Università Ca'Foscari Venezia

Concorso pubblico, per titoli ed esami, per la copertura di n. 1 posto a tempo indeterminato di categoria C, posizione economica C1, area tecnica, tecnico scientifica ed elaborazione dati, per le esigenze dell'Ufficio Supporto e Sviluppo Tecnologico dell'Area Servizi Informatici e Telecomunicazioni dell'Università Ca' Foscari Venezia. bandito con DDG n. 13 prot. n. 1884 del 14/01/2022, pubblicato all'Albo on line di Ateneo il 18/02/2022.

Prova orale – TRACCIA 1

1. Il candidato spieghi in che modo si usa la funzione stampa unione di word.
2. Il candidato, con riferimento alla sicurezza dei dati, paragoni le due soluzioni per la lettura delle email: a) utilizzo del browser web b) utilizzo di un client di posta elettronica che scarichi le email sul PC.
3. Il candidato illustri la differenza tra il backup incrementale e il backup full. Nel caso del backup di un filesystem che tipo di backup consiglierebbe?
4. Il candidato illustri cosa si intende per dato personale.

Il candidato legga e traduca:

In 1972, the National Bureau of Standards (NBS), now the National Institute of Standards and Technology (NIST), initiated a program to protect computer and communications data. As part of that program, they wanted to develop a single, standard cryptographic algorithm. A single algorithm could be tested and certified, and different cryptographic equipment using it could interoperate. It would also be cheaper to implement and readily available. In the May 15, 1973 Federal Register, the NBS issued a public request for proposals for a standard cryptographic algorithm.

Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd Edition di Bruce Schneier ISBN: 9780471117094

Università Ca'Foscari Venezia

Concorso pubblico, per titoli ed esami, per la copertura di n. 1 posto a tempo indeterminato di categoria C, posizione economica C1, area tecnica, tecnico scientifica ed elaborazione dati, per le esigenze dell'Ufficio Supporto e Sviluppo Tecnologico dell'Area Servizi Informatici e Telecomunicazioni dell'Università Ca' Foscari Venezia. bandito con DDG n. 13 prot. n. 1884 del 14/01/2022, pubblicato all'Albo on line di Ateneo il 18/02/2022.

Prova orale – TRACCIA 2

1. Il candidato illustri il funzionamento della funzione cerca verticale di Excel.
2. Il candidato esponga cos'è un attacco DDOS e come è possibile proteggersi da questo tipo di attacchi.
3. Il candidato illustri cos'è una Macchina Virtuale elencando vantaggi e svantaggi del loro utilizzo.
4. Il candidato illustri cosa si intende, secondo il Regolamento UE 2016/679, per valutazione d'impatto sulla protezione dei dati personali e in quali casi è necessaria.

Il candidato legga e traduca:

In the early 1970s, non-military cryptographic research was haphazard. Almost no research papers were published in the field. Most people knew that the military used special coding equipment to communicate, but few understood the science of cryptography. The National Security Agency (NSA) had considerable knowledge, but they did not even publicly admit their own existence. Buyers didn't know what they were buying. Several small companies made and sold cryptographic equipment, primarily to overseas governments. The equipment was all different and couldn't interoperate. No one really knew if any of it was secure; there was no independent body to certify the security.

Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd Edition di Bruce Schneier ISBN: 9780471117094

Università Ca'Foscari Venezia

Concorso pubblico, per titoli ed esami, per la copertura di n. 1 posto a tempo indeterminato di categoria C, posizione economica C1, area tecnica, tecnico scientifica ed elaborazione dati, per le esigenze dell'Ufficio Supporto e Sviluppo Tecnologico dell'Area Servizi Informatici e Telecomunicazioni dell'Università Ca' Foscari Venezia. bandito con DDG n. 13 prot. n. 1884 del 14/01/2022, pubblicato all'Albo on line di Ateneo il 18/02/2022.

Prova orale – TRACCIA 3

1. Il candidato illustri il funzionamento delle tabelle pivot su Excel.
2. Il candidato esponga cos'è il phishing e come è possibile proteggersi da questo tipo di attacchi.
3. Il candidato descriva quali siano le funzioni di maggiore importanza per un software di videoconferenza da utilizzare per la didattica a distanza.
4. Il candidato illustri quali siano le precauzioni che andrebbero prese per l'invio tramite sistemi elettronici di un file contenente i dati personali di studenti.

Il candidato legga e traduca:

An NSA-employed acquaintance, when asked whether the government can crack DES traffic, quipped that real systems are so insecure that they never need to bother. Unfortunately, there are no easy recipes for making a system secure, no substitute for careful design and critical, ongoing scrutiny. Good cryptosystems have the nice property of making life much harder for the attacker than for the legitimate user; this is not the case for almost every other aspect of computer and communication security.

Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd Edition di Bruce Schneier ISBN: 9780471117094

Università Ca'Foscari Venezia

Concorso pubblico, per titoli ed esami, per la copertura di n. 1 posto a tempo indeterminato di categoria C, posizione economica C1, area tecnica, tecnico scientifica ed elaborazione dati, per le esigenze dell'Ufficio Supporto e Sviluppo Tecnologico dell'Area Servizi Informatici e Telecomunicazioni dell'Università Ca' Foscari Venezia. bandito con DDG n. 13 prot. n. 1884 del 14/01/2022, pubblicato all'Albo on line di Ateneo il 18/02/2022.

Prova orale – TRACCIA 4

1. Nel caso in cui si abbia un elenco di diversi prodotti disposti in vari magazzini e vogliamo sommare le quantità complessive disponibili come bisogna fare con excel?
2. Il candidato esponga cos'è un malware e come è possibile proteggersi da questo tipo di attacchi.
3. Il candidato illustri come attrezzerebbe un'aula per l'utilizzo nella didattica a distanza
4. Il candidato illustri cosa si intende per dato anonimo.

Il candidato legga e traduca:

High-quality ciphers and protocols are important tools, but by themselves make poor substitutes for realistic, critical thinking about what is actually being protected and how various defenses might fail (attackers, after all, rarely restrict themselves to the clean, well-defined threat models of the academic world). Ross Anderson gives examples of cryptographically strong systems (in the banking industry) that fail when exposed to the threats of the real world [43, 44]. Even when the attacker has access only to ciphertext, seemingly minor breaches in other parts of the system can leak enough information to render good cryptosystems useless.

Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd Edition di Bruce Schneier ISBN: 9780471117094

Università Ca'Foscari Venezia

Concorso pubblico, per titoli ed esami, per la copertura di n. 1 posto a tempo indeterminato di categoria C, posizione economica C1, area tecnica, tecnico scientifica ed elaborazione dati, per le esigenze dell'Ufficio Supporto e Sviluppo Tecnologico dell'Area Servizi Informatici e Telecomunicazioni dell'Università Ca' Foscari Venezia. bandito con DDG n. 13 prot. n. 1884 del 14/01/2022, pubblicato all'Albo on line di Ateneo il 18/02/2022.

Prova orale – TRACCIA 5

1. Il candidato illustri come, avendo due o più elenchi di nomi o numeri, si possono individuare i valori doppi con Excel.
2. Il candidato illustri come avviene un attacco Man in the Middle e come è possibile proteggersi da questo tipo di attacco.
3. Il candidato illustri come attrezzerebbe un'aula per la registrazione di pillole formative.
4. Il candidato illustri cosa si intende per data breach? Quali sono le azioni che si devono porre in essere nel caso si verifichi un data breach?

Il candidato legga e traduca:

One of the most dangerous aspects of cryptology (and, by extension, of this book), is that you can almost measure it. Knowledge of key lengths, factoring methods, and cryptanalytic techniques makes it possible to estimate (in the absence of a real theory of cipher design) the "work factor" required to break a particular cipher. It's all too tempting to misuse these estimates as if they were overall security metrics for the systems in which they are used. The real world offers the attacker a richer menu of options than mere cryptanalysis.

Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd Edition di Bruce Schneier ISBN: 9780471117094

Università Ca'Foscari Venezia

Concorso pubblico, per titoli ed esami, per la copertura di n. 1 posto a tempo indeterminato di categoria C, posizione economica C1, area tecnica, tecnico scientifica ed elaborazione dati, per le esigenze dell'Ufficio Supporto e Sviluppo Tecnologico dell'Area Servizi Informatici e Telecomunicazioni dell'Università Ca' Foscari Venezia. bandito con DDG n. 13 prot. n. 1884 del 14/01/2022, pubblicato all'Albo on line di Ateneo il 18/02/2022.

Prova orale – TRACCIA 6

1. Il candidato illustri se Excel ha una funzione per contare i giorni lavorativi, tenendo conto delle domeniche e dei giorni festivi infrasettimanali.
2. Il candidato illustri cos'è un attacco "zero-day" e come è possibile proteggersi da questo tipo di attacco.
3. Il candidato illustri quale sarebbe la dotazione standard migliore per un impiegato dell'università che deve svolgere la sua attività da remoto.
4. Il candidato illustri cosa si intende per dati pseudoanonimi e quando vanno considerati dati personali.

Il candidato legga e traduca:

An attempted cryptanalysis is called an attack. A fundamental assumption in cryptanalysis, first enunciated by the Dutchman A. Kerckhoffs in the nineteenth century, is that the secrecy must reside entirely in the key [794]. Kerckhoffs assumes that the cryptanalyst has complete details of the cryptographic algorithm and implementation. (Of course, one would assume that the CIA does not make a habit of telling Mossad about its cryptographic algorithms, but Mossad probably finds out anyway.) While real-world cryptanalysts don't always have such detailed information, it's a good assumption to make. If others can't break an algorithm, even with knowledge of how it works, then they certainly won't be able to break it without that knowledge.

Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd Edition di Bruce Schneier ISBN: 9780471117094

Università Ca'Foscari Venezia

Concorso pubblico, per titoli ed esami, per la copertura di n. 1 posto a tempo indeterminato di categoria C, posizione economica C1, area tecnica, tecnico scientifica ed elaborazione dati, per le esigenze dell'Ufficio Supporto e Sviluppo Tecnologico dell'Area Servizi Informatici e Telecomunicazioni dell'Università Ca' Foscari Venezia. bandito con DDG n. 13 prot. n. 1884 del 14/01/2022, pubblicato all'Albo on line di Ateneo il 18/02/2022.

Prova orale – TRACCIA 7

1. Il candidato illustri che cos'è il formato PDF/A e perché è di fondamentale importanza per la conservazione dei documenti?
2. Il candidato illustri la differenza tra la posta elettronica e la posta elettronica certificata.
3. Il candidato illustri cos'è un driver, a cosa serve, come si usa e quali sono i più comuni problemi legati ai drivers.
4. Il candidato illustri il concetto di accountability collegato con il GDPR

Il candidato legga e traduca:

The whole point of cryptography is to keep the plaintext (or the key, or both) secret from eavesdroppers (also called adversaries, attackers, interceptors, interlopers, intruders, opponents, or simply the enemy). Eavesdroppers are assumed to have complete access to the communications between the sender and receiver. Cryptanalysis is the science of recovering the plaintext of a message without access to the key. Successful cryptanalysis may recover the plaintext or the key. It also may find weaknesses in a cryptosystem that eventually lead to the previous results. (The loss of a key through noncryptanalytic means is called a compromise.)

Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd Edition di Bruce Schneier ISBN: 9780471117094

Università Ca'Foscari Venezia

Concorso pubblico, per titoli ed esami, per la copertura di n. 1 posto a tempo indeterminato di categoria C, posizione economica C1, area tecnica, tecnico scientifica ed elaborazione dati, per le esigenze dell'Ufficio Supporto e Sviluppo Tecnologico dell'Area Servizi Informatici e Telecomunicazioni dell'Università Ca' Foscari Venezia. bandito con DDG n. 13 prot. n. 1884 del 14/01/2022, pubblicato all'Albo on line di Ateneo il 18/02/2022.

Prova orale – TRACCIA 8

1. Il candidato illustri come si può convertire un file PDF in PDF/A.
2. Il candidato illustri cosa si intende per "two factor authentication" e quando ritiene che sia il caso di utilizzarla.
3. Il candidato illustri le differenze tra la telefonia tradizionale e telefonia VoIP.
4. Il candidato illustri il ciclo di vita del dato in relazione alla normativa privacy.

Il candidato legga e traduca:

Public-key algorithms (also called asymmetric algorithms) are designed so that the key used for encryption is different from the key used for decryption. Furthermore, the decryption key cannot (at least in any reasonable amount of time) be calculated from the encryption key. The algorithms are called "public-key" because the encryption key can be made public: A complete stranger can use the encryption key to encrypt a message, but only a specific person with the corresponding decryption key can decrypt the message. In these systems, the encryption key is often called the public key, and the decryption key is often called the private key.

Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd Edition di Bruce Schneier ISBN: 9780471117094

Università Ca'Foscari Venezia

Concorso pubblico, per titoli ed esami, per la copertura di n. 1 posto a tempo indeterminato di categoria C, posizione economica C1, area tecnica, tecnico scientifica ed elaborazione dati, per le esigenze dell'Ufficio Supporto e Sviluppo Tecnologico dell'Area Servizi Informatici e Telecomunicazioni dell'Università Ca' Foscari Venezia. bandito con DDG n. 13 prot. n. 1884 del 14/01/2022, pubblicato all'Albo on line di Ateneo il 18/02/2022.

Prova orale – TRACCIA 9

1. Il candidato illustri come è possibile evidenziare tutti i valori di una colonna superiori a 50 in Excel.
2. Il candidato descriva cos'è una Virtual Private Networks (VPN) e quali benefici comporta il suo utilizzo.
3. Il candidato illustri quali siano gli elementi fondamentali di un cablaggio strutturato.
4. Il candidato illustri la differenza tra marca temporale e riferimento temporale di un documento.

Il candidato legga e traduca:

Symmetric algorithms can be divided into two categories. Some operate on the plaintext a single bit (or sometimes byte) at a time; these are called stream algorithms or stream ciphers. Others operate on the plaintext in groups of bits. The groups of bits are called blocks, and the algorithms are called block algorithms or block ciphers. For modern computer algorithms, a typical block size is 64 bits—large enough to preclude analysis and small enough to be workable. (Before computers, algorithms generally operated on plaintext one character at a time. You can think of this as a stream algorithm operating on a stream of characters.)

Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd Edition di Bruce Schneier ISBN: 9780471117094

Università Ca'Foscari Venezia

Concorso pubblico, per titoli ed esami, per la copertura di n. 1 posto a tempo indeterminato di categoria C, posizione economica C1, area tecnica, tecnico scientifica ed elaborazione dati, per le esigenze dell'Ufficio Supporto e Sviluppo Tecnologico dell'Area Servizi Informatici e Telecomunicazioni dell'Università Ca' Foscari Venezia. bandito con DDG n. 13 prot. n. 1884 del 14/01/2022, pubblicato all'Albo on line di Ateneo il 18/02/2022.

Prova orale – TRACCIA 10

1. Il candidato descriva a cosa serve la seguente icona di word ¶.
2. Il candidato illustri i vantaggi e gli svantaggi dell'utilizzo dei sistemi SSO.
3. Il candidato illustri come procederebbe per la scelta delle caratteristiche tecniche dei computer di un laboratorio informatico.
4. Il candidato illustri la differenza tra Firma Digitale (FD) e Firma Elettronica Qualificata (FEQ).

Il candidato legga e traduca:

There are two general types of key-based algorithms: symmetric and public-key. Symmetric algorithms, sometimes called conventional algorithms, are algorithms where the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms, the encryption key and the decryption key are the same. These algorithms, also called secret-key algorithms, singlekey algorithms, or one-key algorithms, require that the sender and receiver agree on a key before they can communicate securely.

Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd Edition di Bruce Schneier ISBN: 9780471117094

Università Ca'Foscari Venezia

Concorso pubblico, per titoli ed esami, per la copertura di n. 1 posto a tempo indeterminato di categoria C, posizione economica C1, area tecnica, tecnico scientifica ed elaborazione dati, per le esigenze dell'Ufficio Supporto e Sviluppo Tecnologico dell'Area Servizi Informatici e Telecomunicazioni dell'Università Ca' Foscari Venezia. bandito con DDG n. 13 prot. n. 1884 del 14/01/2022, pubblicato all'Albo on line di Ateneo il 18/02/2022.

Prova orale – TRACCIA 11

1. Il candidato illustri che cosa si intende per "portabilità" di un programma software.
2. Il candidato illustri quali precauzione consiglierebbe ad un utente che svolge la sua attività 2 giorni a settimana in modalità di lavoro agile.
3. Il candidato illustri i vantaggi e gli svantaggi dell'utilizzo di un sistema VDI (virtual desktop infrastracture).
4. Il candidato illustri cosa si intende per "domicilio digitale".

Il candidato legga e traduca:

Restricted algorithms allow no quality control or standardization. Every group of users must have their own unique algorithm. Such a group can't use off-the-shelf hardware or software products; an eavesdropper can buy the same product and learn the algorithm. They have to write their own algorithms and implementations. If no one in the group is a good cryptographer, then they won't know if they have a secure algorithm. Despite these major drawbacks, restricted algorithms are enormously popular for low-security applications.

Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd Edition di Bruce Schneier ISBN: 9780471117094

Università Ca'Foscari Venezia

Concorso pubblico, per titoli ed esami, per la copertura di n. 1 posto a tempo indeterminato di categoria C, posizione economica C1, area tecnica, tecnico scientifica ed elaborazione dati, per le esigenze dell'Ufficio Supporto e Sviluppo Tecnologico dell'Area Servizi Informatici e Telecomunicazioni dell'Università Ca' Foscari Venezia. bandito con DDG n. 13 prot. n. 1884 del 14/01/2022, pubblicato all'Albo on line di Ateneo il 18/02/2022.

Prova orale – TRACCIA 12

1. Il candidato illustri la funzionalità della modalità "revisioni" di un documento word.
2. Il candidato illustri i vantaggi e gli svantaggi del salvataggio dei documenti di lavoro sul proprio portatile o sul Google drive dell'Ateneo.
3. Il candidato illustri vantaggi e svantaggi di un sistema di stampa centralizzato rispetto l'uso di stampanti locali.
4. Il candidato illustri le differenze tra lo scambio di messaggi tra due caselle PEC o tra una casella PEC e una casella di posta elettronica ordinaria.

Il candidato legga e traduca:

A cryptographic algorithm, also called a cipher, is the mathematical function used for encryption and decryption. (Generally, there are two related functions: one for encryption and the other for decryption.). If the security of an algorithm is based on keeping the way that algorithm works a secret, it is a restricted algorithm. Restricted algorithms have historical interest, but are woefully inadequate by today's standards. A large or changing group of users cannot use them, because every time a user leaves the group everyone else must switch to a different algorithm. If someone accidentally reveals the secret, everyone must change their algorithm.

Applied Cryptography: Protocols, Algorithms, and Source Code in C 2nd Edition di Bruce Schneier ISBN: 9780471117094