Symmetric Ciphers: 3DES (cont.)

Example: Target and 3DES

On Dec. 23, 2013, Target confirmed malware was to blame for an infection of its point-of-sale system that likely exposed details associated with 40 million debit and credit cards (50GB of encrypted data) between Nov. 27 and Dec. 15.

In its statement, Target notes that:
"The most important thing for our guests to know is that their debit card accounts have not been compromised due to the encrypted PIN numbers being taken."
"... PINs are encrypted at the keypad with what is known as Triple DES" - a standard the retailer refers to as being highly secure and used broadly throughout the U.S.

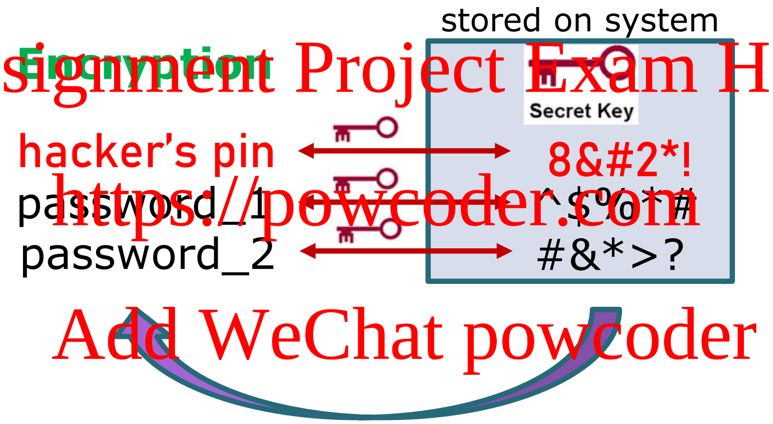
"Most people object to 3DES because it's an ancient algorithm that was designed as a patch for (now broken) DES until AES was finalized," ... "Now we've had AES for more than a decade, it's questionable why we'd be using 3DES."

https://threatpost.com/targets-use-of-3des-encryption-invites-scrutiny-worry/103389

Symmetric Ciphers: 3DES (cont.)

Example: Target and 3DES

Should passwords be encrypted?



Decryption is time consuming as it requires the search through 168/112 -bit key space!

Plus, passwords are hard to validate (likely not plain English words).

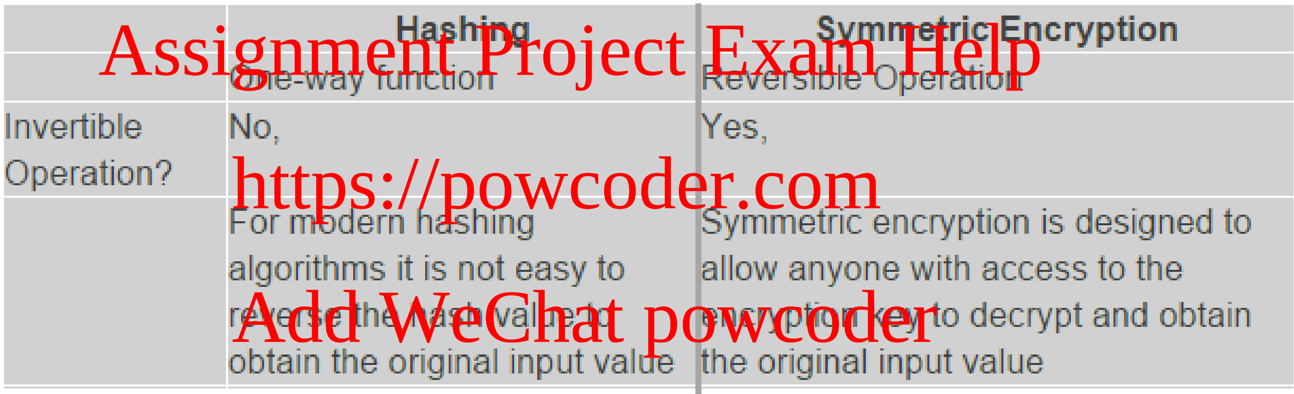
But, what if 'chosen plaintext' attack is conducted ??

If hacker knows one pin (e.g., his own) and its respective cyphertext in Target's database, he will be very quickly able to identify all other pins from the same POS device!

Symmetric Ciphers: 3DES (cont.)

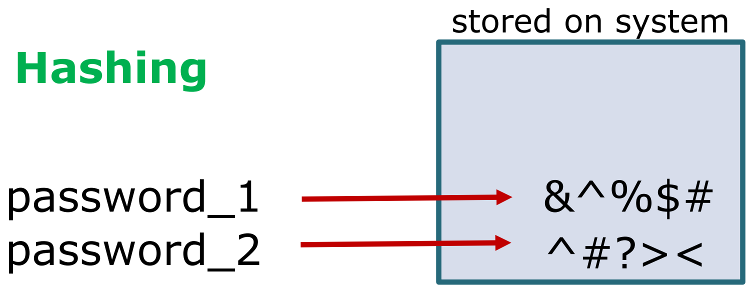
Example: Target and 3DES

Should passwords be encrypted?

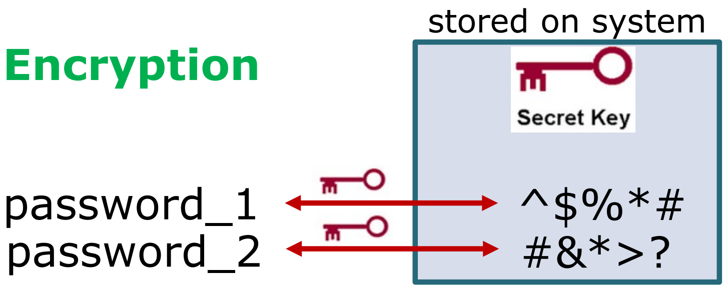


	Hashing	Symmetric Encryption
	One-way function	Reversible Operation
Invertible Operation?	No,	Yes,
	For modern hashing algorithms it is not easy to reverse the hash value to obtain the original input value	Symmetric encryption is designed to allow anyone with access to the encryption key to decrypt and obtain the original input value

http://www.darkreading.com/safely-storing-user-passwords-hashing-vs-encrypting/a/d-id/1269374



cracking one password does not assist in cracking other passwords – passwords have to be cracked 'one by one'

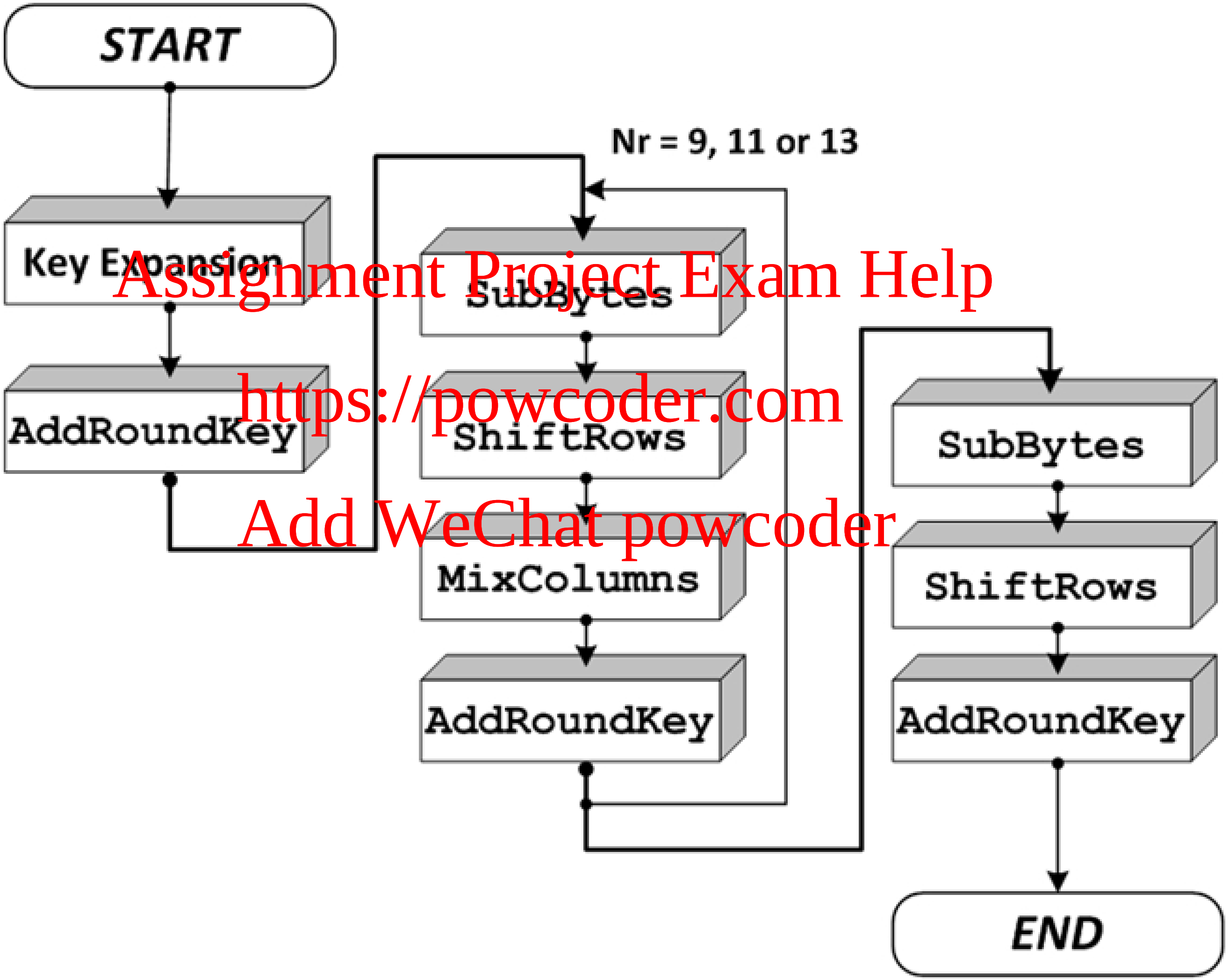


obtaining the key or cracking one password expedites cracking of all other passwords

Symmetric Ciphers: AES

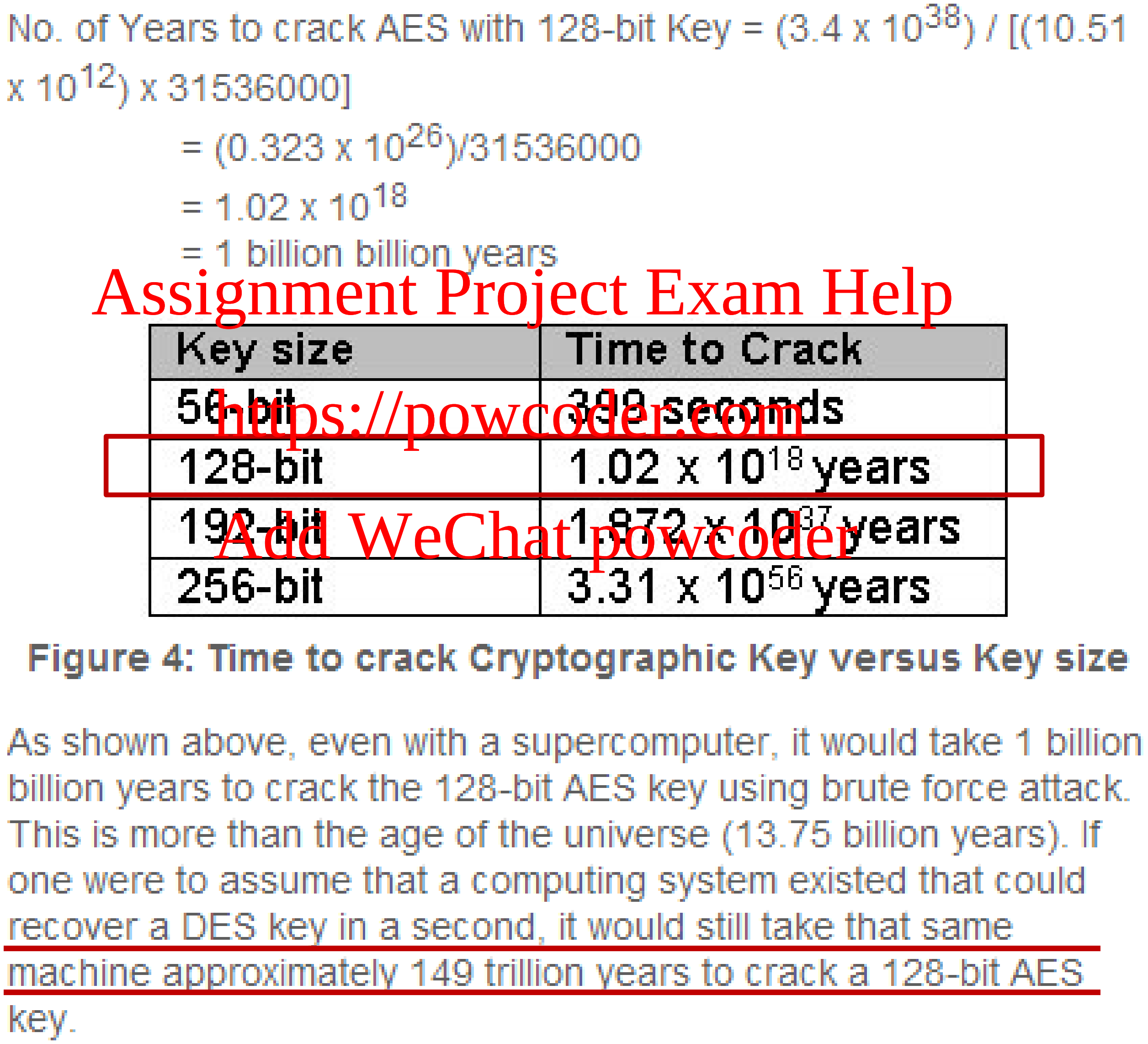
- **AES** – Advanced Encryption Standard
  - NIST issued call for a 3DES replacement in 1997 with requirements:
    - * symmetric block cipher
    - * block size 128
    - * key lengths 128, 192 or 256
  - initially 15, then 5 competing standards were evaluated
  - Rijndael cipher was selected as the most suitable for AES
  - AES became a US FIPS in November 2001
  - AES is intended to replace 3DES, but this process is taking longer than expected …

Symmetric Ciphers: AES (cont.)



https://www.youtube.com/watch?v=H2LlHOw_ANg

Symmetric Ciphers: AES (cont.)



No. of Years to crack AES with 128-bit Key = $(3.4 \times 10^{38}) / [(10.51 \times 10^{12}) \times 31536000]$

$= (0.323 \times 10^{26})/31536000$

$= 1.02 \times 10^{18}$

= 1 billion billion years

Key size	Time to Crack
56-bit	399 seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

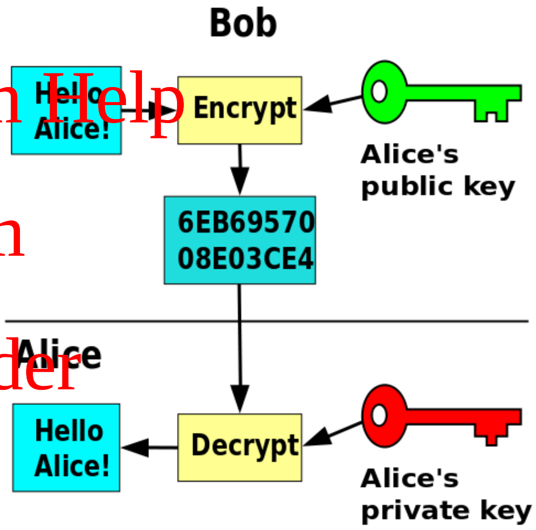
Figure 4: Time to crack Cryptographic Key versus Key size

As shown above, even with a supercomputer, it would take 1 billion billion years to crack the 128-bit AES key using brute force attack. This is more than the age of the universe (13.75 billion years). If one were to assume that a computing system existed that could recover a DES key in a second, it would still take that same machine approximately 149 trillion years to crack a 128-bit AES key.

http://www.eetimes.com/document.asp?doc_id=1279619 - July 2012

Asymmetric Ciphers

- **Asymmetric Encryption** – aka Public-Key Encryption – involves the use of two separate but related keys: public key and private key



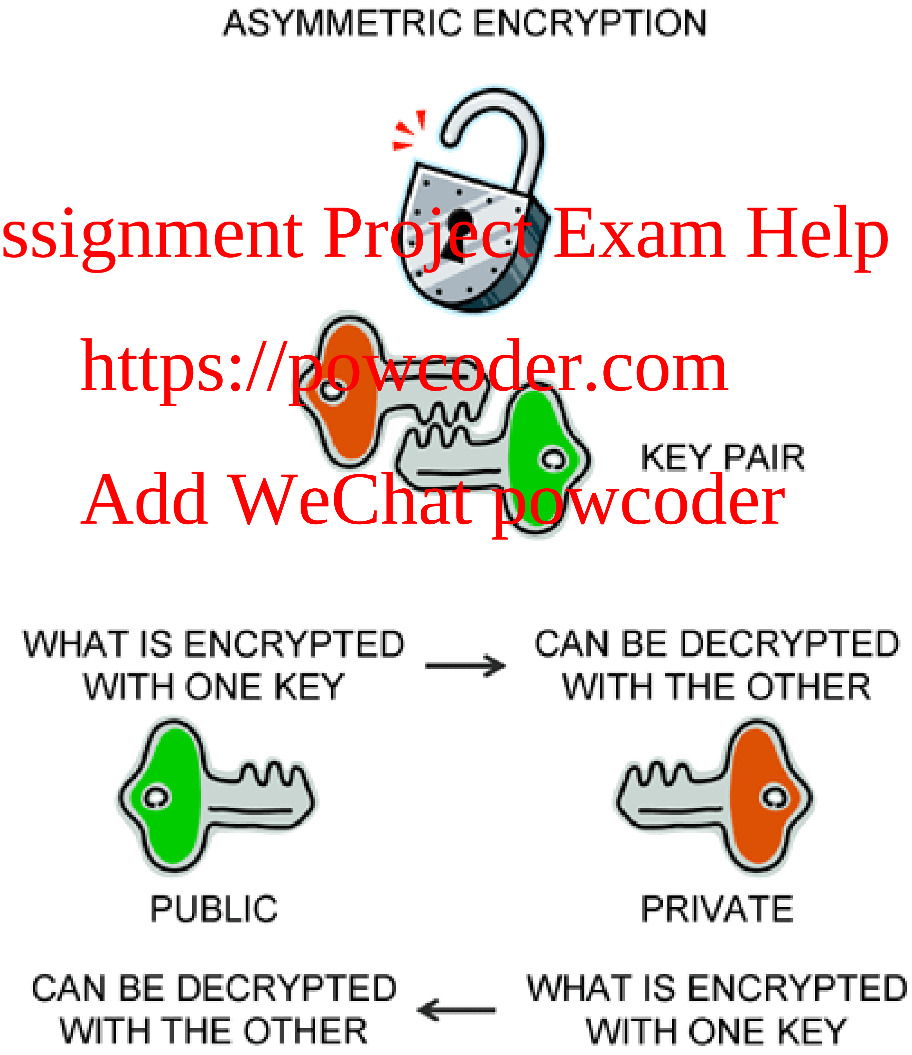
  - public key is made public for others to use, private key is known only to its owner
  - either key can encrypt a message – the other key must be used for decryption
  - first truly revolutionary advance in encryption, with profound consequences in the areas of

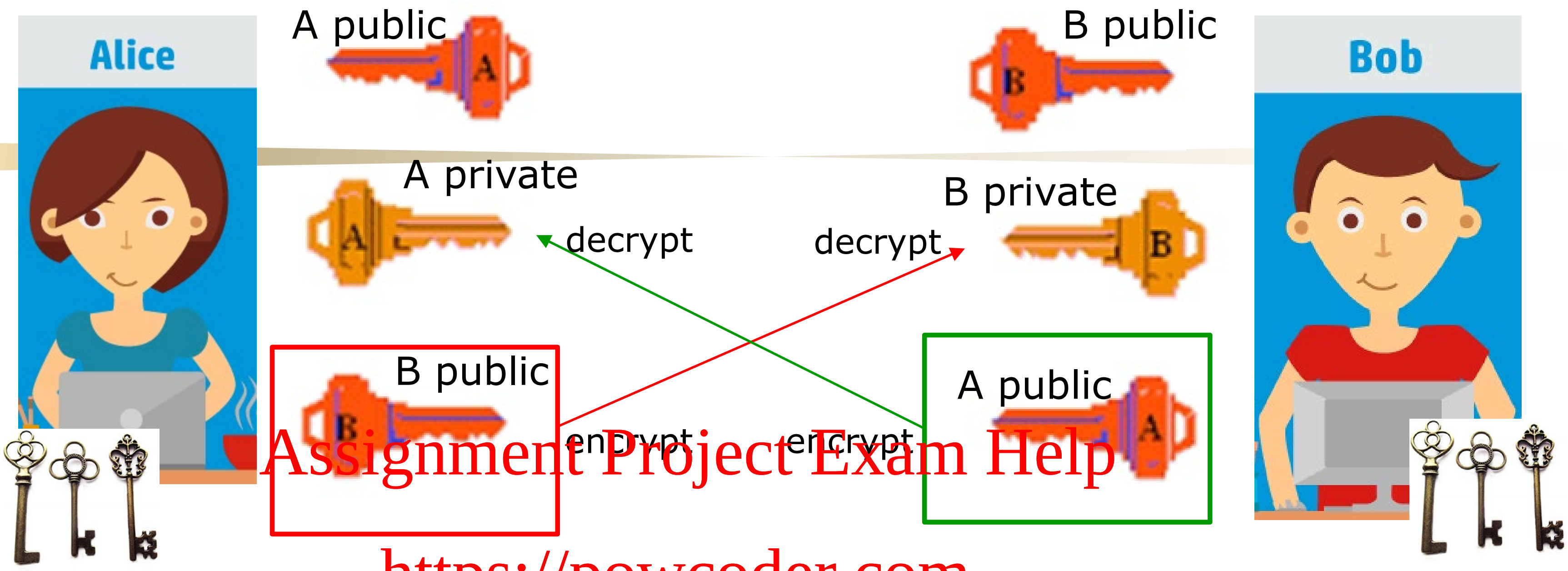
    * confidentiality

    * authentication

    * key distribution

Asymmetric Ciphers (cont.)

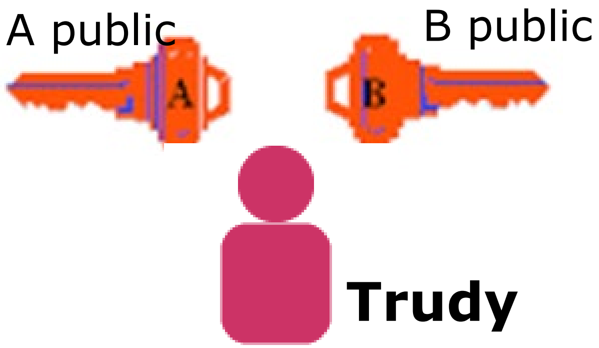

ASYMMETRIC ENCRYPTION
KEY PAIR
WHAT IS ENCRYPTED WITH ONE KEY
CAN BE DECRYPTED WITH THE OTHER
PUBLIC
PRIVATE
CAN BE DECRYPTED WITH THE OTHER
WHAT IS ENCRYPTED WITH ONE KEY



What key should Alice use to

a) Send a confidential message to Bob???

b) Receive a confidential message from Bob???



Asymmetric Ciphers (cont.)

Asymmetric Encryption: Mode 1.a)

Protection of Confidentiality: Alice receives message from Bob

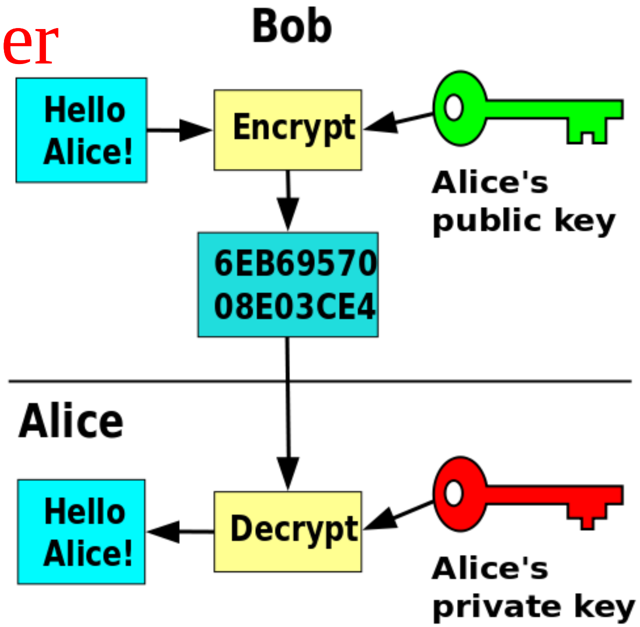
(1) Each user generates a pair of keys.

(2) Each user places one of the keys in a public register - this becomes the public key; the other is private key.

(3) If Bob wishes to send a private message to Alice, he uses Alice's public key.

(4) To decrypt Bob's message, Alice uses her private key.

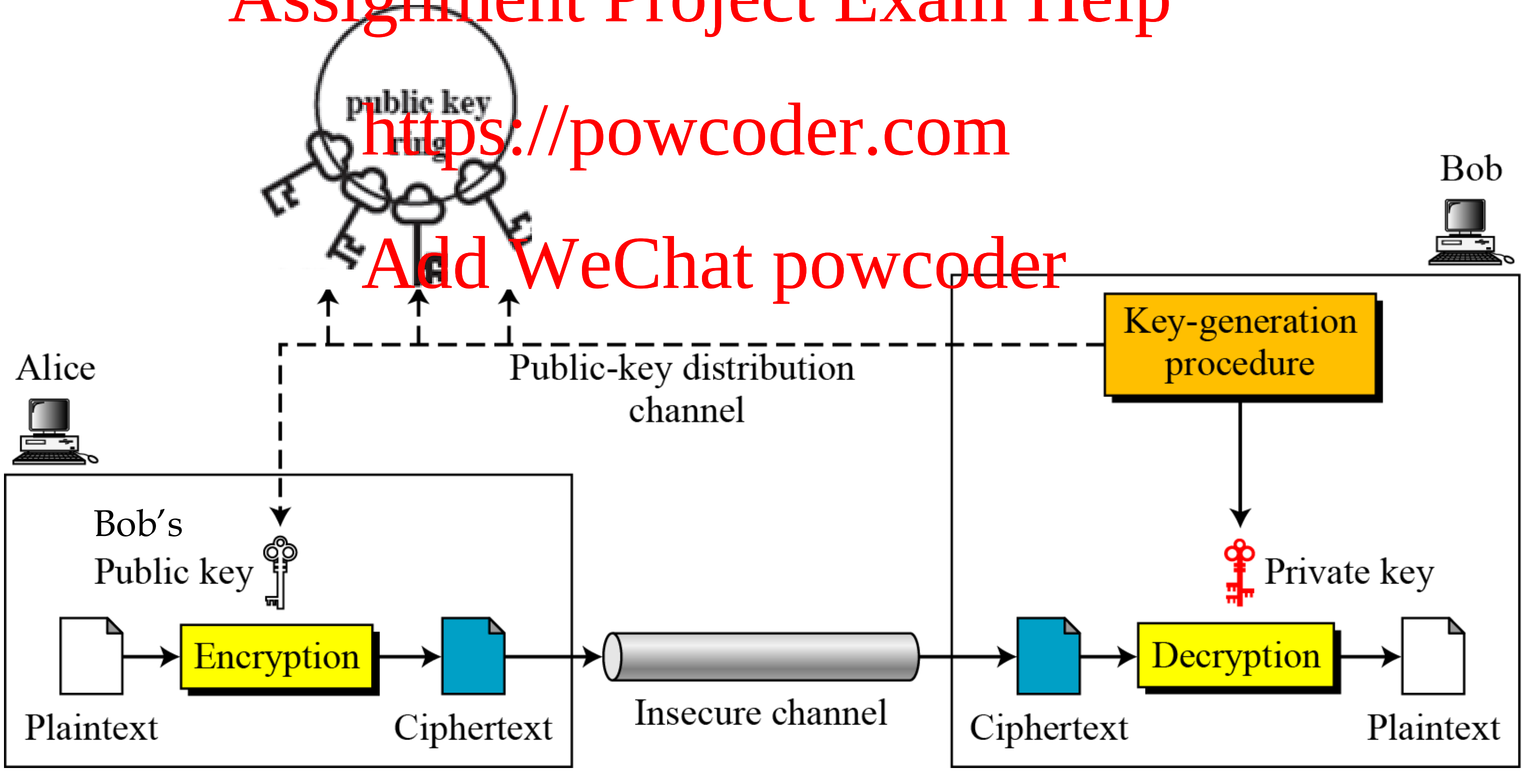
No other recipient can decrypt Bob's message as only Alice knows her key.



Asymmetric Ciphers (cont.)

Example: Asymmetric Encryption: Mode 1.b)

Protection of Confidentiality: Alice sends message to Bob



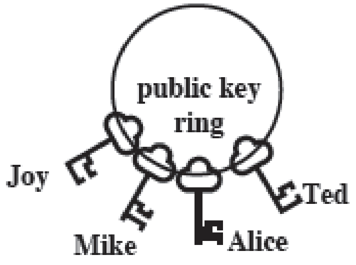
Cryptography and Network Security, B. E. Forouzan, pp. 295

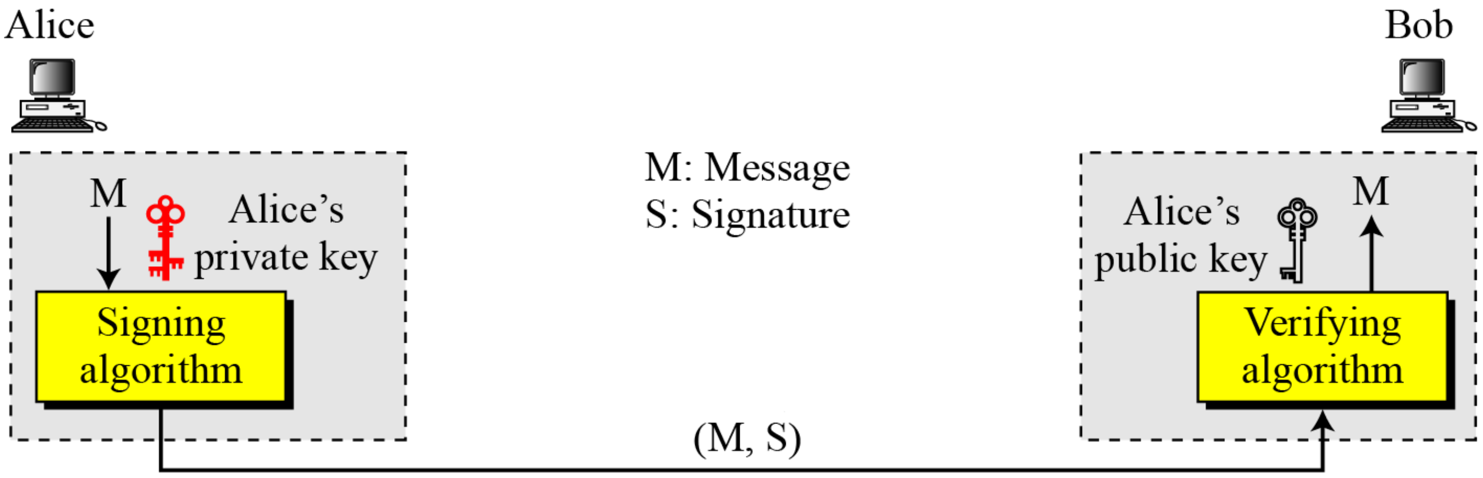
Asymmetric Ciphers (cont.)

Example: Asymmetric Encryption: Mode 2

Protection of Message & Sender Integrity

Alice sends a message to Bob - Bob is able to verify that Alice sent the message & data was not changed.





Cryptography and Network Security, B. E. Forouzan, pp. 391

Asymmetric Ciphers (cont.)

- **Symmetric vs. Asymmetric Encryption** – common misconceptions

(1) **public-key encryption is a general-purpose technique that has made symmetric encryption obsolete**

* public-key encryption is versatile but very slow – **symmetric encryption is still needed for encryption of large messages.**

* public-key encryption is used for authentication, digital signatures, and exchanges of secret keys!

(2) **exchange of asymmetric/public keys is much simpler than exchange of symmetric/secret keys**

* both schemes require a well established system and protocols

Asymmetric Ciphers (cont.)

- Symmetric vs. Asymmetric Encryption (cont.)

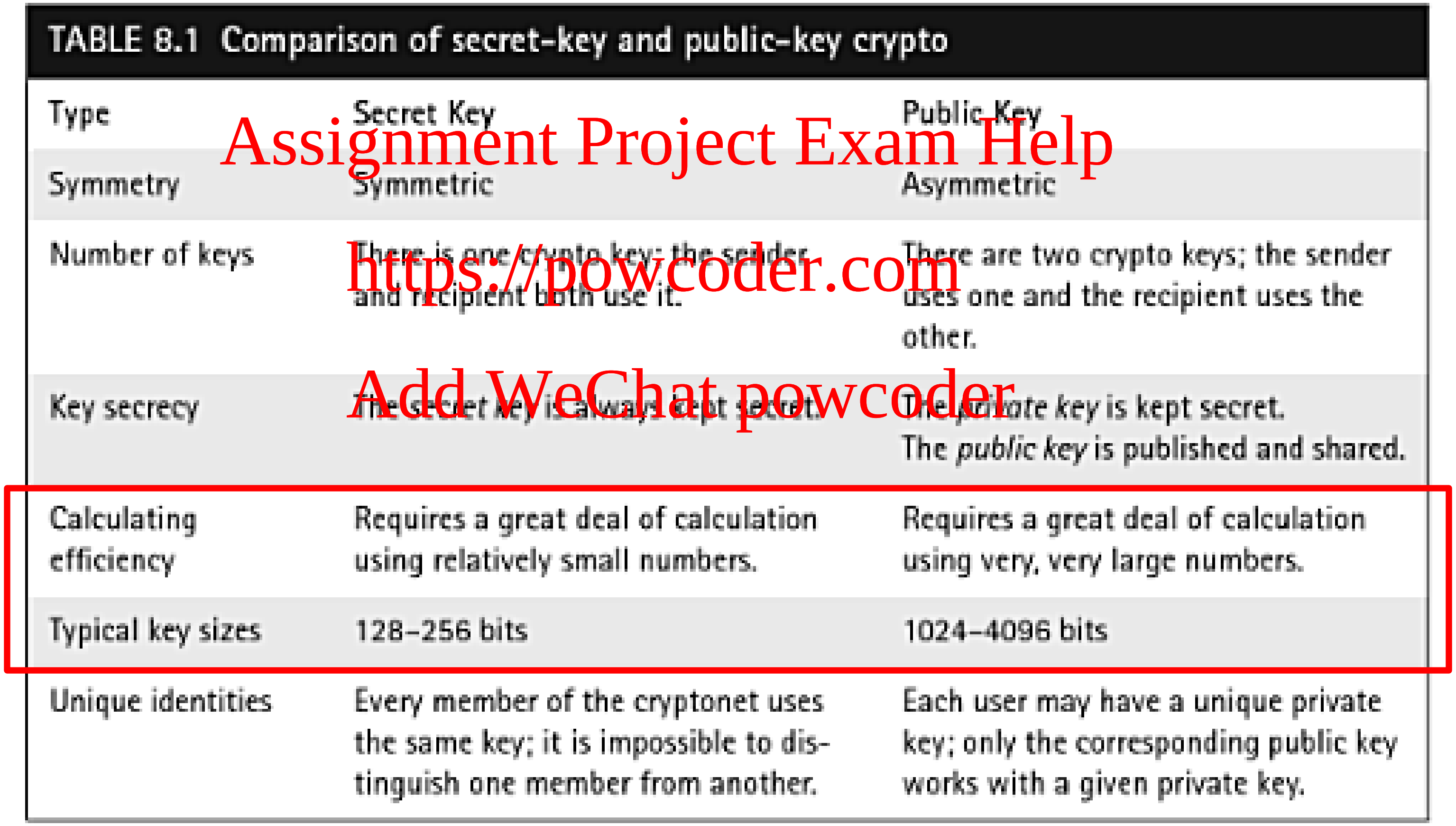


TABLE 8.1 Comparison of secret-key and public-key crypto

Type	Secret Key	Public Key
Symmetry	Symmetric	Asymmetric
Number of keys	There is one crypto key; the sender and recipient both use it.	There are two crypto keys; the sender uses one and the recipient uses the other.
Key secrecy	The *secret key* is always kept secret.	The *private key* is kept secret. The *public key* is published and shared.
Calculating efficiency	Requires a great deal of calculation using relatively small numbers.	Requires a great deal of calculation using very, very large numbers.
Typical key sizes	128–256 bits	1024–4096 bits
Unique identities	Every member of the cryptonet uses the same key; it is impossible to distinguish one member from another.	Each user may have a unique private key; only the corresponding public key works with a given private key.

Elementary Information Security, R. E. Smith, pp. 347