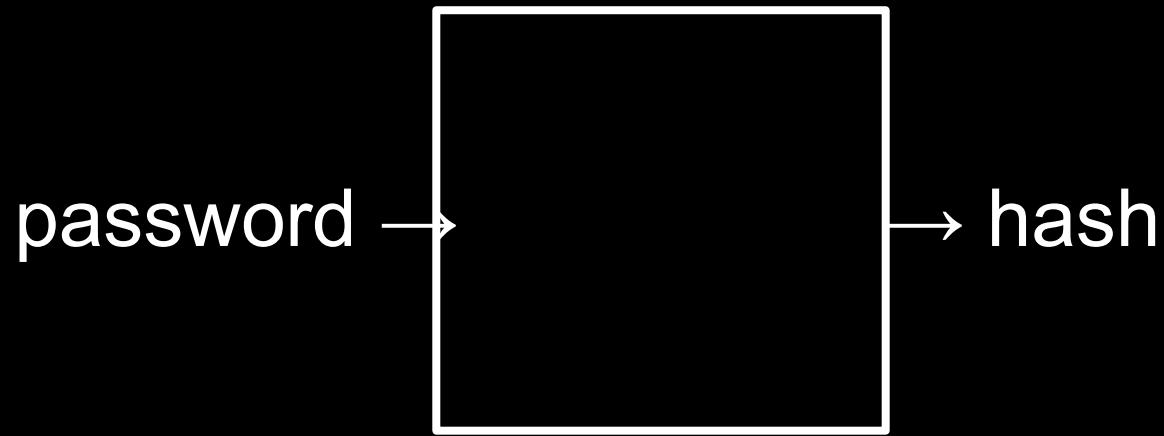
input →





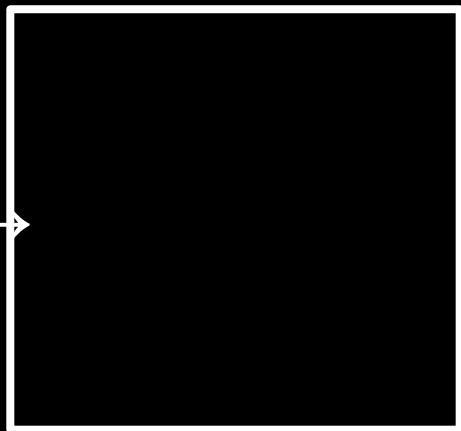




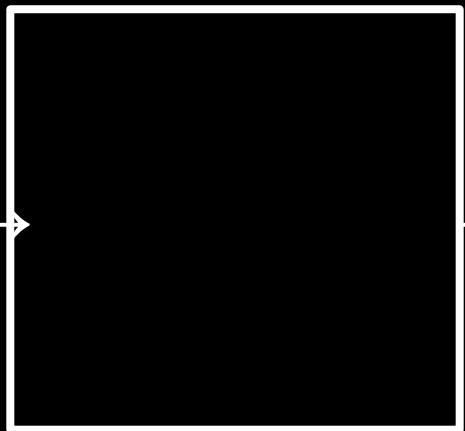




apple →

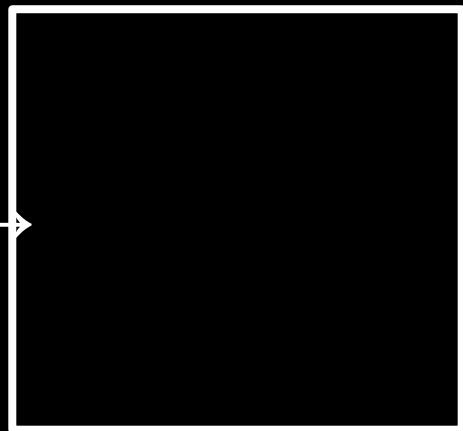


apple →



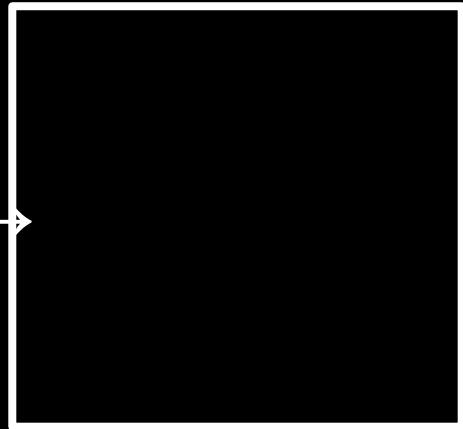
→ 1

banana →



→ 2

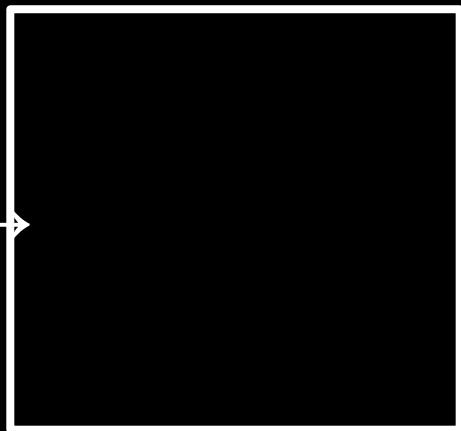
cherry →



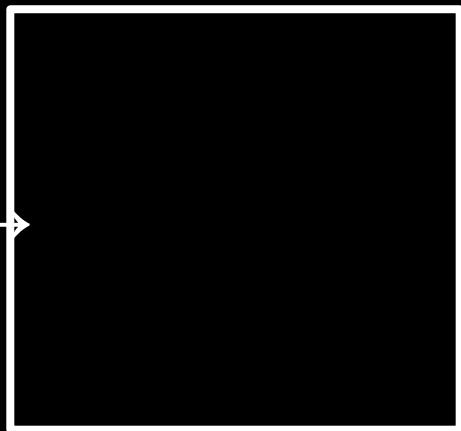
→ 3



apple →

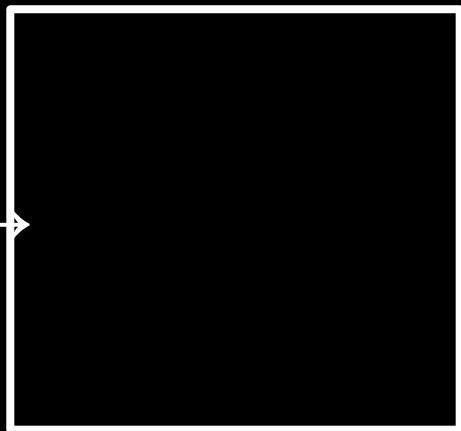


apple →



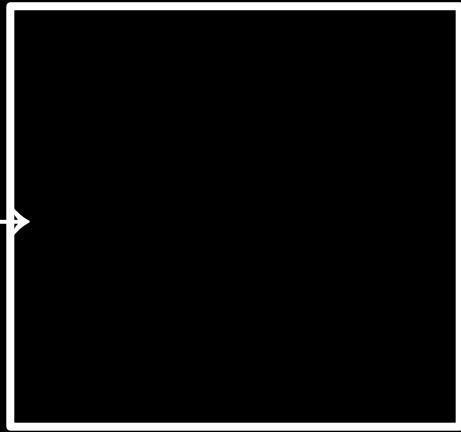
→ ...ekWXA83dhiA

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

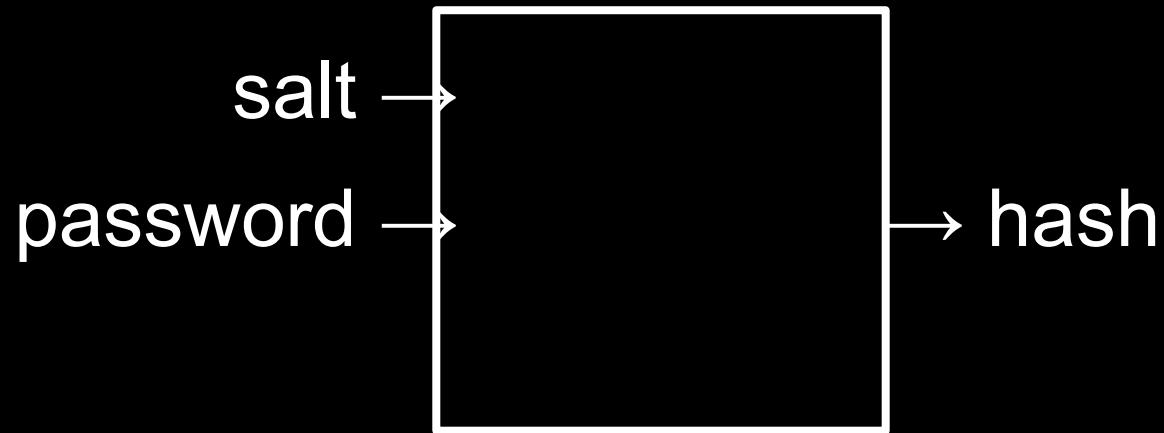
bob:..ZS4zkCo/P7E

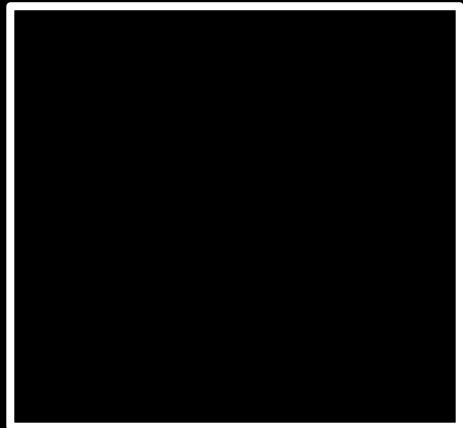
carol:..rj98gxDTYfM

charlie:..rj98gxDTYfM

...

Salting



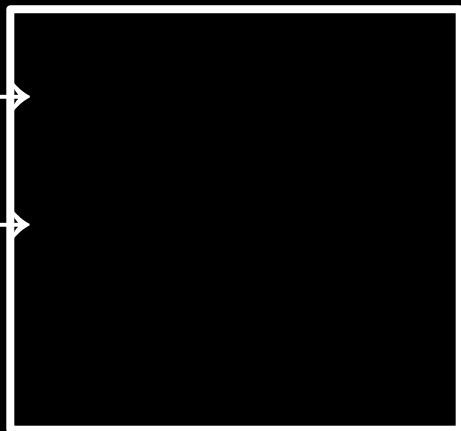


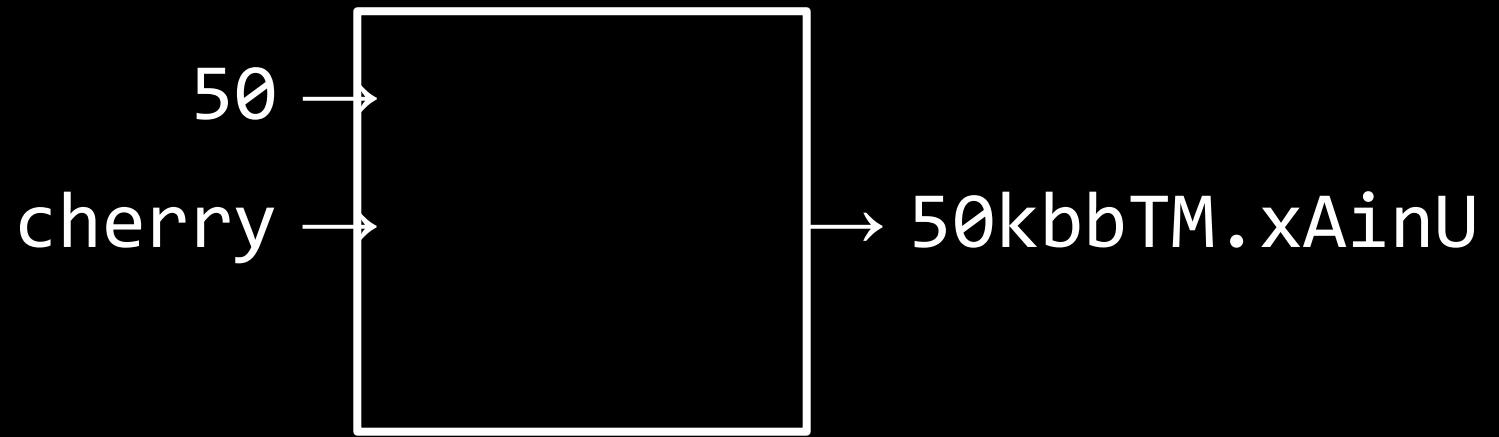
cherry →

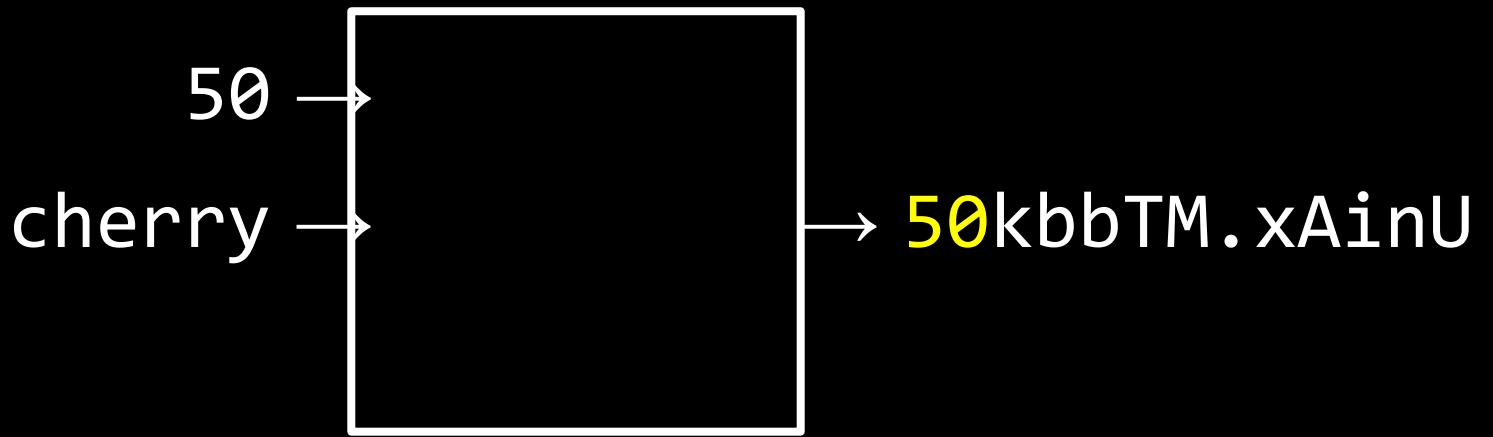


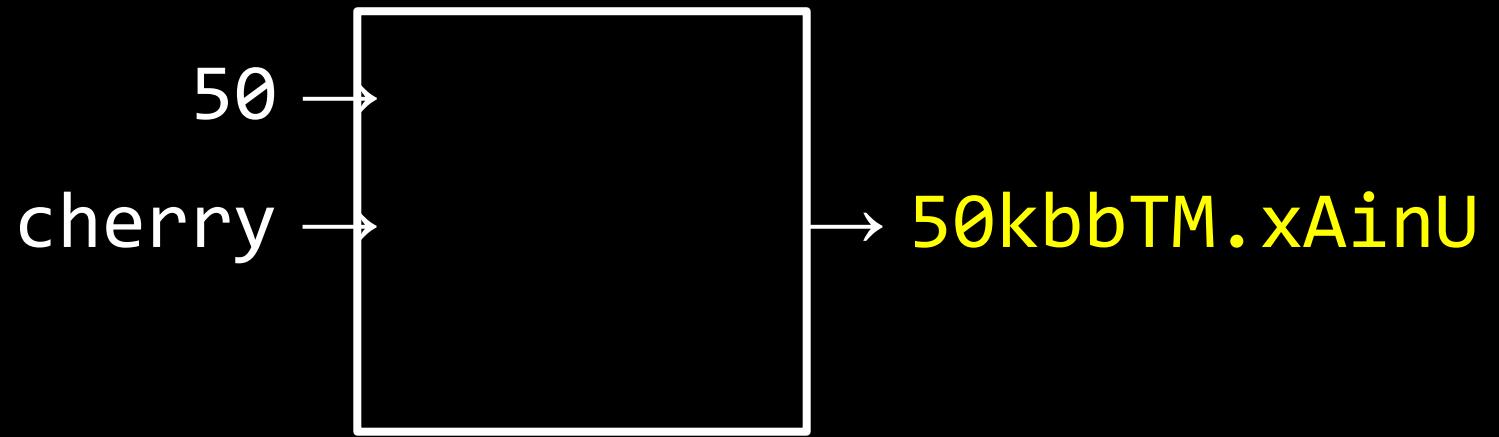
50

cherry



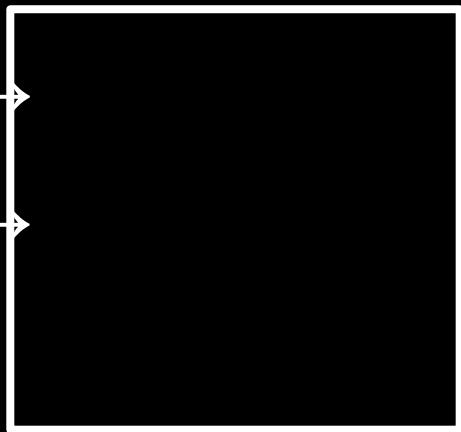






49

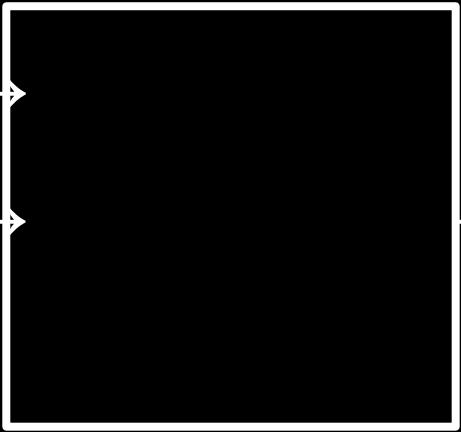
cherry



493vg4DKt4MKg

49

cherry



493vg4DKt4MKg

alice:...ekWXa83dhiA

bob:...ZS4zkCo/P7E

carol:50kbbTM.xAinU

charlie:493vg4DKt4MKg

...

alice:\$y\$j9T\$DTXfskUxbz6we5RbfdPCz0\$zFd93JMuTyEJHrdIf.6bZ8Rbw4otHvybd0uLn.eD.s3
bob:\$y\$j9T\$ty3B9GwDhm4f6zQIgm9uL.\$SbFq.iSFt48A5iQlue8DtUd.57KaBN1tIEDLPmtEjwC
carol:\$y\$j9T\$hq0Zx7o4Ts0wyCx0/Yct5/\$bMqofMaf6jnOZFS.gT8jXw7gGI1SM5L1DjR77cm.xt2
charlie:\$y\$j9T\$wf55sBgrtZfj2K.2kcV0d.\$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



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

AUTHORITY

Code word C	Code No 187	Message or true reading.
Cannot	00	Authority—Continued
Cannula	01	Give them authority
Cannulated	02	Give you authority
Canny	03	Great authority
Canoe	04	Has authority
Canoeed	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
Canonie	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

AUTHORITY

Code word C	Code No 187	Message or true reading.
Canterbury	50	Authority—Continued
Centered	51	You have authority
Centering	52	You have no authority
Canters	53	Your authority
Canthook	54	Authorizations
Canthus	55	Authorizations
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
Cants	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
Cantonment	68	Will you authorize
Cantone	69	Authorized
Cantone	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	Did you authorized
Cants	77	Is authorized
Canty	78	Is he authorized
Canvasback	79	Is not authorized
Canvas	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
Capacines	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
Capapie	97	You are hereby authorized to
Caparison	98	You are not authorized
Caparisons	99	Authorizes

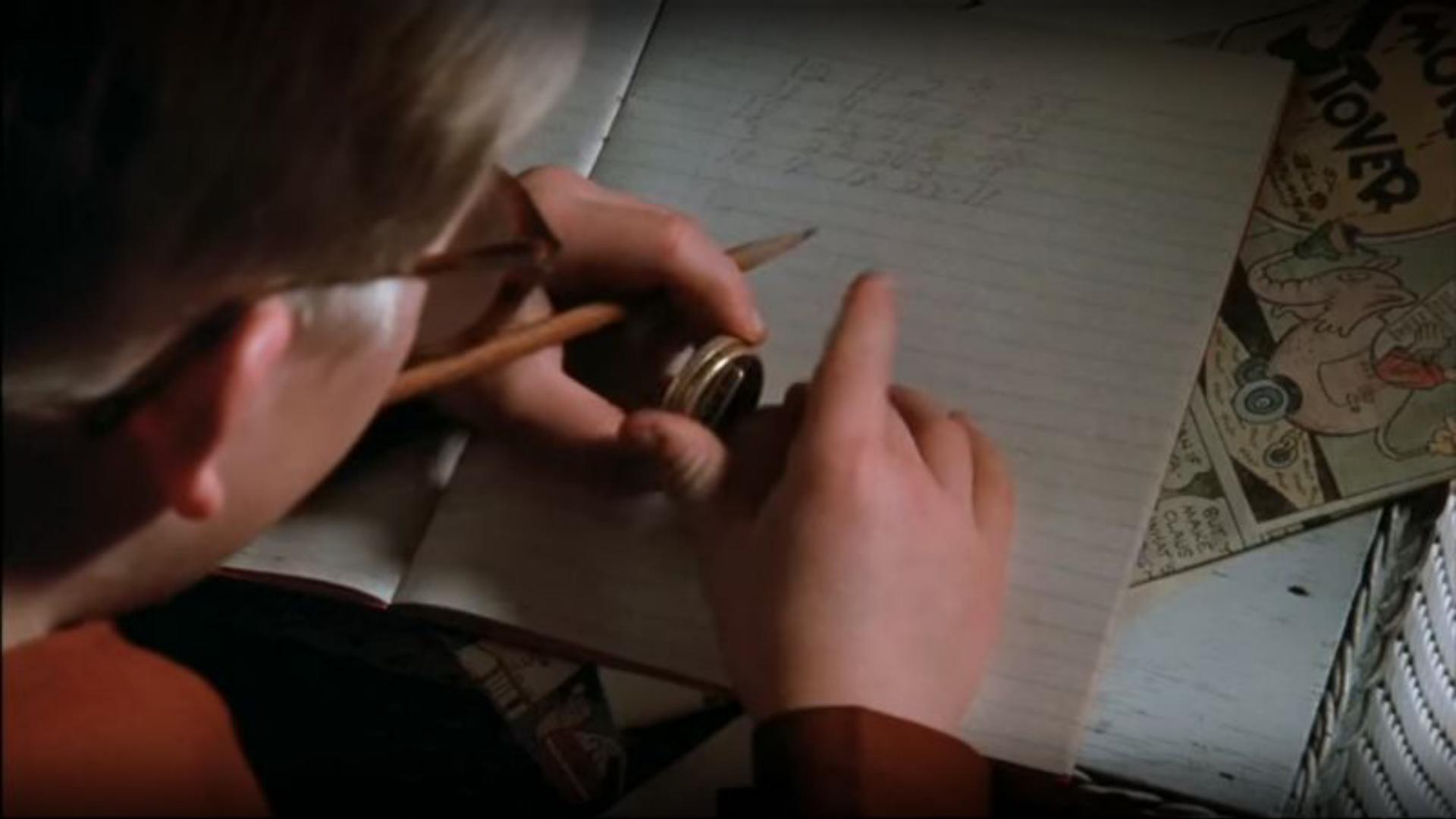
Encode

plaintext → codetext

Decode

codetext → plaintext

Ciphers



20 21 22 23
24 25

1940
1940



Encipher

plaintext → ciphertext

Encrypt

plaintext → ciphertext

Encryption

plaintext → ciphertext

Decipher

ciphertext → plaintext

Decrypt

ciphertext → plaintext

Decryption

ciphertext → plaintext

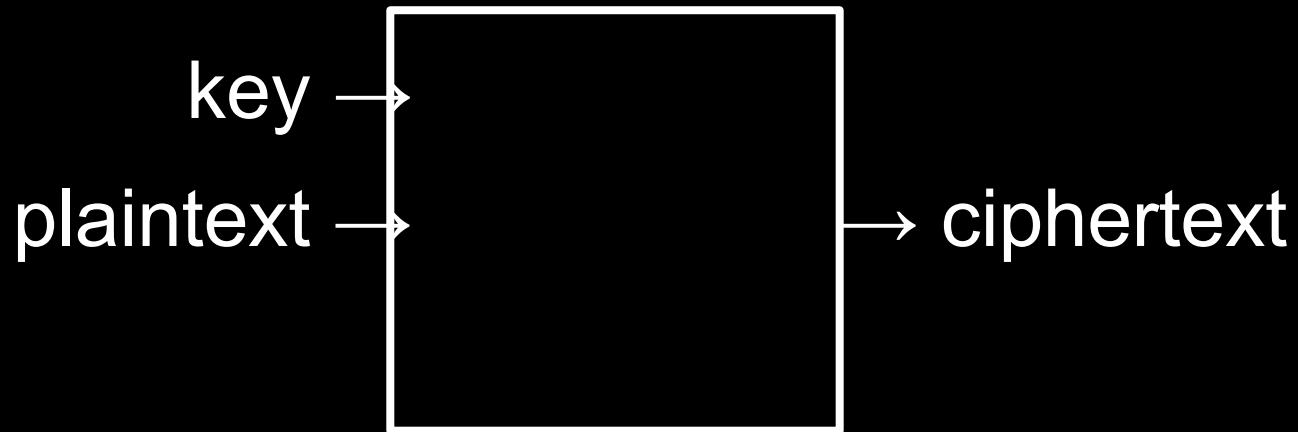
Keys

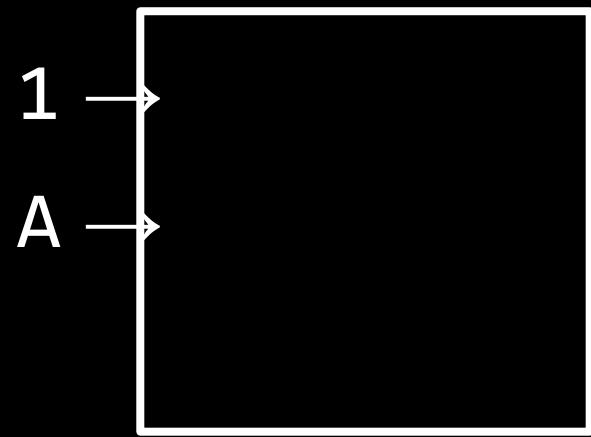
Secret-Key Cryptography

Secret-Key Encryption

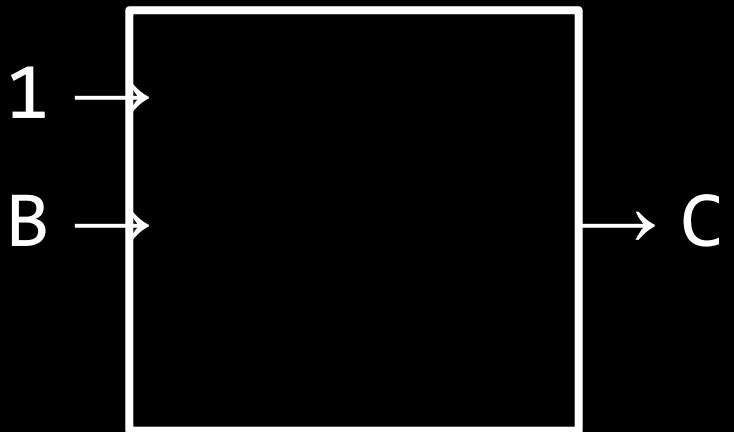
Symmetric-Key Encryption











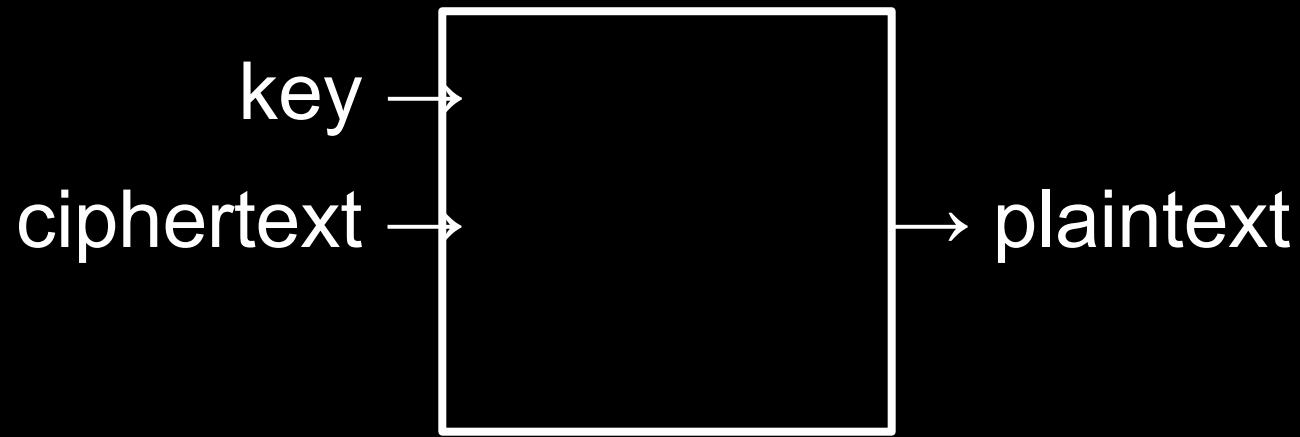






OR FHER GB QEVA~~X~~ LBHE BINYGVAR

Decrypting





OR FHER GB QEVA~~X~~ LBHE BINYGVAR

Cryptanalysis

OR FHER GB QEVA~~X~~ LBHE BINYGVAR

BE SURE TO DRINK YOUR OVALTINE

AES

Triple DES

...

Public-Key Cryptography

Diffie-Hellman
MQV
RSA

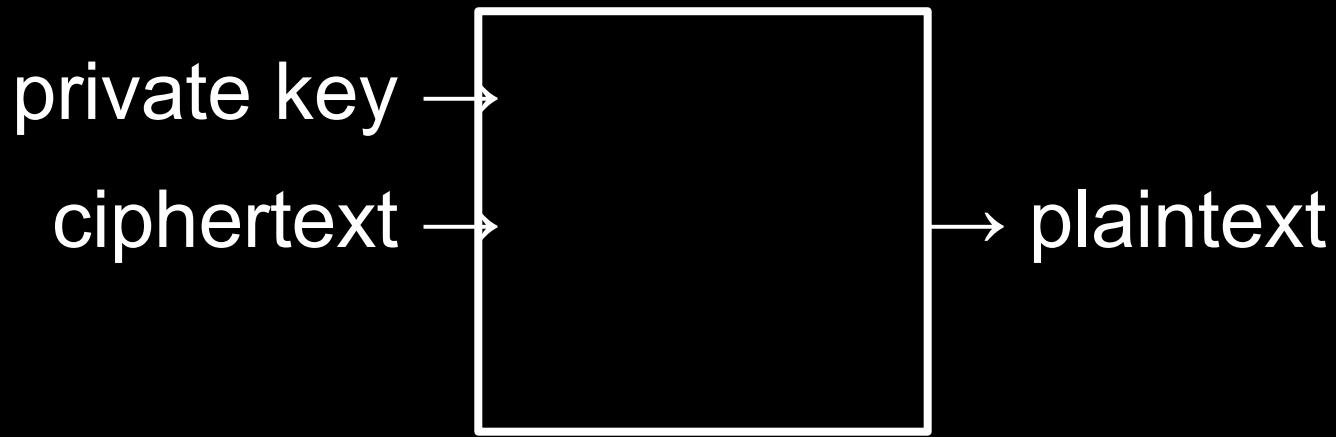
...

Public-Key Encryption

Asymmetric-Key Encryption







RSA

$$n = p \cdot q$$

...

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

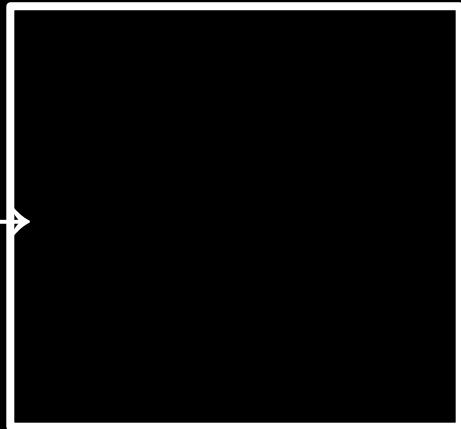
ECDSA

RSA

...

Sign

message →



→ hash

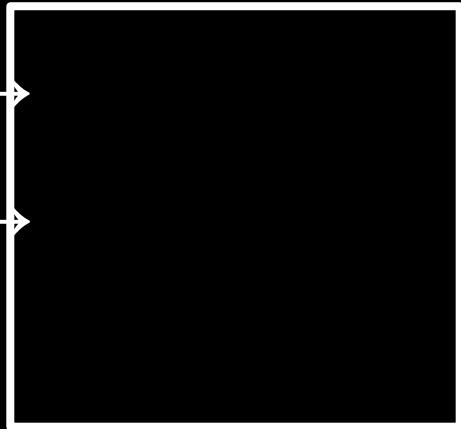
private key



hash

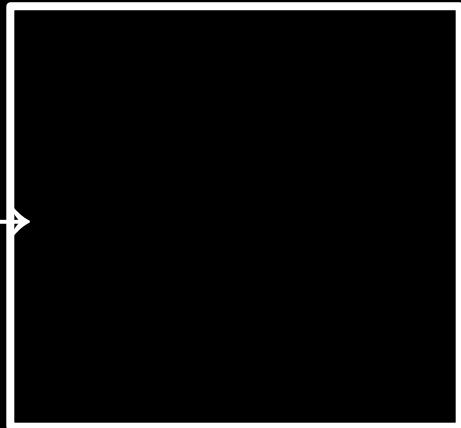


signature

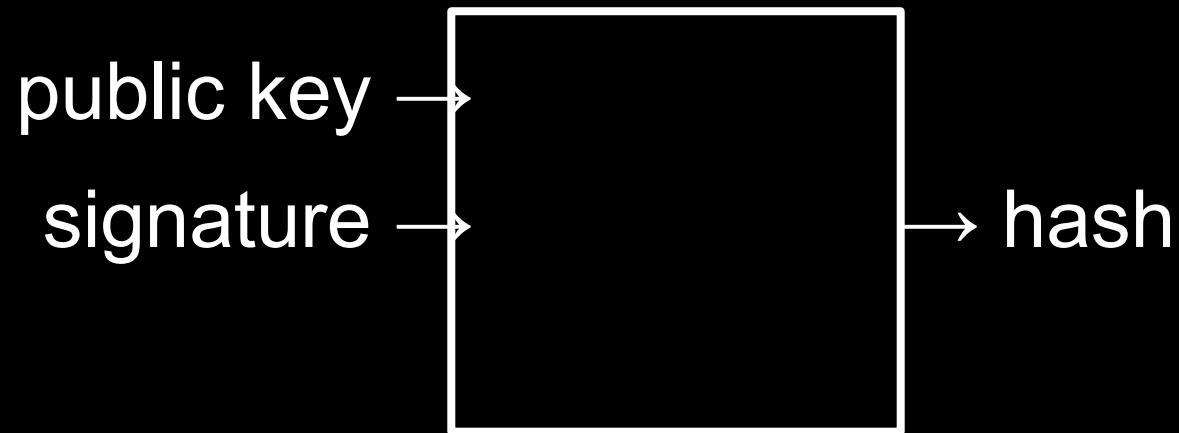


Verify

message →

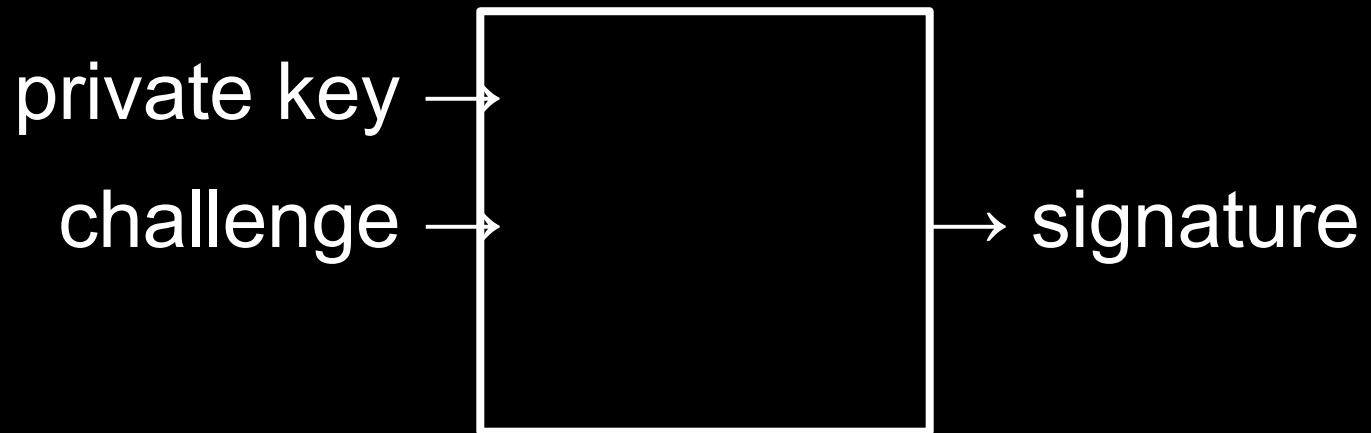


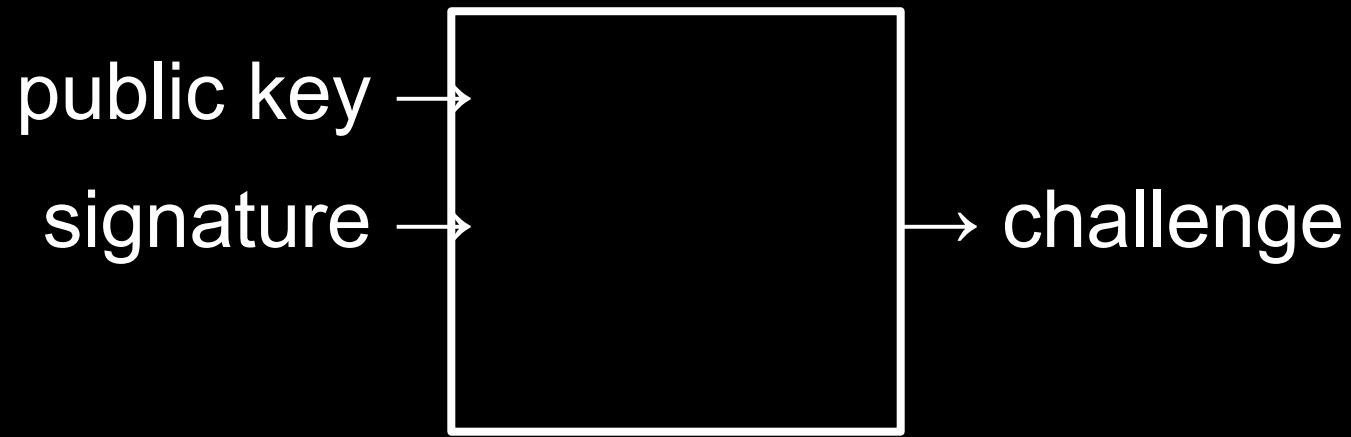
→ hash



Passkeys

WebAuthn





Encryption in Transit

Alice \leftrightarrow Eve \leftrightarrow Bob

End-to-End Encryption

Alice \leftrightarrow Bob

Deletion







Secure Deletion

Full-Disk Encryption

Encryption at Rest

0000111010101100000011011011010111110111000101000100111000011100010111010110100010101100001111010
111110110100111001100011000010111100011000010101010001100001111000101001010110110011110110001
11010100000101100101010111101101100011001100011011110101011010001011011001101001111010011010
001110101001000101111110011111011011100111101111111101000110011010011011011110011111000
10111010011011011110110011011000000100010110111110110111101110111001110011011001011011000111101001
101001101110100111011110000101111100001001100100011011101011010010111000111011000101010111001001100
100000110000011100001110111011101000110110100100011010011000101001011100101001001011000100010
0010111000011000100001101000001101111011100100111111111101101000010010011111001011011001011
001100000001111011011110101110100101000010010001001010110100001010001010110001000100100100
0001110100110110001110111110011001001100100100111111001000100111110101001111101011111111101101110
11100110101110001010000110010010111011100101000000110111000010101010110011101000100000000110010001
00101001010001110011010011110010001110100101110000011110110010110010111110101101011000011010010010111
001100001011101101011011100010011010111100100111001111011110001011111011000110000100010001110
11101101001110011001111100010011000111111101100000000010010001001101000101001010101100011000000100
1001111010000111100101111000011010010111010100101111011100101111111000011011011010010000101010110111
00101001010011100011011111010111101110010111100011110100010000111011100110000100101110100111001100100
011101000011101101010000010001111111011100101001101101001101110100011001000011100000101010000101000
010011110010100000100000100100110111100101000101100111111100110101001100001111011011100111101010
101000000111001100100000010101001000010011000001111111011000110111111101101111001100100001111010010001
10110111000001110111110111110001110000110111000101011010011000000011100010110100110100000000111101
100111010010010110100110111111000011110000111000001010010101101111110011001010011001010101101
011101000010110110001110111110011110001101010000011001110100101111000010001011100001001001010100
11110100111110100011001110000001011010010001110001010001011010011011011011111101011000001101111
01101011110100001011001101001010101011000000010110001101111000010011100101010110100001011100001010
01100011110001000011011110111110001010011111111000011100000010101100111100011001000011110110100101
011011110010011001001101111110001001100000101100000100100110111100011001000110101011100001101001

Ransomware

Quantum Computing

Introduction to Cybersecurity

David J. Malan
malan@harvard.edu