Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES AFFAIRES ÉTRANGÈRES ET DU DÉVELOPPEMENT INTERNATIONAL

DIRECTION GENERALE DE L'ADMINISTRATION
ET DE LA MODERNISATION

DIRECTION DES RESSOURCES HUMAINES

Sous-direction de la Formation et des Concours

Bureau des concours et examens professionnels
RH4B

CONCOURS EXTERNE ET INTERNE
DE SECRETAIRE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION
AU TITRE DE L'ANNEE 2017

EPREUVES ECRITES D'ADMISSIBILITE - 10 ET 11 JANVIER 2017

ANGLAIS

Traduction en français d'un texte à caractère technique rédigé en anglais.

Durée : 1 heure
Coefficient : 2
Toute note inférieure à 8 sur 20 est éliminatoire.

SUJET

Voir au dos de la feuille.

Security Experts Oppose Government Access to Encrypted Communication

By NICOLE PERLROTH JULY 7, 2015, New York Times

SAN FRANCISCO — A group of security technologists has concluded that the American and British governments cannot demand special access to encrypted communications without putting the world's most confidential data and critical infrastructure in danger.

A new paper from the group, made up of 14 of the world's pre-eminent cryptographers and computer scientists, is a formidable salvo in a skirmish between intelligence and law enforcement leaders, and technologists and privacy advocates. After Edward J. Snowden's revelations — with security breaches and awareness of nation-state surveillance at a record high and data moving online at breakneck speeds — encryption has emerged as a major issue in the debate over privacy rights.

That has put Silicon Valley at the center of a tug of war. Technology companies including Apple, Microsoft and Google have been moving to encrypt more of their corporate and customer data after learning that the National Security Agency and its counterparts were siphoning off digital communications and hacking into corporate data centers.

Yet law enforcement and intelligence agency leaders argue that such efforts thwart their ability to monitor kidnappers, terrorists and other adversaries.

The encryption debate has left both sides bitterly divided. The group of cryptographers deliberately issued its report a day before the director of the Federal Bureau of Investigation and the deputy Attorney general at the Justice Department, are scheduled to testify before a Senate Committee on their concerns that encryption technologies will prevent them from effectively doing their jobs.

The new paper is the first in-depth technical analysis of government proposals by a group of leading cryptographers and security thinkers. The report states that any effort to give the government "exceptional access" to encrypted communications was technically unfeasible and would leave confidential data and critical infrastructure like banks and the power grid at risk.

Handing governments a key to encrypted communications would also require an extraordinary degree of trust. The security specialists said authorities could not be trusted to keep such keys safe from hackers and criminals. They added that if the United States and Britain mandated backdoor keys to communications, China and other governments in foreign markets would be spurred to do the same.

"Such access will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend," the report said. "The costs would be substantial, the damage to innovation severe and the consequences to economic growth hard to predict. The costs to the developed countries' soft power and to our moral authority would also be considerable."/.