

Introduction to  
**Cybersecurity**

David J. Malan  
malan@harvard.edu

# Securing Data

Passwords

alice:apple

bob:banana

...

alice:apple

bob:banana

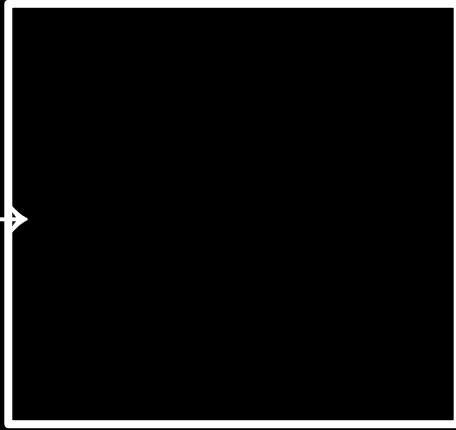
...

# Hashing

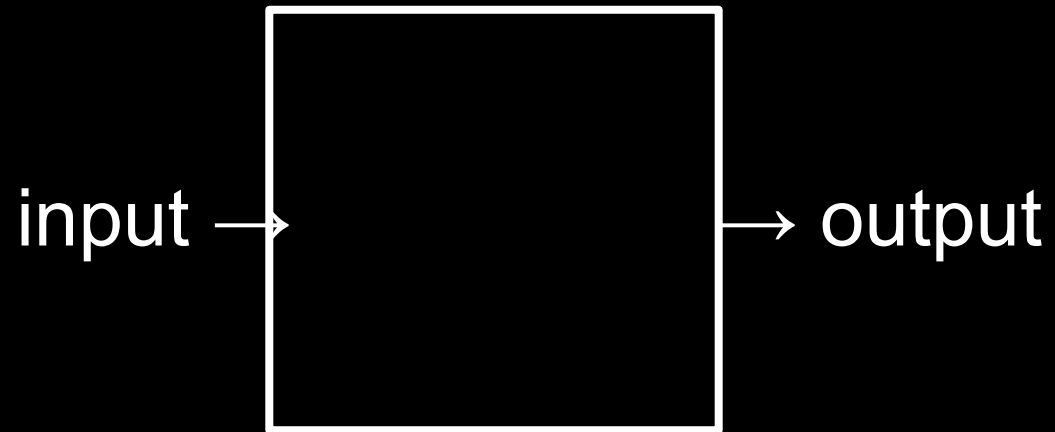
password → hash

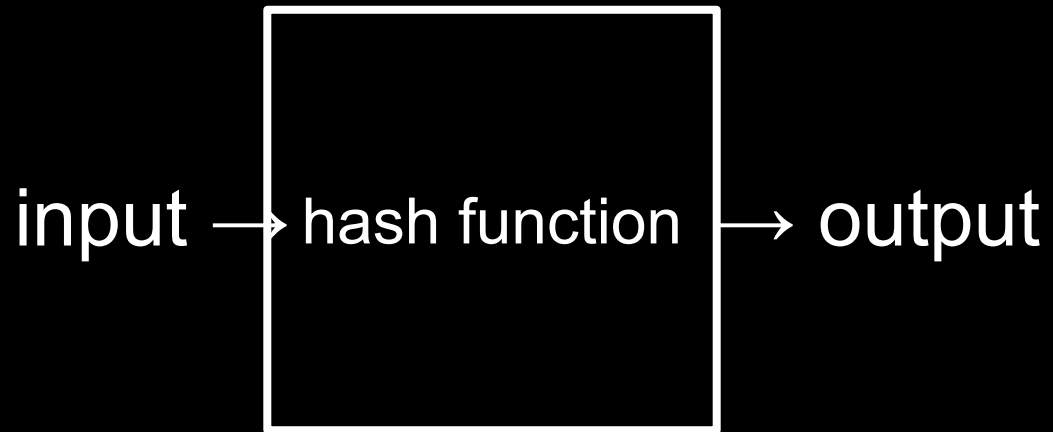


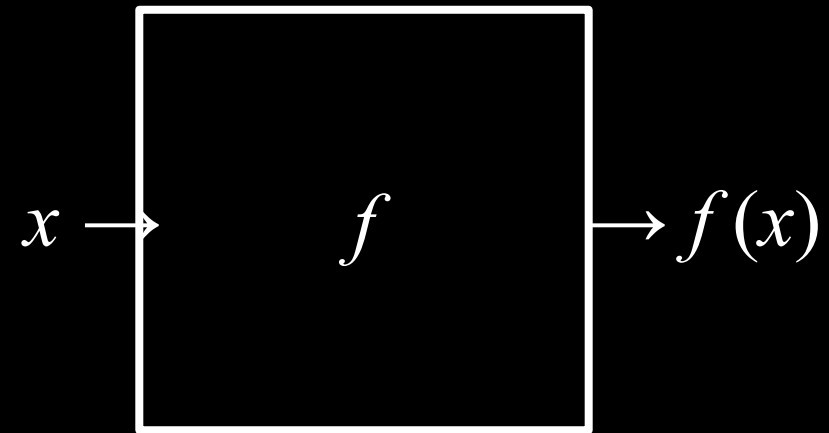
input

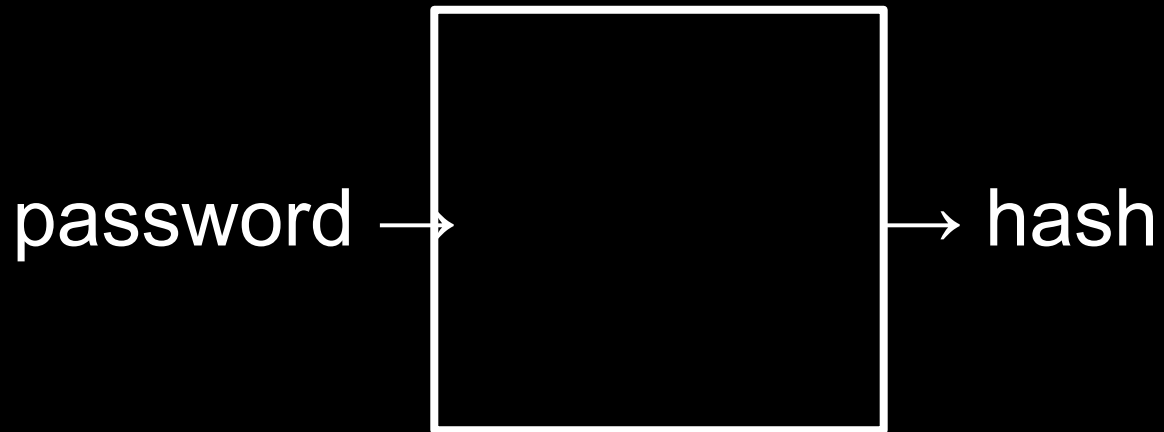






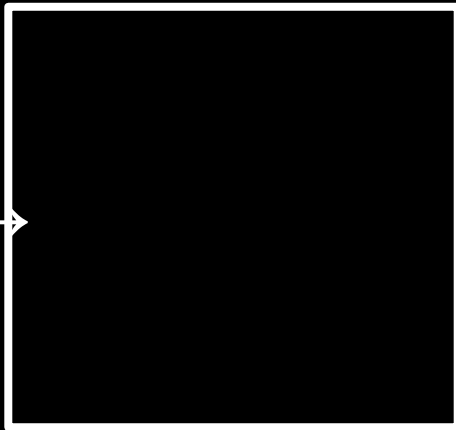




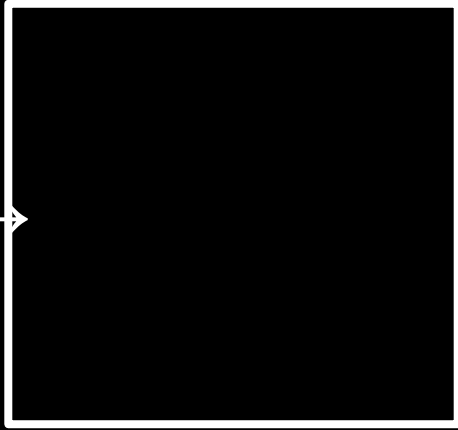




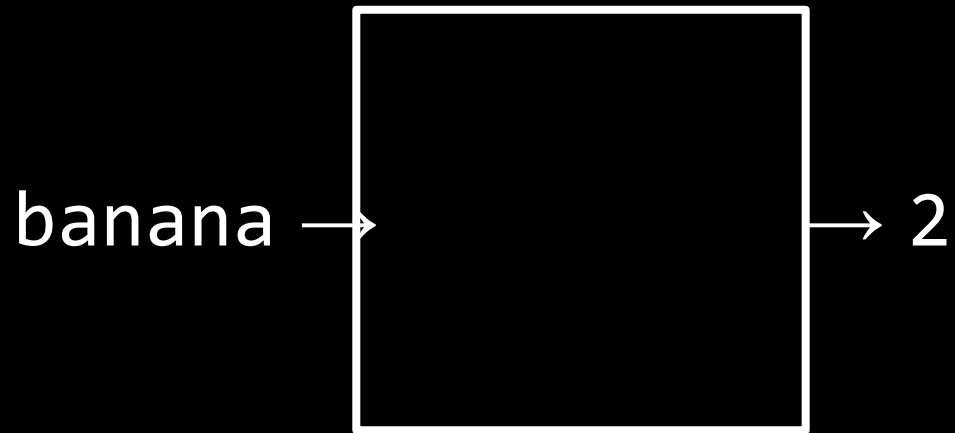
apple →



apple

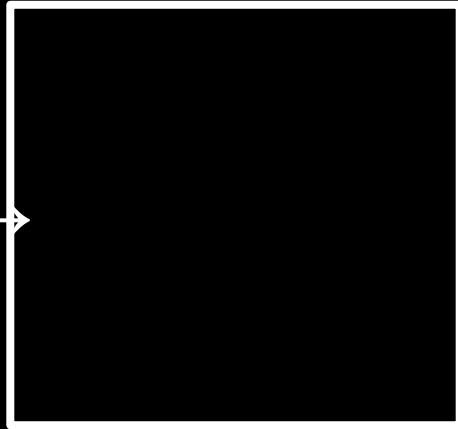


1





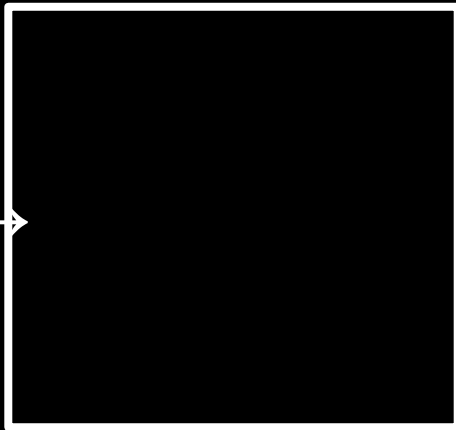
cherry

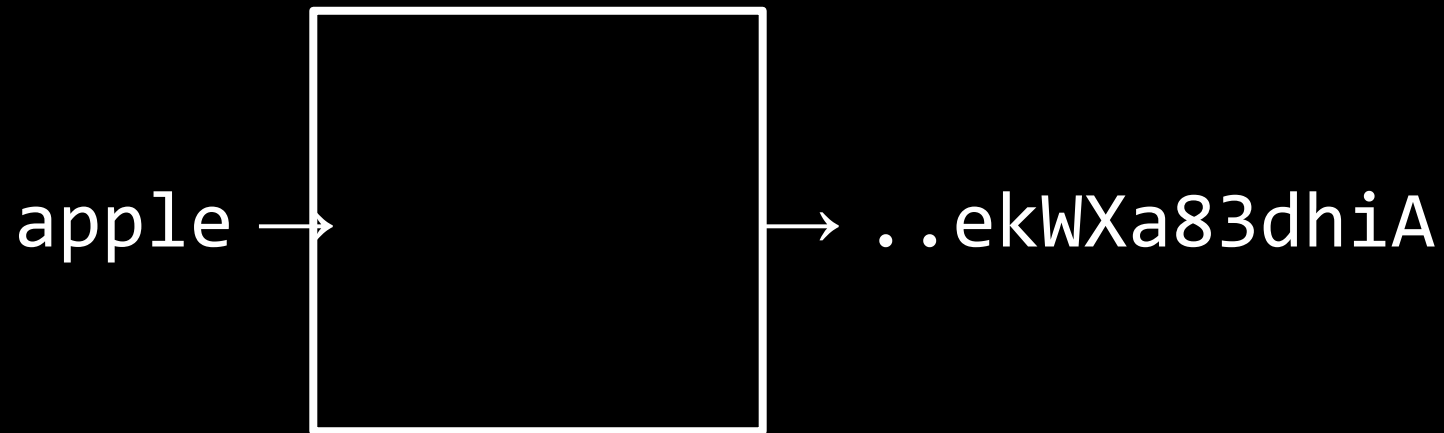


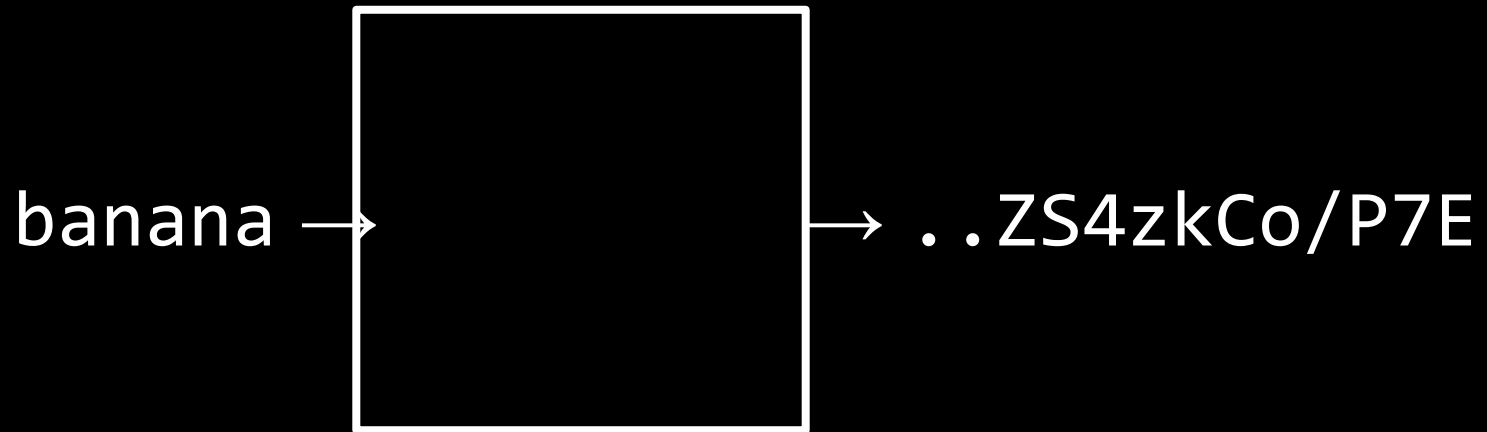
3



apple →







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

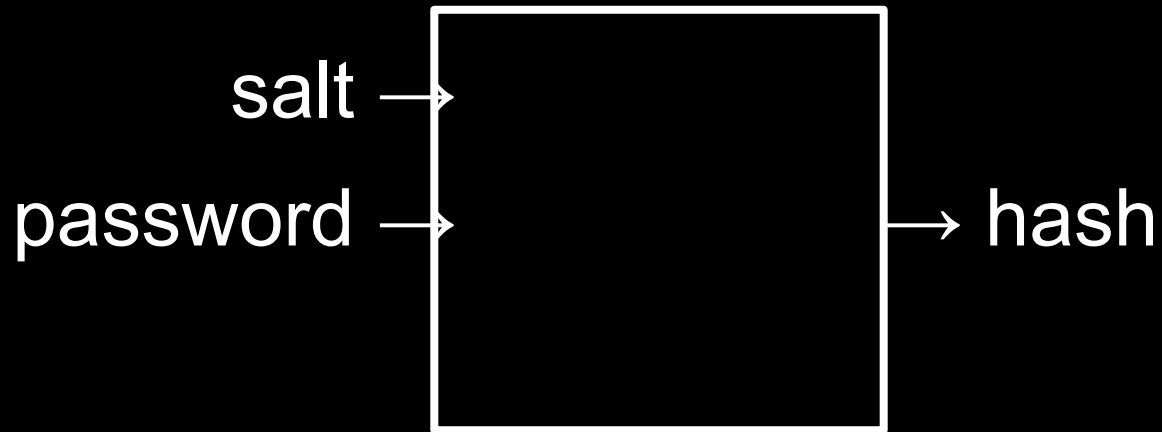
bob:..ZS4zkCo/P7E

carol:..rj98gxDTYfM

charlie:..rj98gxDTYfM

...

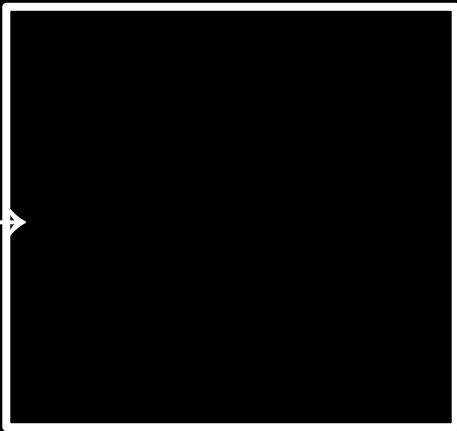
Salting

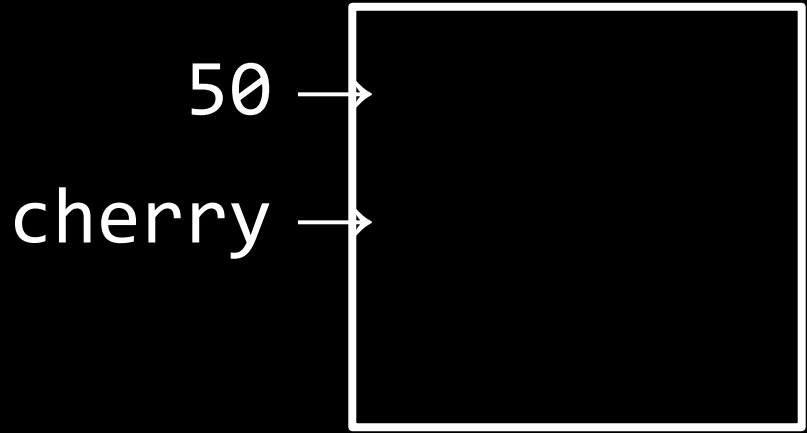


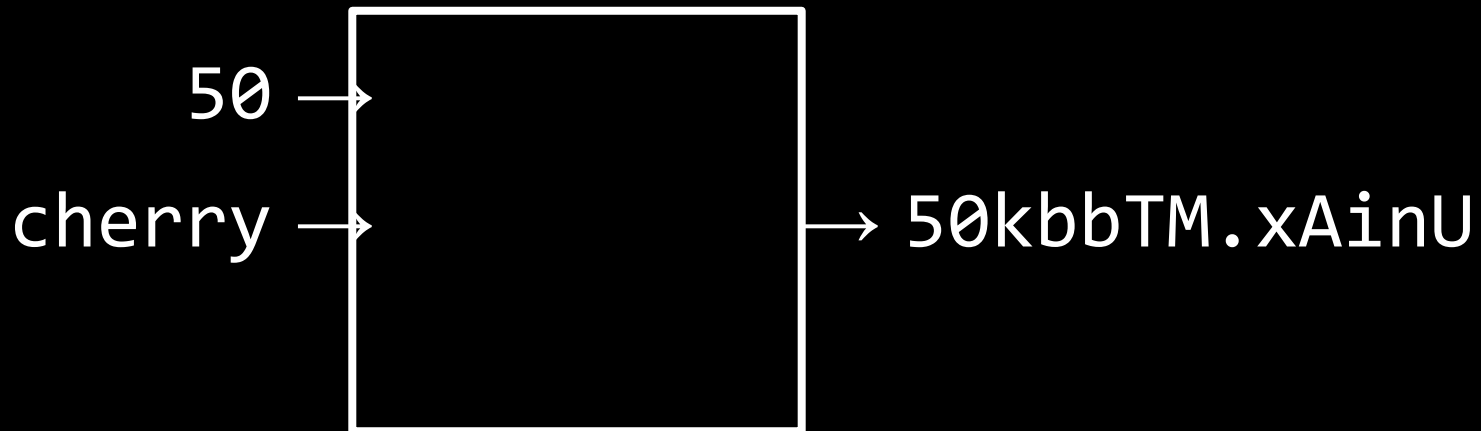


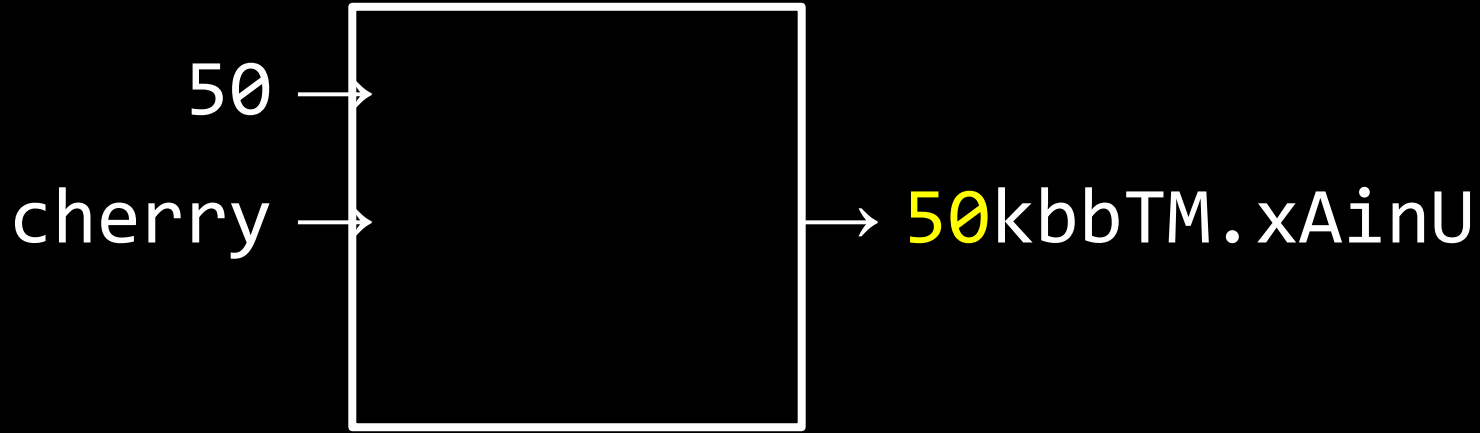


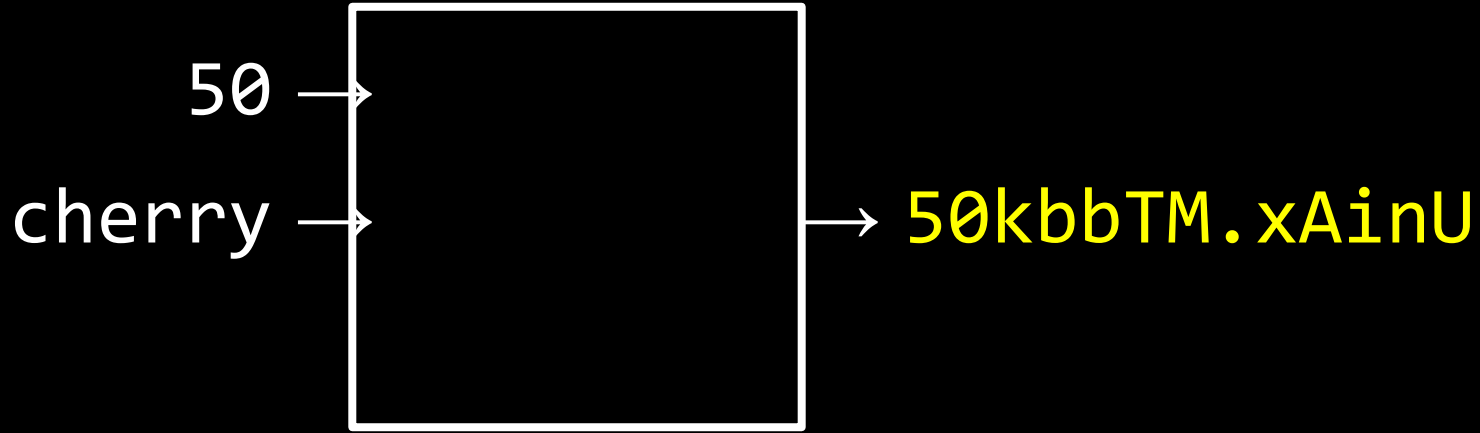
cherry

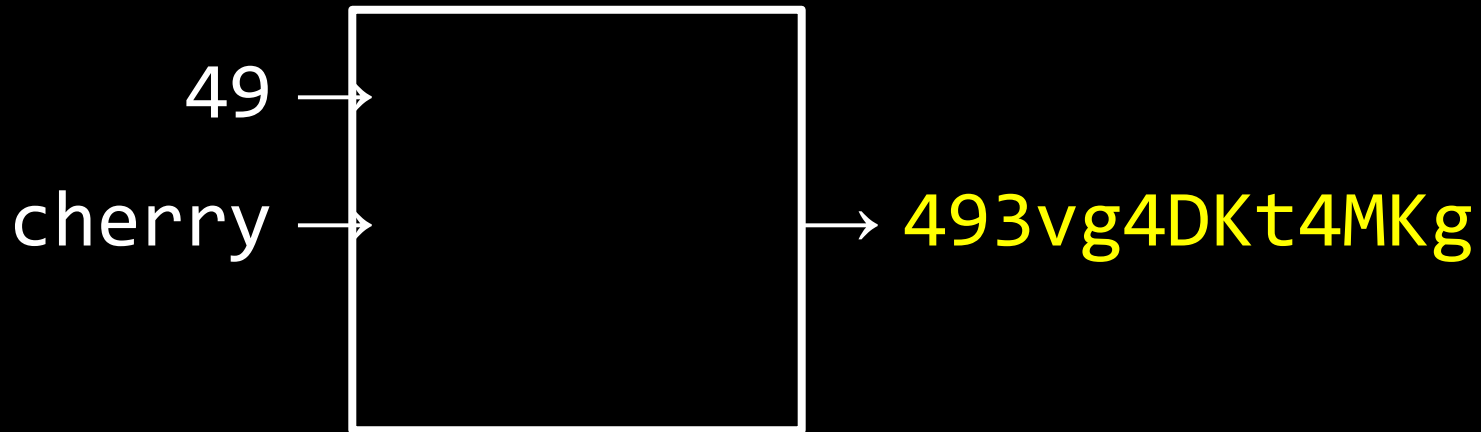


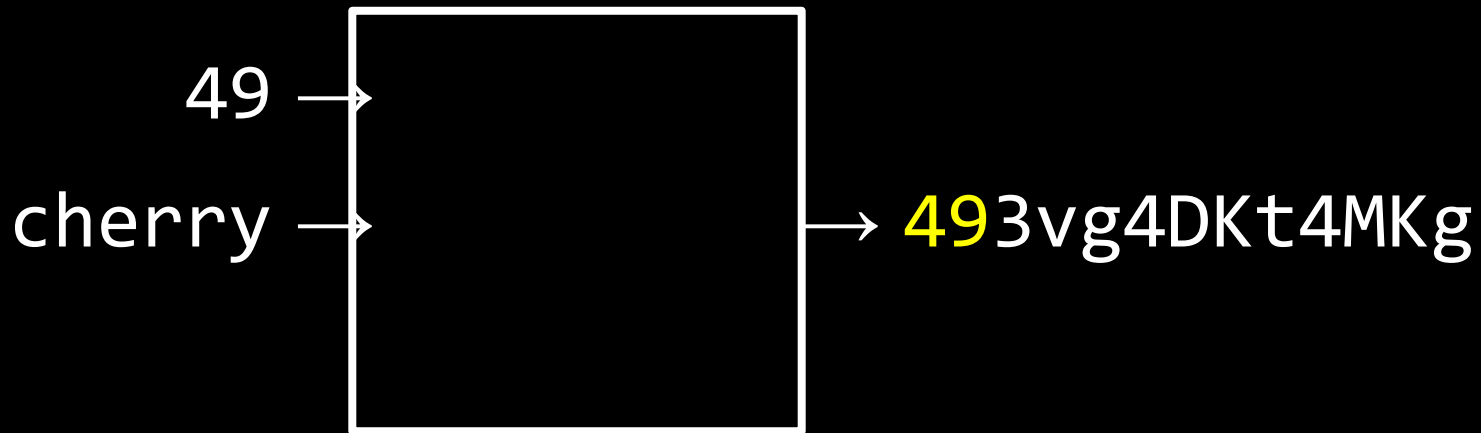












alice:..ekWxa83dhiA

bob:..ZS4zkCo/P7E

carol:50kbbTM.xAinU

charlie:493vg4DKt4MKg

...



alice:\$y\$j9T\$DIXfskUxbz6we5RbfdPCz0\$zFd93JMuTyEJHrdIf.6bZ8Rbw4otHvybdOuLn.eD.s3  
bob:\$y\$j9T\$ty3B9GwDhm4f6zQIgm9uL.\$SbFq.iSFt48A5iQ1ue8DtUd.57KaBN1tIEdLPmtEjwC  
carol:\$y\$j9T\$hqOZx7o4Ts0wyCx0/Yct5/\$bMqofMaf6jnOZFS.gT8jXw7gGI1SM5L1DjR77cm.xt2  
charlie:\$y\$j9T\$wf55sBgrrZfj2K.2kcV0d.\$gzmxkKEQRkVKoCHw0dvYefnT/XZ4VyS9sy1QN6M7Kr6

...

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

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  $\rightarrow$  fixed length

# Cryptographic Hash Functions

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

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
Canterings	53	Authorization
Canteris	54	Authorizations
Canthook	55	Authorize
Canthook	56	Authorize them to
Canthook	57	Authorize us to
Canthook	58	Authorize you to
Canthook	59	Do not authorize
Canthook	60	Do they authorize
Canthook	61	Do you authorize
Canthook	62	I authorize
Canthook	63	They authorize
Canthook	64	They will not authorize
Canthook	65	To authorize
Canthook	66	Will authorize
Canthook	67	Will not authorize
Canthook	68	Will you authorize
Canthook	69	Authorized
Canthook	70	Am authorized to
Canthook	71	Are authorized to
Canthook	72	Are not authorized to
Canthook	73	Are they authorized to
Canthook	74	Are we authorized to
Canthook	75	Are you authorized to
Canthook	76	Duly authorized
Canthook	77	Is authorized
Canthook	78	Is he authorized
Canthook	79	Is not authorized
Canthook	80	No more authorized
Canthook	81	Not authorized
Canthook	82	Not authorized to
Canthook	83	Properly authorized
Canthook	84	They are authorized to
Canthook	85	They are not authorized to
Canthook	86	Was authorized
Canthook	87	Was not authorized
Canthook	88	We are authorized to
Canthook	89	We are not authorized to
Canthook	90	You are authorized
Canthook	91	You are authorized to
Canthook	92	You are authorized to answer
Canthook	93	You are authorized to assure
Canthook	94	You are authorized to convey
Canthook	95	You are authorized to state
Canthook	96	You are hereby authorized
Canthook	97	You are hereby authorized to
Canthook	98	You are not authorized
Canthook	99	Authorizes

# Encode

plaintext  $\rightarrow$  codetext

# Decode

codetext → plaintext

# Ciphers







24  
25  
1940  
MADE IN U.S.A.  
WIND-UP



# Encipher

plaintext → ciphertext

# Encrypt

plaintext → ciphertext

# Encryption

plaintext → ciphertext

# Decipher

ciphertext  $\rightarrow$  plaintext

# Decrypt

ciphertext  $\rightarrow$  plaintext



# Decryption

ciphertext  $\rightarrow$  plaintext

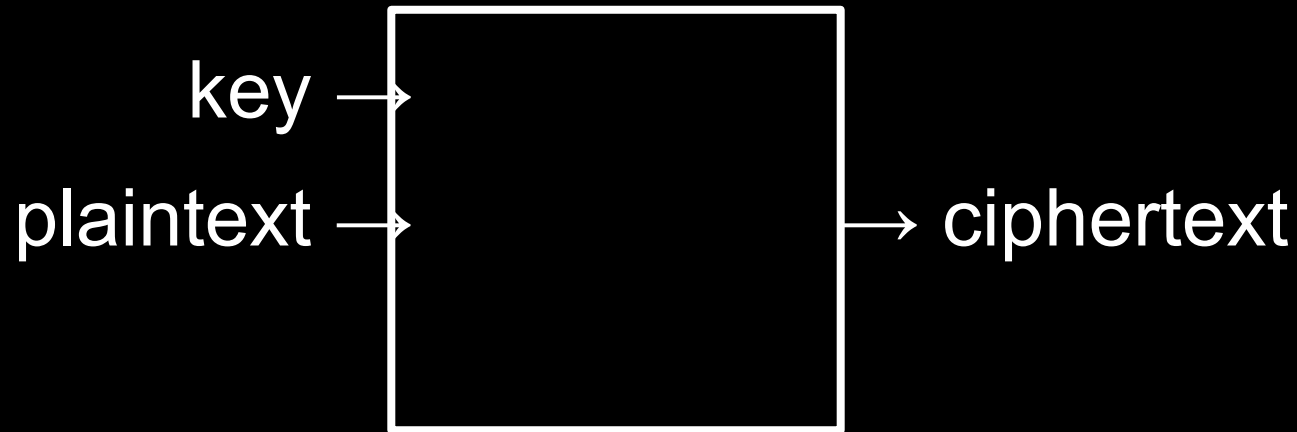
Keys

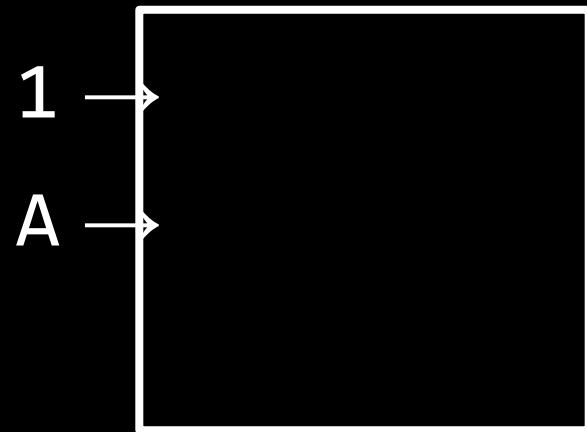
# Secret-Key Cryptography

# Secret-Key Encryption

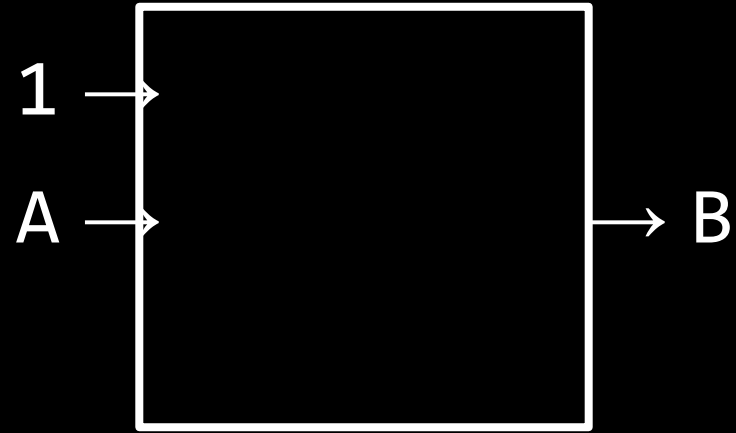
# Symmetric-Key Encryption





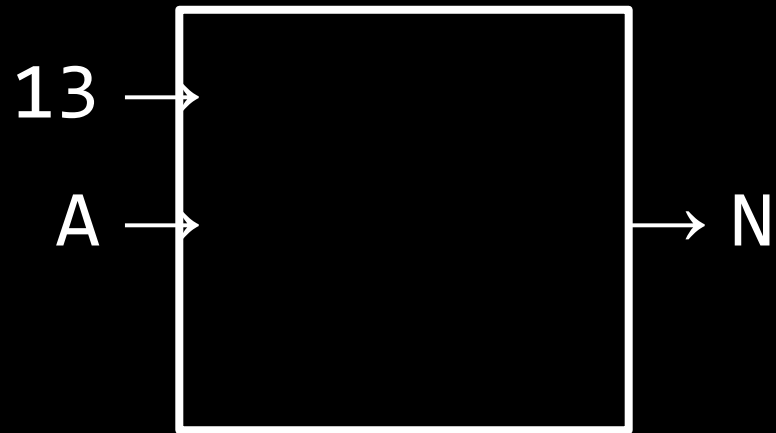


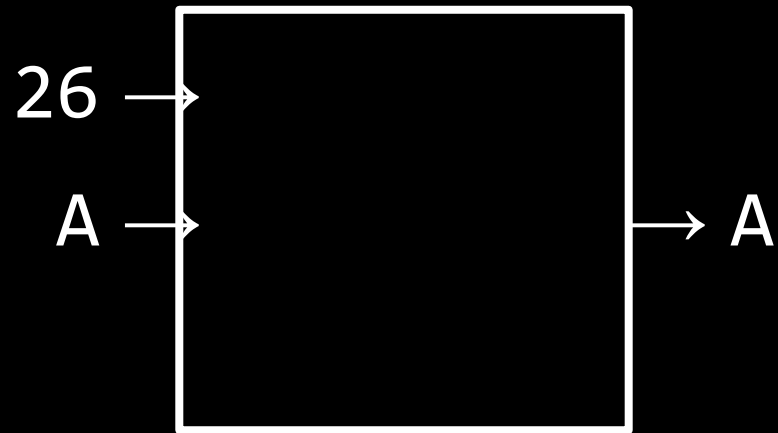






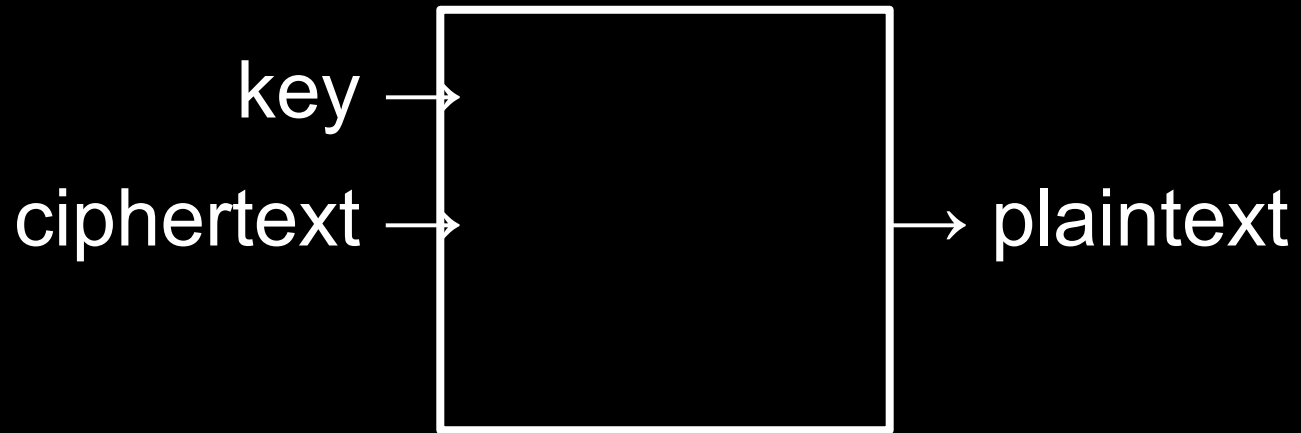




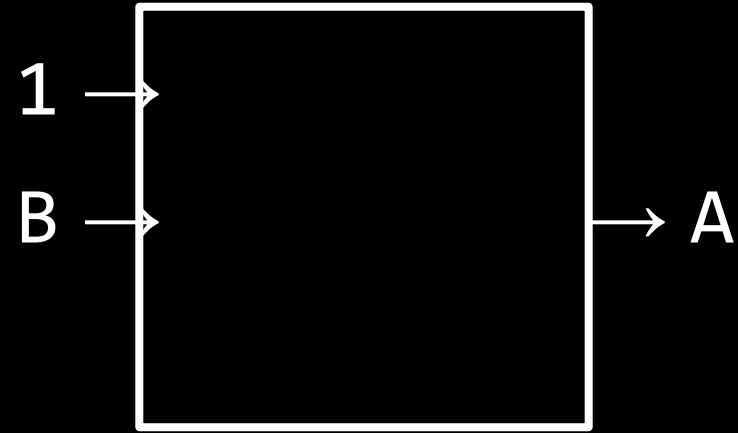


OR FHER GB QEVAX LBHE BINYGVAR

Decrypting







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

...

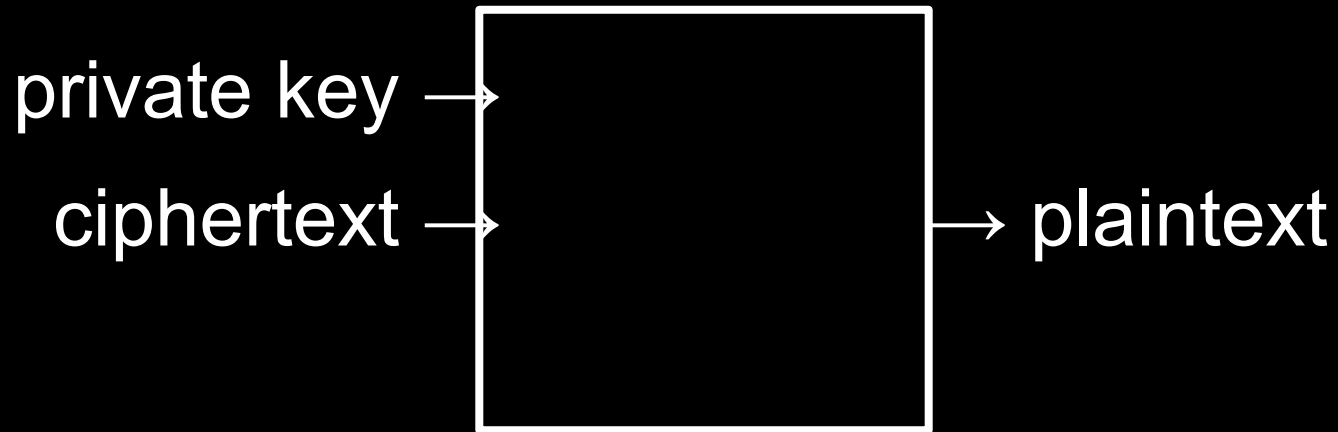


# Public-Key Encryption

# Asymmetric-Key Encryption







# 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

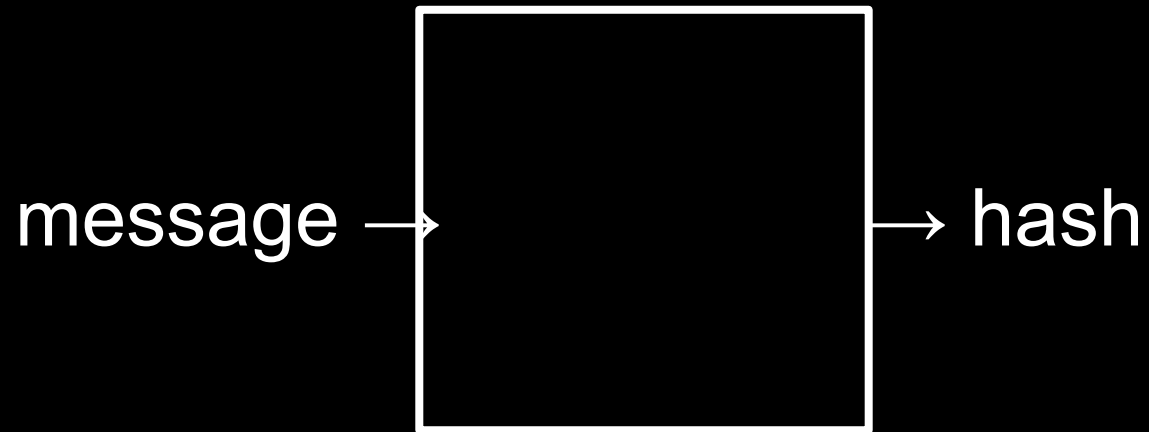
$$s = g^{ab} \bmod p$$

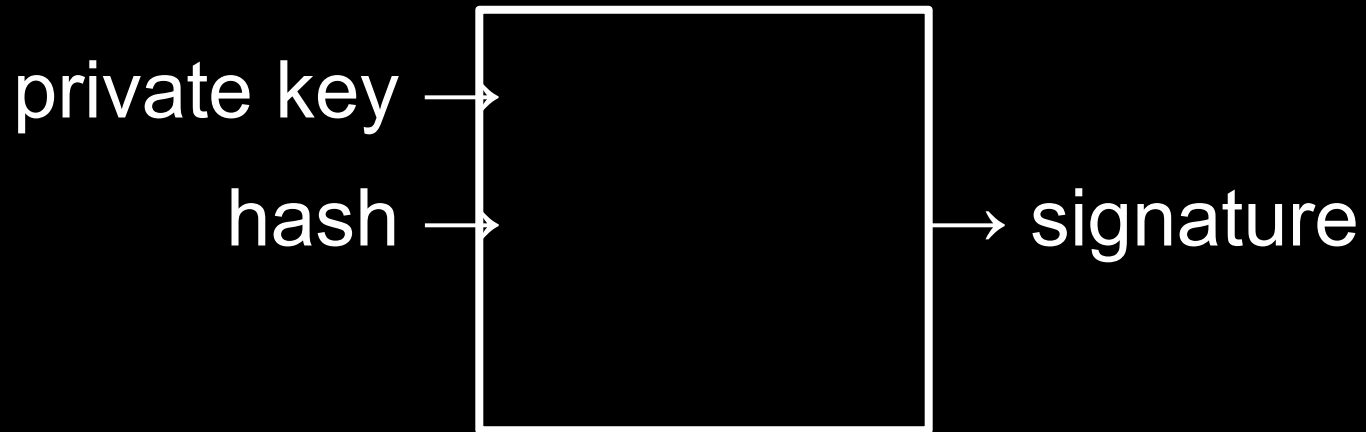
# Digital Signatures

DSA  
ECDSA  
RSA

...

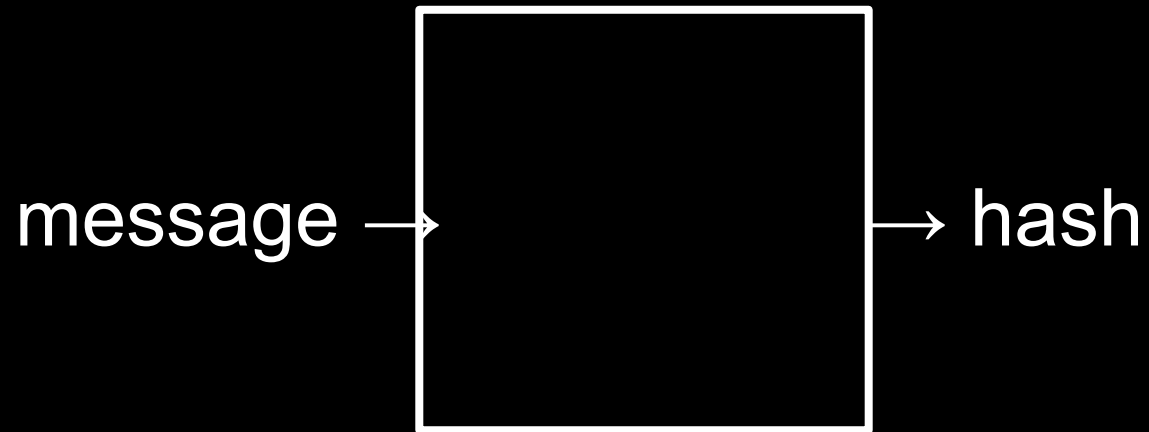
Sign

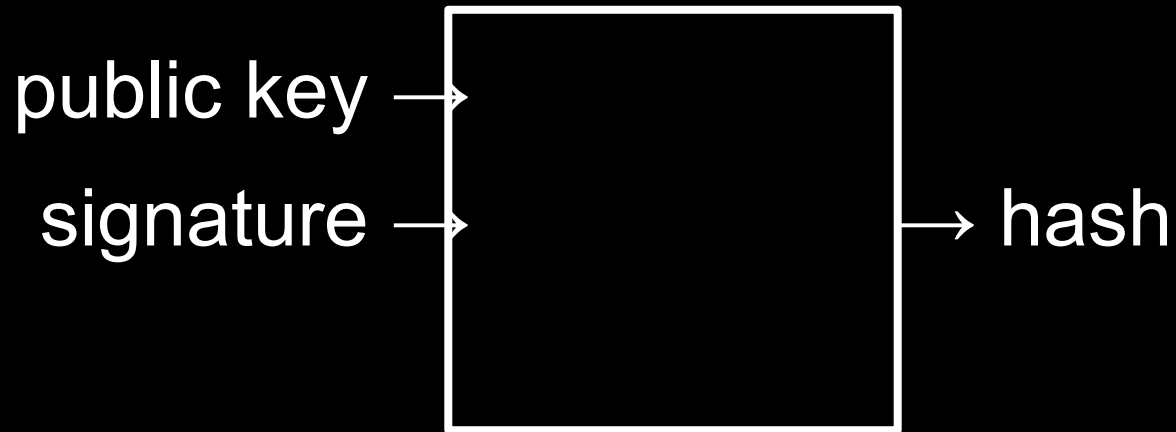






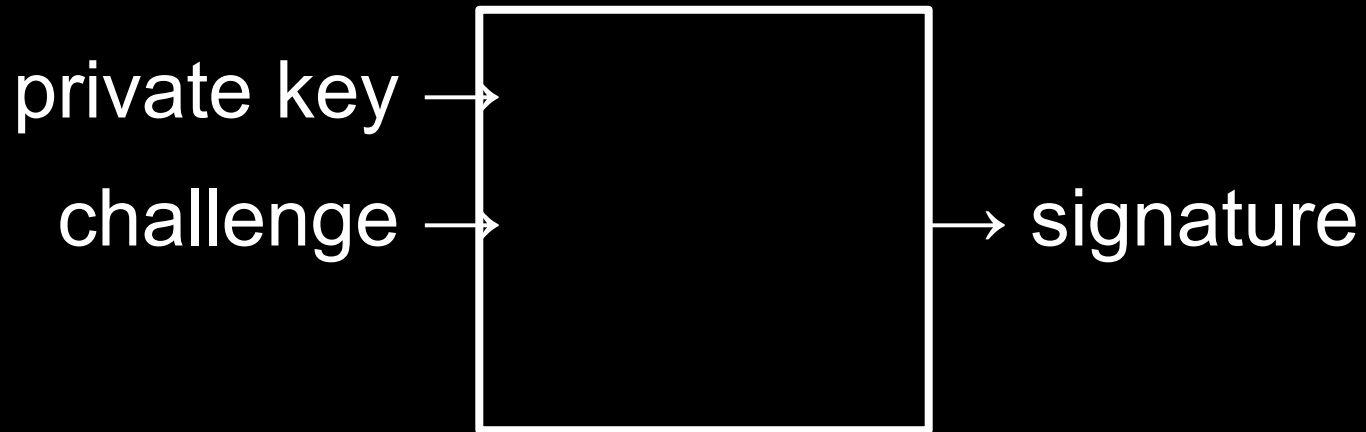
Verify

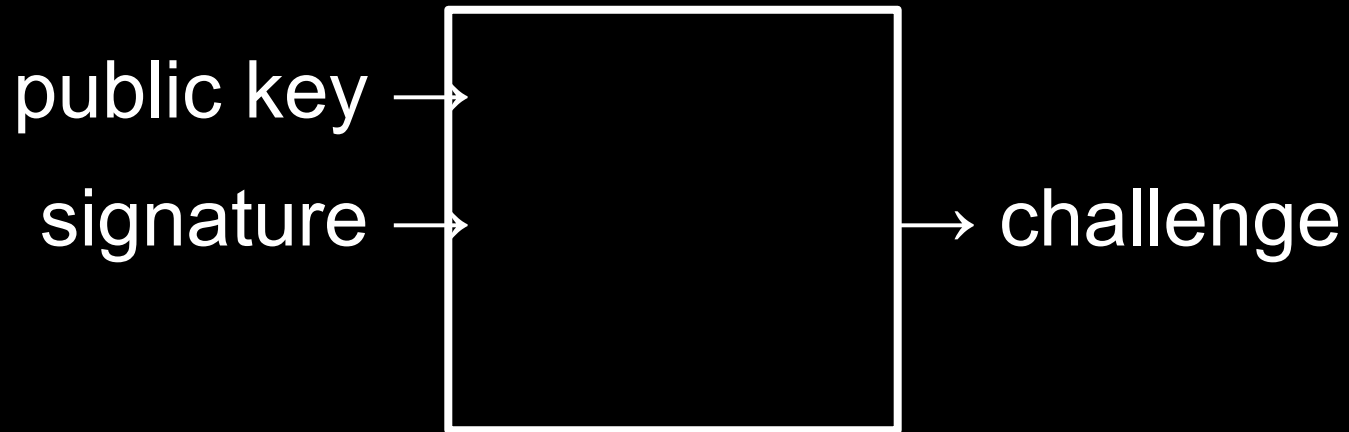




Passkeys

WebAuthn





# Encryption in Transit

Alice ↔ Eve ↔ Bob



# End-to-End Encryption

Alice ↔ Bob

Deletion















# Secure Deletion











# Full-Disk Encryption

# Encryption at Rest





0000111010101100000011011011101101101111110111000101000100111000011100010111010110100010101100001111010  
1111110110100111001100011000010111100011000001010101000011000011110001010010101101110011110111001100001  
1101010000010110010101011111011011000110011000110111110101010111010110000101101100011010011111010011010  
00111010100100001011111100111110110111001111001111011110111111111110100011001101100110110111100111110000  
101110100110110111101100110110000000100010110111111011011111011100111001101100101101100001111010001  
1010011011101001110111100001011111000001001100100001101110101101001011100011101100010101011100100101100  
10000011000001110000111011101110100001101101010010001100011010011000101001011100101001001011000100010  
001011100001100010000110100000110111101110011111000100111111111100110100000100100111110001011011001011  
001100000000111101101111010111011010010001010000100100001000101010110100000101000100100100100  
00011101001101100111000111011111100110010011001001010001001111110010001001111101011111111110110111101  
11100110101110001010000110010010101110111001010000000110111000010101011001110100001000000001100100001  
0010100101000111001101001111001000111101001111000001111011001011001011111010110101100000110100100101111  
001100001011101101011011101110001001101101111001110001001111011110001011111011000110000100010001110  
11101101001110011001111100010010110001111111011000000000010010001001101000101001010101100011000000100  
1001111010000111100101111000011010011010111010100101111011100101111111000011011011010010000101010110111  
0010100101001110001101111101011110111001011110001111010001000011101110011000010010111010011100110010010  
0111010000111011010100000100011111110111001010011011011001101111010001100100001110000010101010000101000  
0100111100101000001000001001001101111001010001000010110011111111100110101001100001111011011100111101010  
101000000111001100100000010101001000010011000001111111011000110111111101101111001100100001111010010001  
1011011100000011101111101111100011100001101110001010110100110000000011100010110100110110000000001111101  
1001101100100100110100110110111111100001111000011100000101001010011011111110011001010011001010010110101  
0111010000101101110001110111110011110011100110101100000011001110100101111000010001011100001001001010100  
11110101001111101000110011100000001011010010001110001010001011010011011011011111101011000001101111  
0110101111010000101100110100100101010101100000000010110001101111000010011100101010110100001011100001010  
011000111100010000110111101111101000101001111111110000111000000101011001111000110010000011110110100101  
0110111100100110010010011011111100100110110101000111111100010110000001001001001101011100001101001011101



Ransomware

# Quantum Computing

Introduction to  
**Cybersecurity**

David J. Malan  
malan@harvard.edu