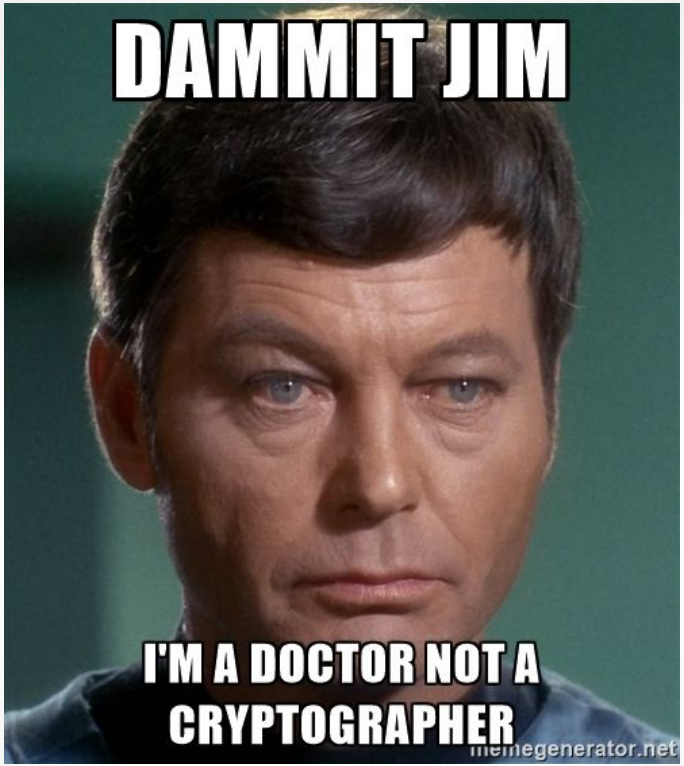
Papers We Love $f(x)=x$

New Directions in Cryptography
+
A Method for Obtaining Digital Signatures and Public Key Cryptosystems


DAMMIT JIM
I'M A DOCTOR NOT A
CRYPTOGRAPHER
memegenerator.net

DISCLAIMER

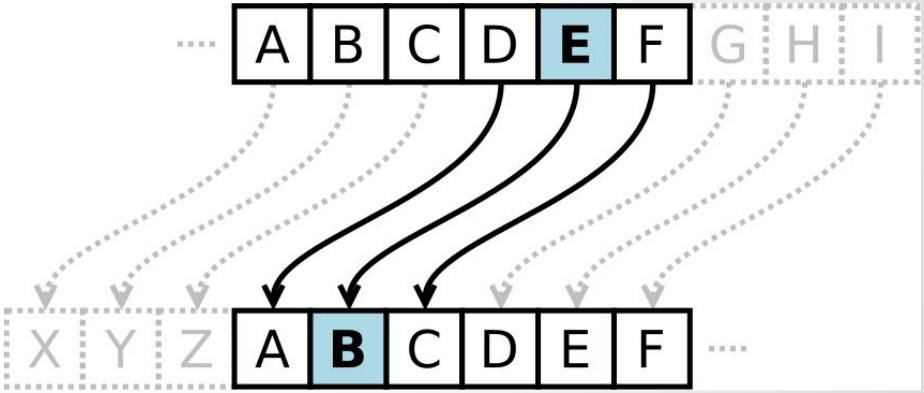
A Brief* History of Cryptography

* Oversimplified, Incomplete, Probably Wrong

Caesar Cipher

M: ATTACKATDAWN

E: XQQXZHXQAXTK

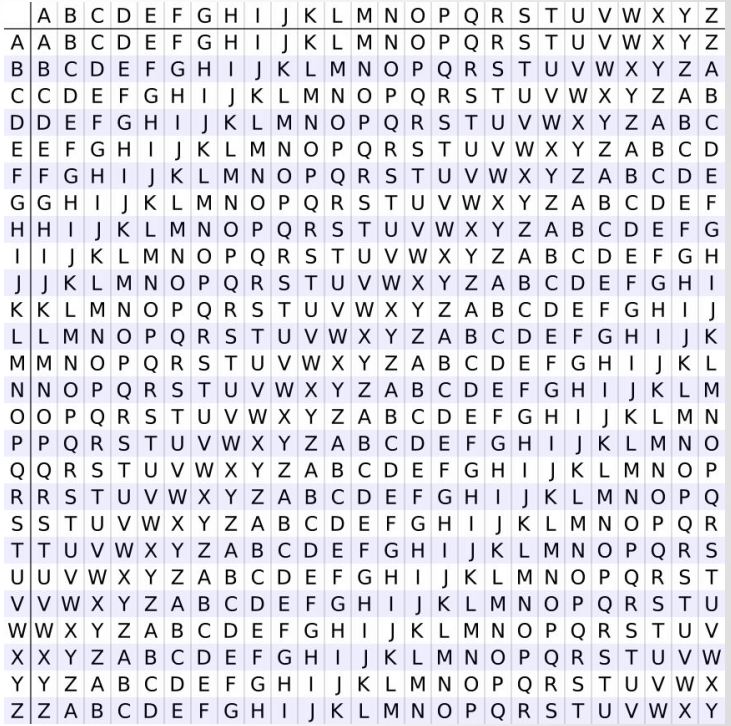


Vigenère Cipher

M: ATTACKATDAWN

K: LEMONLEMONLE

E: LXFOPVEFRNHR



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

A Mathematical Theory of Crypto

- T_k: {M} -> {E} ;; T_k^{-1}: {E} -> {M}
- $T_k^{-1}(T_k(M)) = M$

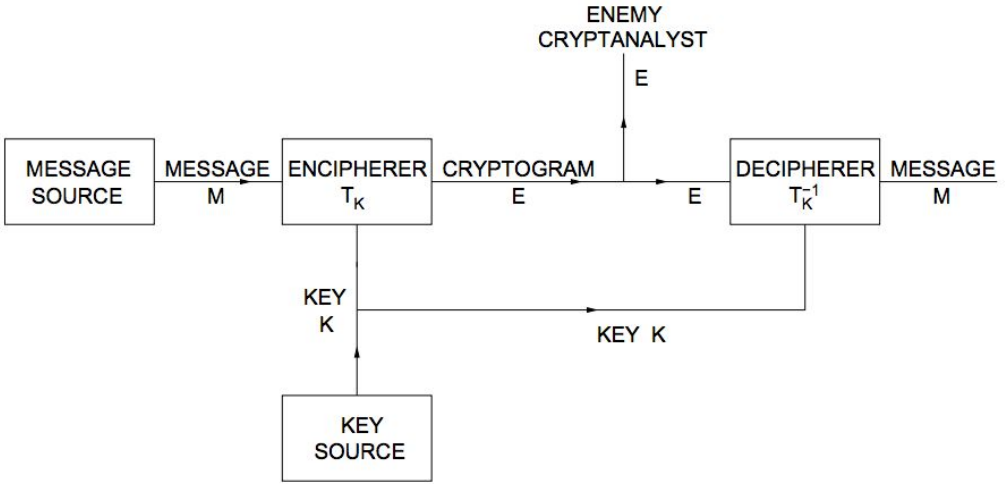


Fig. 1. Schematic of a general secrecy system

New Directions in Cryptography

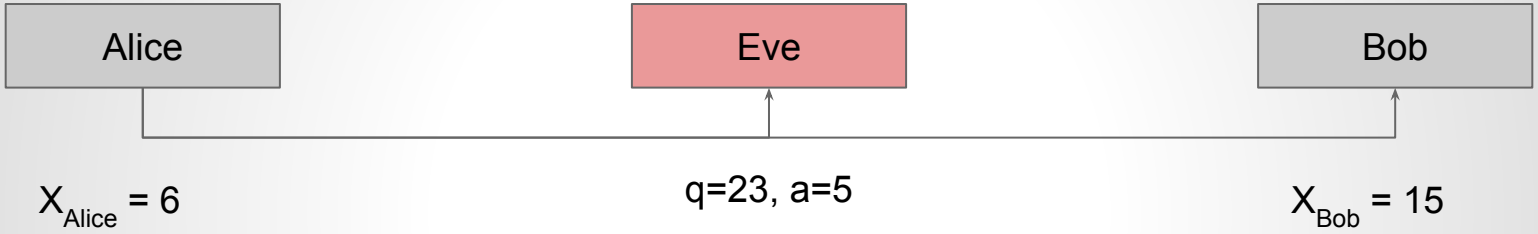
Whitfield Diffie and Martin E. Hellman

New Directions in Cryptography

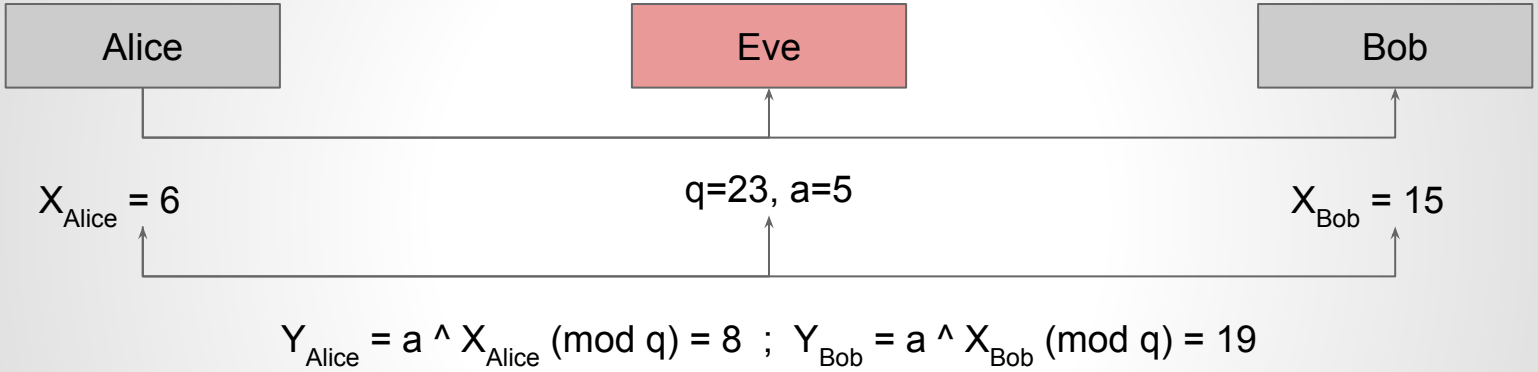
- It’s 1976
- ARPANET’s a thing (‘69)
- The Internet/email are coming soon
- They should probably be secure?
- The crypto we know won’t do it

Public Key Exchange

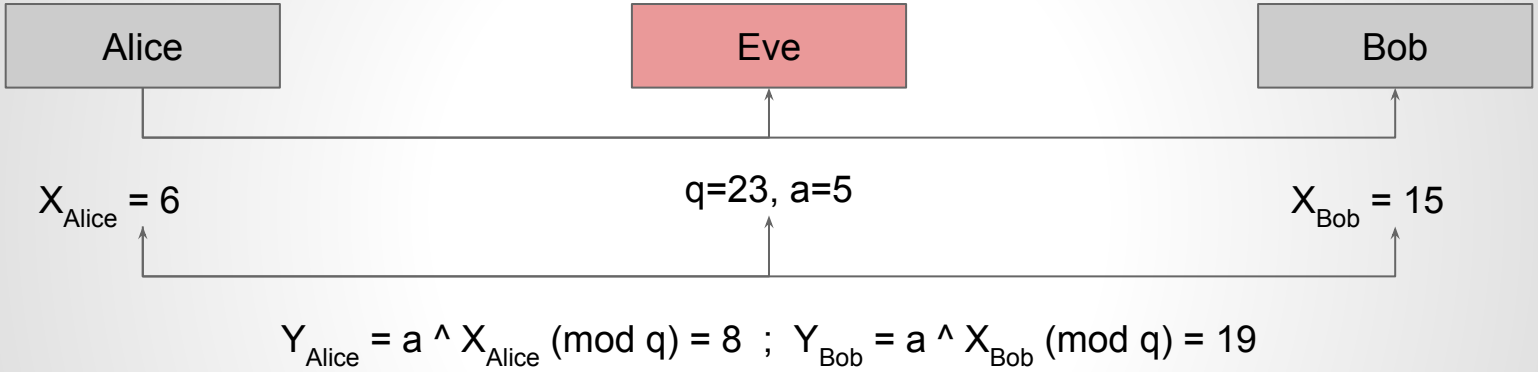
Public Key Exchange

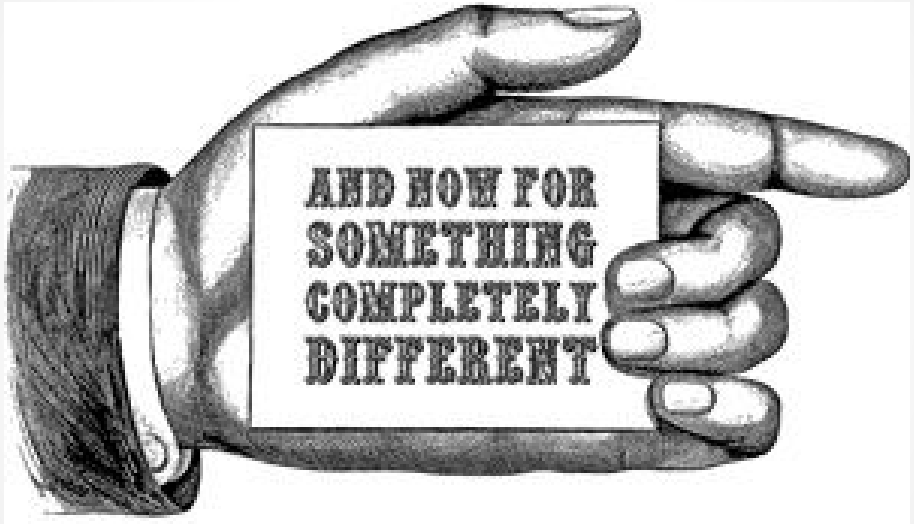


Public Key Exchange



Public Key Exchange




AND NOW FOR
SOMETHING
COMPLETELY
DIFFERENT

Public Key Cryptosystems

- E_k: {M} -> {M} ;; D_k: {M} -> {M}
- $D_k(E_k(M)) = E_k(D_k(M)) = M$
- E_k and D_k are “easy” to compute
- Given k, finding E_k and D_k is “feasible”
- Given just E_k, finding D_k is “infeasible”

Digital Signatures

- Alice computes $S = D_k(M)$
- S came from Alice iff $E_k(S) = M$
- Bob can keep S to prove M came from Alice

Trap Doors

- One-way functions are hard to invert
- One-way trap-door functions are too…
  - Unless you know the “trap door”
- A PKCS is a one-way trap-door function
- A one-way trap-door permutation is a PKCS
  - “one-to-one” and “onto”

Math Time

- Problems in P are always “easy”
  - a^X (mod n) is in P - (best known alg is O(log x))
- Problems in NP can be **checked** easily
  - You can check if $\log_a y = x$ by computing a^x (mod n)
  - So you can brute force it by trying all the x’s
- As yet unknown whether P<NP
  - No algorithm for finding $\log_a y$ (mod n) in P … yet

A Method for Obtaining Digital Signatures and Public Key Cryptosystems

R.L. Rivest, A. Shamir, and L. Adleman
(AKA “RSA”)

The RSA Algorithm

$$
\begin{aligned}
C \equiv\ & E(M) \equiv M^e \pmod{n}, \text{ for a message } M\ . \\
& D(C) \equiv C^d \pmod{n}, \text{ for a ciphertext } C\ .
\end{aligned}
$$

The RSA Algorithm

- Choose p and q; n = p*q

The RSA Algorithm

- Choose p and q; n = p*q
- Choose d relatively prime to (p-1)*(q-1)

The RSA Algorithm

- Choose p and q; n = p*q
- Choose d relatively prime to (p-1)*(q-1)
- Find e such that d*e = 1 (mod (p-1)*(q-1))

Proving Things

1. $X^{phi(n)} = 1 \pmod{n}$
2. phi(p) = (p-1) if p is prime
3. phi(n) = phi(p)*phi(q) = (p-1)*(q-1)
4. $D(E(M)) = E(D(M)) = M^{e*d}$
5. $M^{e*d} = M^{k*phi(n) + 1}$ since $e*d = 1 \pmod{phi(n)}$
6. $M^{k*phi(n) + 1} = M*(M^{k})^{phi(n)} = M$ by (1)
7. D(E(M)) = E(D(M)) = M

The RSA Algorithm

- Still theoretically unbroken
- Still in use all over the place
- The cool kids are using elliptic curves


The End